УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ
ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННОГО ПРОСТРАНСТВА

Сборник трудов
XIX Всероссийской научно-практической конференции
студентов, аспирантов и молодых ученых

(Екатеринбург, 8–11 декабря 2020 г.)

Министерство науки и высшего образования Российской Федерации
Уральское отделение Вольного экономического общества России
Уральский государственный экономический университет

Безопасность информационного пространства

Сборник трудов
XIX Всероссийской научно-практической конференции
студентов, аспирантов и молодых ученых

(Екатеринбург, 8—11 декабря 2020 г.)

Екатеринбург
Издательство Уральского государственного
экономического университета
2021

УДК 004.056(07)+621.391(07)
ББК 32.973я4+32.81я4
Б40

Б40 **Безопасность информационного пространства :** сб. тр. XIX Всерос. науч.-практ. конф. студентов, аспирантов и молодых ученых (Екатеринбург, 8—11 декабря 2020 г.) / [отв. за вып.: А. Ю. Коковихин, Д. М. Назаров, ред. кол.: А. Е. Плахин, Е. Н. Стариков] ; М-во науки и высш. образования Рос. Федерации, Урал. гос. экон. ун-т. — Екатеринбург : Изд-во Урал. гос. экон. ун-та, 2021. — 265 с.

ISBN 978-5-9656-0313-8

В сборнике представлены статьи участников XIX Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых «Безопасность информационного пространства». Рассмотрены актуальные вопросы организационного и правового обеспечения информационной безопасности в условиях цифровой экономики Российской Федерации. Анализируются современные научные и прикладные исследования в области технической защиты и программно-аппаратных средств защиты информации. Исследуются возможности применения математических методов информационной безопасности. Обсуждаются проблемы обеспечения компьютерной безопасности.

Материалы сборника будут интересны представителям академической науки, вузовским исследователям, соискателям ученых степеней, специалистам-практикам, магистрантам, студентам.

УДК 004.056(07)+621.391(07)
ББК 32.973я4+32.81я4

ISBN 978-5-9656-0313-8

Научные и прикладные исследования в области технической защиты информации

Е. А. Бусыгин
Уральский государственный университет путей сообщения, г. Екатеринбург

Средства мобильной связи как средства разведки

Аннотация. Статья раскрывает возможности мобильных устройств, используемые при шпионаже, и методы противодействия угрозам, обусловленным этими возможностями.
Ключевые слова: мобильный телефон; разведка; программа; SIM-карта.

Несколько десятилетий назад, когда правоохранительные органы и спецслужбы начали достаточно регулярно использовать все возможные устройства, предназначенные для «прослушки», чтобы сохранить неприкосновенность частной жизни от данного вида наблюдения, достаточно было закрыть окно или дверь. Прослушка телефонных разговоров и другие виды электронного наблюдения были ограничены и применялись только для мониторинга крошечного сегмента населения, в случаях наблюдения за подозреваемыми, диверсантами или политическими врагами.

В современном мире численность мобильных устройств растет огромными темпами. Так по состоянию на начало 2020 г. численность мобильных устройств составило около 14 млрд экземпляров[1]. В связи, с чем для разведки или правоохранительных органов появился еще один способ досконально кого-либо изучить, если на это есть причина или основание, это не составит особых проблем.

В настоящее время большинство мобильных телефонов состоит из дисплея, системной платы, SIM-карты, камер и все возможных датчиков. Непосредственный интерес для правоохранительных органов представляют следующие элементы мобильного устройства, а именно GPS-модуль, GSM-модуль, внутренняя память, динамик и конечно же камера. Но каждый элемент в отдельности не представляет никакой ценности, а лишь в совокупности они могут применятся как средства разведки.

Мобильные устройства могут быть очень мощным устройством при ведении как акустической, так и видовой разведки. В наше время технологии позволяют обеспечить работу мобильных устройств до нескольких недель, что в свою очередь позволит использовать мобильное

[1] *Статистический* сайт «Statista». URL: https://www.statista.com.

устройство как «акустическую закладку» позволяющую передавать информацию на дальние расстояния, активировать данное устройство на дальних расстояниях или же просто хранить полученную информацию на самом устройстве и в любой удобный момент забрать само устройство. Наличие камеры в мобильном устройстве позволяет вести видовую разведку, порой даже владелец устройства сам того не подозревая может осуществлять видовую разведку для правоохранительных органов или злоумышленников, всего лишь установив приложение из неофициальных источников, например замаскированное под один из популярных мессенджеров, начав при этом скрытно от владельца передавать изображения с камер на заданный адрес в сети «Интернет» или же любой другой аналогичной сети.

Так же необходимо сказать о SIM-карте, ведь благодаря ей можно получить огромное количество сведений об устройстве и его владельце, независимо от производителя устройства.

В 1999 г. израильскими программистами Алексом Бирюковым и Ади Шамиром был опубликован отчет об успешной атаке на алгоритм A5/1, используемый для передаваемых данных в стандарте GSM.

В 2009 г. немецкая хакерская группы CCC (Chaos Computer Club) объявила об удачной попытке взлома алгоритма кодирования данных в сетях GSM.

В 2013 г. Карстен Нол (Karsten Nohl), основатель компании Security Research Labs, заявил об обнаружении уязвимости SIM-карт со стандартом шифрования DES (Data Encryption Standard).

В 2019 г. появляется уязвимость, получившая название SimJacker, которая находится в программном обеспечении SIMalliance Toolbox Browser (S@T Browser).

SimJacker, находится в программном обеспечении SIMalliance Toolbox Browser (S@T Browser), встроенном в большинство SIM-карт, которые используются мобильными операторами как минимум в 30 странах мира. S@T Browser представляет собой приложение, которое устанавливается на SIM-карты, в том числе и на eSIM, как часть SIM Tool Kit (STK), и предназначено для того, чтобы мобильные операторы могли предоставлять своим клиентам разные базовые услуги[1].

Атака Simjacker подразумевает, что злоумышленник злоупотребляет данным механизмом и приказывает устройству жертвы передать данные о местоположении и IMEI, которые SIM-карта отправит в SMS-сообщении на стороннее устройство, и атакующий в итоге сможет узнать местоположение своей цели. При этом пострадавшие от атаки пользователи не видят никаких SMS-сообщений и других следов компрометации.

[1] *Электронный* журнала «Хакер». URL: https://xakep.ru.

То есть злоумышленники могут постоянно заваливать своих жертв SMS-сообщениями и таким образом отслеживать их местоположение постоянно, на протяжении долгих недель или даже месяцев. Так как атака Simjacker направлена на SIM-карту, она не зависит от платформы и типа устройства пользователя.

Используя GSM-модем за 10 долл., злоумышленники могут отправить на аппарат жертвы поддельное сообщение, содержащее вредоносный код, что позволит: IMEI целевого устройства; распространять любую информацию путем отправки поддельных сообщений от имени жертв; совершать звонки на платные номера; шпионить, приказав устройству позвонить по но-меру телефона злоумышленника; загружать вредоносные программы, заставляя браузер устройства открывать вредоносные веб-страницы; отключить SIM-карту; получать информацию о языке на устройстве, заряде аккумулятора и т.д.

Самыми популярными программами, направленными на негласные получения информации, считаются программы-трояны. Истории звонков, SMS сообщения и сообщения мессенджеров, учетные данные из приложений, мобильных банков — все это может попасть в руки спецслужб или злоумышленников. Некоторые программы-трояны имеют в своем арсенале возможность незаметно для владельца производить съемку с камеры мобильного телефона и отправлять запись, так же это касается и запись звуков.

Стоит понимать, что, используя мобильное устройство, владелец должен понимать, что у него в руках не только удобное устройство для связи, но и в нужный момент - средство визуальной и геоинформационной разведки, сбора персональных и иных данных и даже автоматизированного управления инфраструктурой, к которой он имеет подключение.

Программы-шпионы — это программное обеспечение, которое тайно собирает информацию о человеке или организации.

Широкое определение программ-шпионов также включает в себя любое программное обеспечение, используемое разведкой и правоохранительными органами, для шпионажа за людьми или организациями.

Типичная программа-шпион предполагает перечень базовых функций:

— мониторинг телефонных звонков. Данная функция записывает и хранит основную информацию о всех, входящих и исходящих, телефонных вызовах на целевом устройстве, в том числе номера телефонов, имена абонентов, время и дату вызовов, а также длительность разговора;

— email-мониторинг позволяет пользователю приложения получить доступ к содержанию электронных писем, в том числе контактную информацию, время и дату;

— SMS-мониторинг дает доступ к содержимому SMS сообщений, а также времени и дате их получения или отправке;

— мониторинг переписки в программах обмена сообщениями. Большинство шпионских приложений предлагают мониторинг некоторых программ обмена сообщениями. Некоторые из них ограничиваются одной или двумя программами, другие, более продвинутые шпионские приложения предлагают мониторинг почти всех популярных программ обмена сообщениями;

— история программ браузеров позволяет пользователю просматривать URL-адреса всех посещенных адресов в сети «Интернет», в том числе сведения о продолжительности сессий, частоту посещения и т.д.;

— мультимедиа мониторинг позволяет получить доступ, к хранящимся на устройстве файлов графических, аудио и видео форматов;

— мониторинг календаря и телефонной книги дает пользователю доступ к телефонной книге, мероприятиям и записям календаря;

— GPS мониторинг записывает и хранит сведения о географическом положении и передвижениях, зачастую в режиме реального времени. Некоторые шпионские приложения предлагают функцию уведомления, когда устройство входит или покидает указанную зону — данная функция имеет название «гео-ограничение».

В целях противодействия попадания информации, имеющейся на устройстве, необходимо соблюдать ряд правил:

— не устанавливать приложения на мобильные устройства, полученное от неизвестных лиц из неизвестных источников. В настоящее время официальные магазины приложения предлагают огромное количество приложений и всегда можно найти альтернативу необходимого приложения;

— установить антивирусное программное обеспечение и поддерживать их антивирусные базы в актуальном состоянии;

— обновлять операционную систему мобильного устройства до последней стабильно работающей версии;

— не передавать мобильное устройство неизвестным лицам;

— установить пароль на разблокировку устройства;

— не предоставлять доступ к устройству при помощи программ, предназначенных для удаленного доступа.

В заключении хотелось бы отметить, что чем старше мобильное устройства, тем вы более защищены от наблюдений и прослушки.

Р. В. Гибилинда
Уральский федеральный университет имени первого Президента России Б. Н. Ельцина,
г. Екатеринбург

Генерация шаблонов воздействий на файлы при расследовании инцидентов информационной безопасности

Аннотация. Описан алгоритм, позволяющий осуществить декомпозицию данных из воздействия на файл для создания шаблона воздействия. Алгоритм дает возможность классифицировать шаблон с позиции аномальности по отношению к информационной системе, в которой произошел инцидент информационной безопасности. Рассматривается инновационная активность как один из факторов экономической безопасности на примере машиностроения Свердловской области.

Ключевые слова: расследование инцидентов информационной безопасности; воздействие на файл; шаблон воздействия.

В рамках расследования инцидента информационной безопасности (ИБ) специалисту-аналитику зачастую приходится обрабатывать значительные объемы информации, связанной с инцидентом. Одним из типов информация является идентификация воздействий на файлы. В процессе функционирования информационной системы (ИС) наряду с санкционированными воздействиями, обусловленными штатными процедурами обработки информации, возникают несанкционированные, вызванные действиями злоумышленника, которые и представляют наибольший интерес для специалиста. Для выявления только несанкционированных воздействий, в целях уменьшения объема анализируемой информации, в работе предлагается алгоритм создания шаблонов воздействий на файлы, которые могут применяться при расследовании инцидентов ИБ.

Шаблон воздействия на файл G представляет собой совокупность фиксированных значений, полученных из полей идентифицированного воздействия и описывается вектором:

$$G = \{\langle G_{name}, G_{anomaly}\rangle, \langle I_G, I_{sign}\rangle, \langle D_G, D_{sign}\rangle, \langle N_G, N_{sign}\rangle, \langle R_G, R_{sign}\rangle\},$$

где в отношении к рассматриваемому шаблону воздействия:

— G_{name} — название шаблона воздействия;
— $G_{anomaly}$ — признак аномальности воздействия;

— I_G — множество значений, описывающих идентификаторы[1] файловых записей;

— D_G — множество значений, описывающих идентификаторы родительских каталогов[2];

— N_G — множество значений, описывающих имена[3] файлов;

— R_G — множество значений, описывающих идентификаторы[4] операций;

— I_{sign}, D_{sing}, N_{sign}, R_{sign} — признаки значимости соответствующих множеств значений I_G, D_G, N_G, R_G для воздействия на файл, описываемого шаблоном G.

Говоря об оценке аномальности воздействия $G_{anomaly}$, следует отметить, что этот параметр непосредственно связан с процедурой экспертной оценки и определяется специалистом-аналитиком, подготавливающим шаблон воздействия на файл с целью последующей их (воздействий) идентификации в рамках расследования инцидента ИБ.

Признаки значимости I_{sign}, D_{sing}, N_{sign}, R_{sign} могут принимать значение 0 или 1 и определяют необходимость использования значений из соответствующих множеств I_G, D_G, R_G при экспресс-анализе воздействий на файлы с использованием шаблонов.

Искомые множества I_G, D_G и R_G формируются автоматически посредством выборки уникальных числовых значений соответствующих полей после применения кластеризационного метода [1] идентификации воздействий на файлы.

Ввиду того, что значения из множества N_G представляют собой не числа, а наборы символов, то в целях повышения точности идентификации воздействий на файлы с применением шаблонов представим N_G как совокупность подмножеств N_{ed}, N_{ext}, N_{ft} и N_{sum}, где:

— N_{ed} — подмножество значений, характеризующих «степень различия» между именами файлов;

— N_{ext} — подмножество значений, описывающих расширения имен файлов;

— N_{ft} — подмножество значений, описывающих уникальные имена файлов;

---

[1] Уникальное числовое значение, используемое драйвером файловой системы для однозначного определения файла.

[2] Уникальное числовое значение, используемое драйвером файловой системы для установления соответствия между файлом и каталогом, в котором файл расположен.

[3] Битовая строка, используемая драйвером файловой системы для представления файла пользователю.

[4] Числовое значение, полученное из полей журналов операционной системы, характеризующее действие, совершенное по отношению к файлу.

— N_{sum} — подмножество значений, описывающих специальные символы[1], содержащиеся в именах файлов.

Значения, принадлежащие каждому из подмножеств N_{ed}, N_{ext}, N_{ft} и N_{sym}, могут быть значимы для шаблона независимо друг от друга. В связи с этим, значение N_{sign} представляется как совокупность значений признаков $N_{ed_{\text{sing}}}$, $N_{ext_{\text{sing}}}$, $N_{ft_{\text{sing}}}$, $N_{sym_{\text{sing}}}$.

Для определения сходств и различий между именами в целях формирования значений множества N_{ed} необходимо получить количественную величину, которая характеризует, насколько два имени файла в рамках одного воздействия отличаются друг от друга. В работах [2; 3] рассмотрен подробный анализ алгоритмов сравнения строк и приведены примеры метрик (перечень примеров не является исчерпывающим), используемых для определения сходства (расстояние) между строками d: метрика Левенштейна, метрика Хэмминга, «эпизодическая» метрика, метрика q-грамм. Примеры расчета расстояний между первым именем в идентифицированном воздействии и всеми остальными с использованием различных метрик указаны в таблице.

Примеры расчета расстояний между именами для различных идентифицированных воздействий

Идентифицированные воздействия	Имена файла(-ов) в рамках воздействия / исходное имя	Расстояние*			
		Л	Х	Э	q
Редактирование «офисного» документа в текстовом процессоре Microsoft Word	~$кладная.docx / Накладная.docx	2	2	∞	4
	WRD0000.tmp / Накладная.docx	14	–	∞	23
	WRL0001.tmp / Накладная.docx	14	–	∞	23
Шифрование файла вредоносным программным обеспечением Jigsaw	Photo0001.bmp.fun / Photo0001.bmp	4	–	∞	4
Шифрование файла вредоносным программным обеспечением WannaCry	Photo01.bmp.WNCRYT / Photo01.bmp	7	–	∞	7
	Photo01.bmp.WNCRY / Photo01.bmp	6	–	∞	6

Примечание. * Рассмотрены вышеуказанные метрики: Л — Левенштейна, Х — Хэмминга, Э — «эпизодическая», q — q-граммы (в рамках статьи $q = 2$).

Из таблицы видно, что в рамках одного идентифицированного воздействия на файл возможно как полное несовпадение имен, так и несущественные различия. Выбор типа метрики влияет на скорость работы алгоритма расчета расстояния и затраты памяти для хранения результатов вычислений. В процессе генерации шаблонов воздействий будем руководствоваться принципом: если расстояние d в нескольких одинаковых воздействиях на файл существенно отличается (непостоянно) и/или

[1] Символы, не являющиеся буквами, цифрами и пробелами, будем относить к категории специальных при рассмотрении имен файлов.

равно длине имени (полное несовпадение имен), то его не следует учитывать в шаблоне. Наоборот, если расстояние в нескольких одинаковых воздействиях на файл не отличается (постоянно), то оно должно быть использовано при генерации шаблона воздействия на файл. С позиции минимального значения расстояния *d*, скорости работы алгоритма расчета расстояния между строками и затрат памяти для хранения результатов вычислений оптимальным выглядит выбор метрики Левенштейна.

Результатом определения всех компонентов вектора *G* является сформированный шаблон воздействия на файл. Подготовленные шаблоны должны быть сохранены в базу данных для последующего применения. Использование базы данных шаблонов в рамках расследования инцидента ИБ позволяет существенно сократить временные затраты на идентификацию воздействий за счет отказа от ресурсоемких алгоритмов классификации в пользу простого сравнения данных о воздействиях на файлы с подготовленными шаблонами.

Библиографический список

1. *Гибилинда Р. В.* Кластеризационный метод идентификации воздействий на файлы с применением алгоритма k-средних, используемый при расследовании инцидентов информационной безопасности // Вестник УрФО. Безопасность в информационной сфере. 2020. № 1 (35). С. 35–47.

2. *Ukkonen E.* Approximate string-matching with q-grams and maximal matches // Theoretical Computer Science. 1992. Vol. 92, issue 1. P. 191–211.

3. *Navarro G.* A Guided Tour to Approximate String Matching // ACM Computing Surveys. 2001. Vol. 33, no. 1. P. 31–88.

А. В. Горев
Уральский государственный экономический университет, г. Екатеринбург

Интеллектуальный анализ DDoS-атак ботнета на IoT устройства при помощи Sap Analytics Cloud

Аннотация. Рассмотрены данные DDoS-атак на IoT устройства с целью их выявления. Проведено исследование с помощью SAP Analytics Cloud для поиска ключевых факторов при обнаружении атак.

Ключевые слова: DDoS; IoT; устройство; анализ; исследование; обнаружение атак.

Информационные технологии за последнее время скакнули далеко вперед и развиваются быстрыми темпами и сегодня. Но эти технологии были бы бессмысленны без интернета.

Интернет стал занимать неотъемлемое место в любом процессе. Информационные и телекоммуникационные технологии стали не только

частью повседневной жизни современного человека, но и необходимой технологической платформой для организации современных бизнес-процессов.

Активное развитие смартфонов, создание мобильных приложений для гаджетов уже сейчас позволяет оперативно отслеживать, фиксировать, сохранять различные аспекты жизни человека: от списка постоянных контактов, последовательности выполнения рабочих функций, осуществленных банковских трансакций, последних покупок до состояния физического и эмоционального самочувствия. Однако новые информационные технологии выводят уровень сбора, агрегации и обмена накопленной информацией на принципиально иной качественный уровень с минимальными ролью и степенью участия человека

Одной из таких информационных технологий стала концепция интернета вещей или The Internet Of Things, сокращенно IoT.

Суть этой технологии заключается в следующем. Вещи, основанные на встроенных технологиях взаимодействия друг с другом или с внешней средой, рассматривая организацию сетей как явление, которое может легко перестроить экономические и социальные процессы, исключающие необходимость участия человека из части действий и операций.

На самом деле это означает, что окружающие нас вещи в повседневной жизни (от самых простых, например, от умных часов, до автомобиля) могут передавать между собой необходимые данные, обеспечивающие максимальный комфорт для человека без его вмешательства.

Область применения таких устройств затрагивает все сферы человеческой жизни, от образовательных целей до элементов критически-важных инфраструктур, но для злых операторов ботнетов все они представляют собой лишь неисчерпаемый источник приумножения своих ботов. И злоумышленники используют их не только для кражи пользовательских данных — такие ботнеты являются чрезвычайно мощной стартовой площадкой для запуска разрушительных DDoS-атак.

Ботнет — это сеть компьютеров, которые управляются хакерами удаленно. Ботнеты используются преступниками для распространения программ-вымогателей на ваш ноутбук, устройство. Они могут быть не обнаружены даже антивирусом, и вы можете долгое время не догадываться, что ваш ноутбук, телефон, планшет или компьютер является частью ботнета.

Согласно прогнозам, в течение 2020 г. во всем мире станут онлайн порядка 20,4 млрд устройств. Операторы ботнетов ждут их с нетерпением. Эта неутомимая группа киберпреступников обязательно обрушит на них свой постоянно увеличивающийся ассортимент вредоносных

программных средств, ориентированных на растущий массив системных архитектур.

Низкая безопасность на многих устройствах интернета вещей делает их простыми мишенями, и владельцы устройств часто даже не подозревают об их заражении. Атаки на устройства IoT прогнозировались давно, чаще всего речь шла о домашней автоматизации и устройствах домашней безопасности. Сегодня политика злоумышленников приняла иную форму: сейчас, как правило, они не так заинтересованы в самой «жертве», как хотят захватить устройство, чтобы добавить его в ботнет, большая часть которого используется для совершения DDoS-атак.

DDoS-атака (Distributed Denial of Service) — атака, направленная на веб-сервер, сетевые инфраструктуры, а также трафик приложений с нескольких ресурсов, тем самым делая веб-сайты и позиции медленными или даже полностью недоступными.

Сегодня более 30 % всех зарегистрированных отключений вызваны DDoS-атаками. В глобальном масштабе ежедневно регистрируется две тысячи DDoS-атак. Средняя атака DDoS обходится крупной компании в 250 долл. в час.

Типичная DDoS-атака, связанная с IoT, осуществляется ботнетом некоторыми подключенными устройствами, которые были скомпрометированы с помощью атак фишинга, вредоносных действий и угадывания паролей. Во время процесса Command and Control (CNC) отображает IP-адреса устройств, расположенных в интернете, обнаруживает плохо защищенные гаджеты и заражает их вредоносными программами, которые необходимы для выполнения атаки. Таким образом, взломанный гаджет становится ботом, ожидающим дальнейших инструкций, и владельцы устройств даже не знают об этом, если не отслеживают сетевой трафик с помощью таких инструментов, как Wireshark.

Он может бездействовать в течение нескольких часов, дней или даже месяцев, прежде чем ботнет достигнет нужного размера; затем устройство приводится в действие. Боты подавляют своих жертв с помощью HTTP или DNS и UDP потоков или спама. 300 Гбит/с достаточно, чтобы сбить большинство веб-сайтов, которые не используют средства снижения DDoS. В случае атаки ботнета Mirai 2016, направленной на серверы Dyn и влияющей на производительность и доступность таких веб-сайтов, как Netflix, Reddit и Twitter, объемы трафика достигали 620 Гбит/с.

Проведем интеллектуальный анализ набора данных DDoS-атак ботнета на IoT устройства. Набор данных был взят с сайта системы организации конкурсов по исследованию данных, а также социальной сети специалистов по обработке данных и машинному обучению «Kaggle». Датасет называется DDoSdata и содержится в csv файле, он состоит из 47 столбцов, измерений и показателей, и более 2000 строк.

Интеллектуальный анализ проводился в SAP Analytics Cloud[1] по столбцу category, который в свою очередь включает в себя данные Normal и DDoS. После того как были внесены данные в программу для анализа, она составила резюме. Алгоритм прогнозирования с интеллектуальным обнаружением определил ряд столбцов, а именно 10, как ключевые факторы влияния для групп классификации столбца category (Категория трафика). Эти ключевые факторы влияния являются измерениями или показателями в модели DDoSdata, которые сильнее всего оказывают влияние на столбец category. Saddr (Исходный IP-адрес) оказывает наибольшее влияние, следом идет dpkts (Счетчик пакетов от места назначения до источника) и третий фактор это dbytes (Счетчик байтов назначения-источника) (рис. 1).

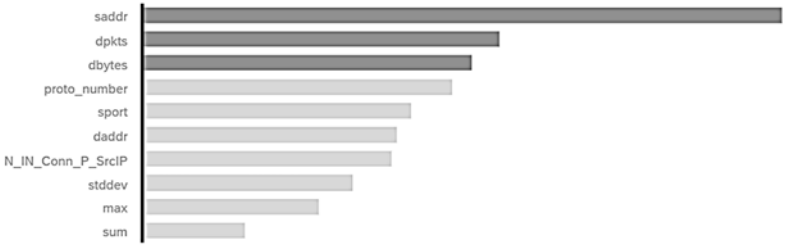


Рис. 1. Ключевые факторы влияния

Также можем увидеть, что saddr (Исходный IP-адрес) атакует с категорией flag «e» (флаги состояния потока, отображаемые в транзакциях) (рис. 2).

Большая часть атак проводились по протоколу tcp (рис. 3).

Скорее всего это связано с тем, что протокол TCP в отличие от UDP является более надежным при передаче данных, в нем не теряются отправленные пакеты, а приходят точно в таком же порядке, в котором и были отправлены.

При исследовании были выявлены важные факторы, которые наиболее значимы при выявлении DDoS-атаки на IoT устройства, а именно saddr, dpkts, dbytes. Данные можно применить при анализе и прогнозирование вредоносных пакетов от ботнетов DDoS. Также можно создать нейронную сеть, которая будет автоматически выявлять по ключевым показателям атаку.

[1] SAP Analytics Cloud — это облачное решение, объединяющее функции планирования, бизнес-аналитики и прогнозного анализа.

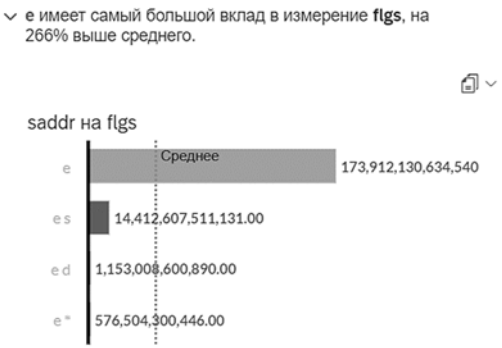


Рис. 2. Объект наибольшего вклада

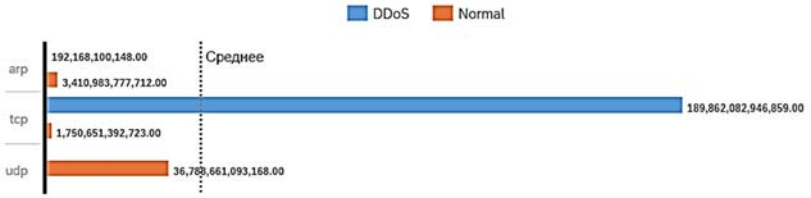


Рис. 3. Статистика атак на уровне протоколов

DDoS-атаки остаются основной целью вирусов, направленных на IoT. С быстрым ростом Интернета вещей увеличение вычислительных мощностей в устройствах может стать причиной изменения тактики в будущем, а у злоумышленников появятся новые возможности для майнинга криптовалют, кражи информации и сетевого шпионажа.

В. С. Колесниченко, Д. М. Назаров
Уральский государственный экономический университет, г. Екатеринбург

Использование интеллектуальных методов при обработке результатов специальных проверок и исследовании технических средств

Аннотация. Обсуждается существующая технология проведения специальных проверок и специальных исследований и возможности интеллектуализации этого процесса. Предполагается, что интеллектуализация этих процедур принесет значимый экономический эффект.

Ключевые слова: специальные проверки; специальные исследования; интеллектуальные методы.

В условиях цифровизации экономики наряду с положительными тенденциями присутствуют и ряд отрицательных факторов, связанных с зависимостью от импортных поставок научного, испытательного оборудования, приборов и электронных компонентов, программных и аппаратных средств вычислительной техники, стратегических материалов в большинстве секторов экономики России. Программа импортозамещения направлена на решение задачи снижения такой зависимости, но полностью избавиться от такой зависимости не представляется возможным в связи с объективной экономической реальностью — глобализации процессов мировой экономики. Поэтому одним из главных направлений обеспечения национальной безопасности в экономической деятельности является повышение уровня технологической безопасности, в том числе в информационном аспекте. Для этого совершенствуется государственная инновационная и промышленная политика, федеральная контрактная система и система государственного заказа развивается государственно-частное партнерство в области науки и технологий, проводятся системные исследования в интересах решения стратегических задач военной, государственной и общественной безопасности, устойчивого развития страны[1].

С целью защиты технических средств, содержащих конфиденциальную информацию и сведения, относящиеся к государственной тайне, проводятся специальные проверки и специальные исследования. Специальная проверка (далее — СП) — порядок действий, направленных на защиту технических средств, а именно, проверка оборудования и технических средств на отсутствие скрытых устройств, предназначенных

[1] *О Стратегии* национальной безопасности Российской Федерации: указ Президента РФ от 31 декабря 2015 г. № 683.

для негласного прослушивания, записи, перехвата и передачи информации[1].

СП технических средств проводится в целях сохранения конфиденциальности информации. Суть данной проверки состоит в том, чтобы удостовериться, что в устройствах нет записывающих и подслушивающих устройств, способствующих утечке информации — скрытых устройств негласного считывания информации.

Для прохождения проверки оформляется заявка и реквизиты организации, технические средства, которые необходимо проверить.

В процессе СП каждая единица подвергается исследованию, используя контрольно-измерительную аппаратуру, в том числе специализированные технические средства.

В ходе испытаний проверяются электромагнитные побочные излучения и наводки, выявляется канал утечки сведений из-за высокочастотного навязывания или облучения, акустоэлектрических преобразований, проводится дозиметрический контроль при помощи рентгенографического оборудования.

Все полученные результаты исследований вносятся в протокол. Документ содержит заключение о том, безопасно ли использовать заявленные технические средства в указанной работе. При обнаружении несоответствия приборов это указывается в протоколе.

Необходимость проведения специальных проверок регулируется Законом РФ от 21 июля 1993 г. № 5485-1 «О государственной тайне». Специальные исследования (далее — СИ) — комплекс действий, направленный на обнаружение потенциальных технических каналов утечки защищаемой информации с помощью специального контрольно-измерительного оборудования.

Проведение СИ определяет возможность считывания и перехвата сигнала специальными средствами разведки в рамках определенных границ (защищенность утечек по каналам ПЭМИН — побочные электромагнитные излучения и наводки).

В рамках специальных исследований выполняются:

— специальные исследования наводок и электромагнитных излучений;

— с использованием рентгенографического оборудования выполняется дозиметрический контроль;

— специальные исследования линий электропередач;

— специальные исследования виброакустических и акустических каналов.

[1] *Специальные* проверки и специальные исследования. URL: https://www.azone-it.ru/specproverki-i-specissledovaniya-tehnicheskih-sredstv.

Необходимость проведения СИ регулируется указом Президента РФ от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена», и обязует все организации, деятельность которых, связана с хранением, обработкой, передачей гостайны, проводить специальные проверки и специальные исследования технических средств иностранного производства.

Результатом специальных проверок и специальных исследований является документ, фиксирующий все этапы проверки и промежуточные итоги. Системой безопасности России в этом направлении накоплено множество результатов. Представляется возможным использовать этот потенциал для ускорения и удешевления процесса проверок и исследований. Для этого можно использовать различные алгоритмы и методы интеллектуального анализа данных. Действительно современные цифровые технологии позволяют обучить системы безопасности на накопленных данных и позволить им принимать решения об оптимизации процесса проверок, которая понимается нами широко от принятия решения какое оборудование использовать до получения значимого экономического эффекта.

В качестве приоритетных для обработки данных специальных проверок и специальных исследований можно выделить методы кластерного анализа данных, факторизационные алгоритмы, регрессионные модели в машинном обучении, нейросетевое моделирование и глубокое обучение. Итак, для повышения эффективности специальных проверок и специальных исследований технических средств предлагается применять не только организационно-управленческие меры, связанные с усилением контроля и систематического учета результатов и процедур, но и использования результатов и отчетов интеллектуального моделирования, основанного на исторических данных, которые позволят оптимизировать этот процесс с технической и экономической точек зрения.

Интеллектуальные специальные проверки и специальные исследования технических средств в последствии могут стать одним из трендов обеспечения безопасности в информационной среде.

А. А. Манилкин, А. Н. Рагозин
Южно-Уральский государственный университет — НИУ, г. Челябинск

Исследование предиктора информационных сигналов на основе фильтра линейного предсказания для целей обнаружения аномалий при автоматизированном управлении технологическими процессами

Аннотация. Рассмотрен предиктор информационных сигналов, наблюдаемых в системах управления технологическими процессами (АСУ ТП). Показано, что для обнаружения аномалий в наблюдаемых сигналах АСУ ТП информативным является сигнал ошибки предсказания предиктора, реализованного с использованием фильтра линейного предсказания.

Ключевые слова: фильтр линейного предсказания; обнаружение аномалий; система управления технологическими процессами.

Введение. Атаки, направленные на системы управления технологическими процессами (АСУ ТП), проявляются как аномалии в динамике наблюдаемых временных рядов данных, наблюдаемых с различных сенсоров АСУ ТП [1]. В исследовании, аномалии рассматриваются как неожидаемое изменение в поведении наблюдаемых процессов временных рядов данных АСУ ТП, отражаемое в виде существенного увеличения ошибки предсказания предиктора, построенного на основе фильтра линейного предсказания временных рядов данных, наблюдаемых с различных сенсоров АСУ ТП [2].

Если, расчет коэффициентов фильтра (синтез фильтра) производится исходно однократно на выбранном временном интервале рядов данных, полученных при нормальной работе АСУТП (работе АСУ ТП в штатном режиме, без влияния дестабилизирующих воздействий), то считается, что полученный (синтезированный) фильтр линейного предсказания является неадаптивным. Если, расчет коэффициентов фильтра (синтез фильтра) происходит с каждым новым отсчетом в реальном времени обрабатываемого сигнала, то считается, что фильтр линейного предсказания работает в адаптивном режиме.

Метод формирования сигнала ошибки предсказания предиктора. Формирователь сигнала ошибки предсказания предиктора, построенного с использованием адаптивного или неадаптивного фильтра линейного предсказания, приведен на рис. 1.

На рис. 1 отображено: $X(n)$ — подаваемый входной сигнал с сенсора АСУ ТП; $x(n)$ — предсказанное значение входного сигнала; LPC — фильтр линейного предсказания (адаптивный, или неадаптивный); $e(n)$ — сигнал ошибки предиктора, т.е. разность между текущим отсчетом входного сигнала $X(n)$ и его предсказанным значением $x(n)$; p — порядок фильтра.

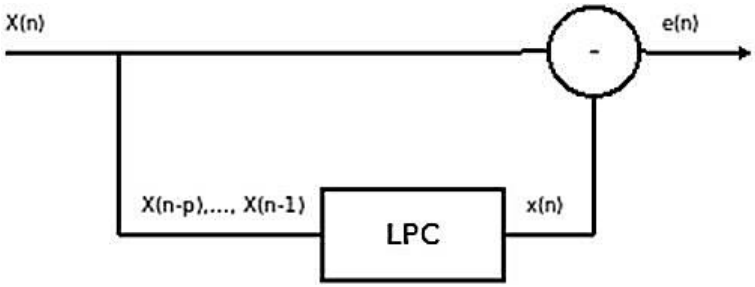


Рис. 1. Формирователь сигнала ошибки предсказания предиктора

Исследование сигнала ошибки предсказания предиктора. Исходный наблюдаемый сигнал без аномалий, полученный с выхода сенсора АСУ ТП, изображен на рис. 2.

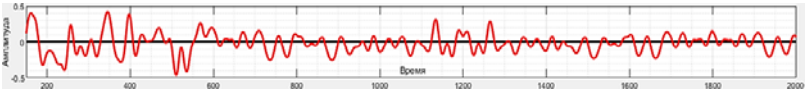


Рис. 2. Сигнал АСУ ТП без аномалий

На рис. 3 построены зависимости от величины порядка *p* фильтра величины среднеквадратического отклонения (СКО) сигнала ошибки предсказания, рассчитанной по всей длительности сигнала, при использовании неадаптивного фильтра и адаптивного фильтра. Порядок фильтра *p* линейного предсказания выбран равным 150, так как в этом случае значения СКО сигналов ошибок предсказания неадаптивного и адаптивного фильтров линейного предсказания наиболее близки и минимальны.

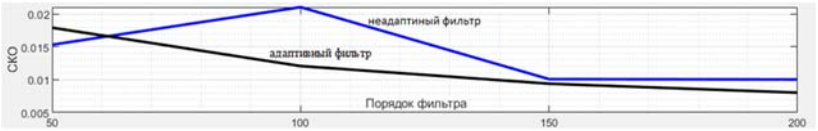


Рис. 3. Зависимость среднеквадратичного отклонения ошибки от порядка фильтра

Рассмотрим пример, когда вторая половина исходного сигнала заменяется на сигнал с другой временной структурой. В данном примере,

измененная вторая половина исходного сигнала заменена на более высокочастотный сигнал (рис. 4). Предполагается, что работа исследуемой АСУ ТП скачкообразно перешла в измененный (аномальный) режим работы, который может продолжаться длительное время.

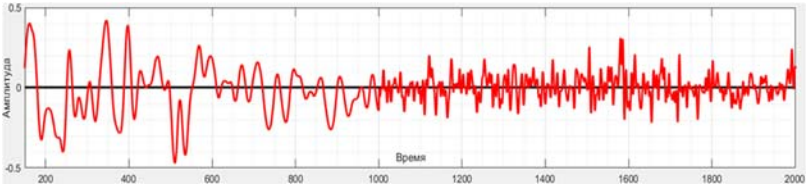


Рис. 4. Сигнал с длительной аномалией (вторая половина сигнала)

Графики сигнала ошибки предсказания для неадаптивного и адаптивного фильтра представлены на рис. 5 (вверху — неадаптивный фильтр, внизу — адаптивный фильтр).

Из анализа рис. 5, видно, что аномальные изменения обрабатываемого сигнала существенно изменяют амплитуду сигналов ошибки фильтров линейного предсказания, что может служить признаком при обнаружении по сигналам ошибки предсказания аномальных возмущений в обрабатываемом сигнале АСУ ТП.

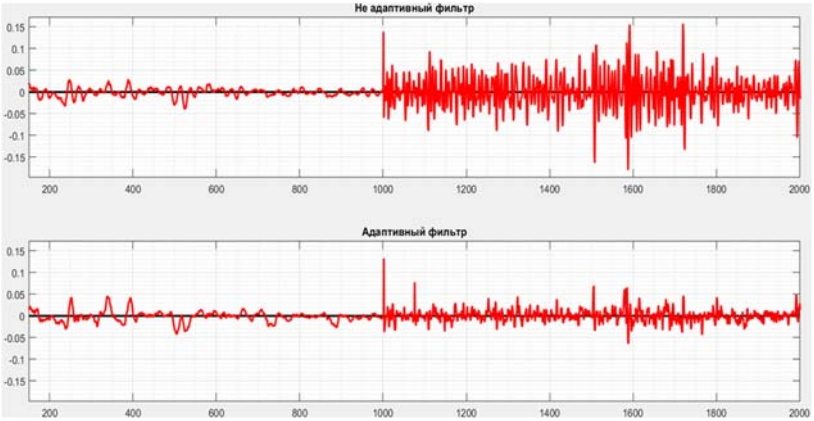


Рис. 5. Графики сигнала ошибок предсказания предиктора

Заключение. По сигналам ошибок предсказания, изображенным на рис. 5 видно, что в точке начала аномального возмущения исходного

сигнала (рис. 4), сигналы ошибок предсказания неадаптивного и адаптивного фильтров приобретают резкое скачкообразное изменение по амплитуде, что может служить признаком при обнаружении по сигналам ошибки предсказания (рис. 5) локального аномального возмущения в обрабатываемом исходном сигнале (рис. 4).

Далее, по сигналам ошибок предсказания, изображенным на рис. 5 также, видно, что сигнал ошибки (верхний рис. 5) неадаптивного фильтра линейного предсказания остается существенно большим по амплитуде на измененной (аномальной) части сигнала, при этом, сигнал ошибки адаптивного фильтра линейного предсказания значительно меньше по амплитуде на измененной (аномальной) части сигнала.

Поэтому, совместный анализ сигналов ошибок неадаптивного и адаптивного фильтров линейного предсказания позволяет обнаруживать длительные аномалии в исследуемых сигналах АСУ ТП.

Библиографический список

1. *Браницкий А. А., Котенко И. В.* Анализ и классификация методов обнаружения сетевых атак // Труды СПИ-ИРАН. 2016. № 2(45). С. 207−244. doi.org/10.15622/sp.45.13.

2. *Рагозин А. Н.* Применение цифровой обработки сигналов и нейронной сети при формировании прогноза временных рядов данных для целей обнаружения аномалий при автоматизированном управлении технологическими процессами // Вестник УрФО. Безопасность в информационной сфере. 2020. № 1 (35). С. 24–34.

Д. Ю. Мельников
Уральский государственный экономический университет, г. Екатеринбург

Интеллектуальный анализ данных трафика компьютерной сети для выявления угроз безопасности при помощи SAP Analytics Cloud

Аннотация. Рассмотрены данные трафика компьютерных сетей с целью обнаружение аномалий и атак. Проведено исследование с использованием интеллектуального анализа сервиса SAP Analytics Cloud, выявлены факторы, влияющие на определения типа атаки.

Ключевые слова: интеллектуальный анализ; IDS; безопасность; компьютерные сети.

С огромным ростом использования компьютерных сетей и увеличением количества приложений, работающих в них, сетевая безопасность становится все более важной. Все компьютерные системы страдают от уязвимостей безопасности, поэтому их своевременное обнаружение и устранение является важнейшей задачей служб и специалистов

в области информационной безопасности. Процесс этот характеризуется технической и интеллектуальной сложностью, а также достаточно большими экономическими затратами [2]. Таким образом, роль систем обнаружения вторжений (IDS) как устройств специального назначения для обнаружения аномалий и атак в сети становится все более важной. Цель исследования состоит в том, чтобы провести интеллектуальный анализ на основе данных систем IDS в мировом масштабе и выявить наиболее значимые факторы, влияющие на распознавание типов компьютерных атак.

Системы обнаружений вторжений и методы их работы. Система обнаружения вторжений (IDS) представляет собой систему, которая контролирует сетевой трафик за подозрительную активность и выдают предупреждения, когда такая деятельность обнаружена [5]. Это программное приложение, которое сканирует сеть или систему на предмет вредоносной активности. Информация о любом инциденте обычно сообщается либо администратору, либо собирается централизованно.

Хотя системы обнаружения вторжений контролируют сети на предмет потенциально вредоносной активности, они также имеют возможность выдавать ложные тревоги. Следовательно, организациям необходимо точно настроить конфигурации систем IDS при их первой установке [4]. Однако ситуация при эксплуатации сетей постоянно изменяется, поэтому перенастройка систем IDS должна проводится регулярно на основе анализа данных, собираемых этими системами с конкретного объекта.

Методы сбора данных о работе сети системами IDS:

— *сигнатурный*: IDS на основе подписи обнаруживает атаки на основе определенных шаблонов, таких как количество байтов, или количество единиц, или количество нулей в сетевом трафике, также обнаруживает на основе уже известной вредоносной последовательности инструкций, которая используется вредоносным ПО [5];

— *аномальный*: IDS на основе аномалий была введена для обнаружения атак неизвестного вредоносного ПО, с использованием машинного обучения для создания доверенной модели деятельности, и все, что приходит, сравнивается с этой моделью и объявляется подозрительным, если это не обнаруживается в модели [1].

Интеллектуальный анализ данных с помощью SAP Analytics Cloud. С целью дальнейшего построения алгоритма для правильной настройки IDS нужно выполнить интеллектуальный анализ. Для его реализации был найден датасет на сервисе «Kaggle» под названием «Network Anamoly Detection», на основе которого и будут вывялятся зависимости типов атак от различных показателей сети. Для проведения анализа был выбран SAP Analytics Cloud [3].

Выбранный датасет был загружен и после загрузки было проведено редактирование данных. Были объединены 39 типов атак в четыре группы (см. таблицу).

Классификация атак

Группа	Тип атаки
DoS	Back, Land, Neptune, Pod, Smurf,Teardrop,Apache2, Udpstorm, Processtable, Worm
Probe	Satan, Ipsweep, Nmap, Portsweep, Mscan, Saint
R2L	Guess_Password, Ftp_write, Imap, Phf, Multihop, Warezmaster, Warezclient, Spy, Xlock, Xsnoop, Snmpguess, Snmpgetattack, Httptunnel, Sendmail, Named (16)
U2R	Buffer_overflow, Loadmodule, Rootkit, Perl, Sqlattack, Xterm, Ps

Датасет состоит из 40 столбцов, измерений и показателей, и более чем 2000 строк.

После проведения интеллектуального анализа мы можем наблюдать, что 3 ключевых фактора влияющих на группу атаки являются Srv_count, Same_srv_rate, Dst_host_count (рис. 1).

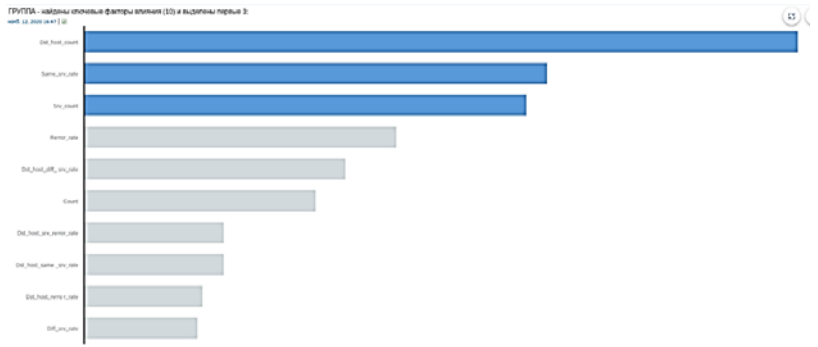


Рис. 1. Ключевые факторы

Самый популярный тип протокола при совершении атаки является TCP (рис. 2).

На рис. 3 представлено моделирование влияния ключевых факторов. Мы можем изменять значения и тем самым точнее определять какая атака была совершена.

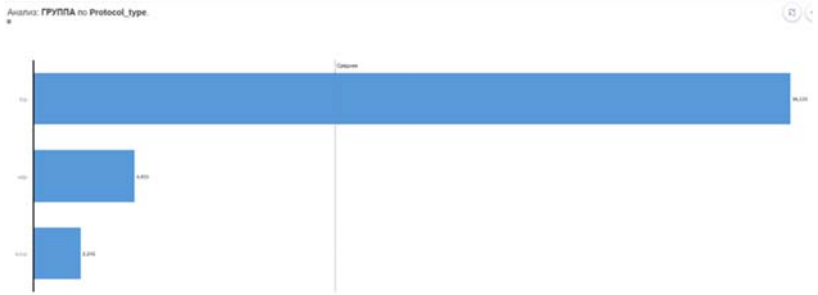


Рис. 2. Типы протокола передачи данных

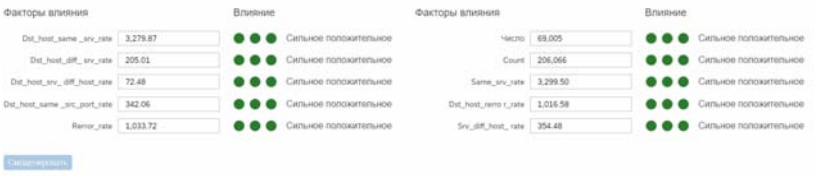


Рис. 3. Моделирование влияния ключевых факторов

На рис. 4 были проведены изменения ключевых факторов, но их влияние остается прежним.

Рис. 4. Изменение численных показателей ключевых факторов

При исследовании были выявлены важные факторы такие как Srv_count, Same_srv_rate, Dst_host_count, которые наиболее значимы для определения типа атаки. Данные исследования можно применить при настройке новой или установленной IDS, а также при создании собственного алгоритма определения компьютерной атаки. Еще один вариант использовать исследование при создании нейронной сети.

Библиографический список

1. *Васильев В. И.* Интеллектуальные системы защиты информации: учеб. пособие. 3-е изд., испр. и доп. М.: Инновационное машиностроение, 2017.

2. *Mann I.* Hacking the Human: Social Engineering Techniques and Security Countermeasures. Gover Publishing Ltd, 2012.

3. *Nazarov D. M., Morozova A. S., Kokovikhin A. Y.* SAP analytic cloud: A tool for the formation of professional competencies of business analyst. Paper presented at the CEUR Workshop Proceedings, 2570.

4. *Nazarov D. M., Nazarov A. D., Kovtun D. B.* Building technology and predictive analytics models in the SAP analytic cloud digital service. Paper presented at the Proceedings - 2020 IEEE 22nd Conference on Business Informatics, CBI 2020, 2 106-110. doi:10.1109/CBI49978.2020.10067.

5. *Roebuck K.* IPS — Intrusion Prevention System. Emereo Publishing, 2011.

А. Д. Плетенкова
Южно-Уральский государственный университет — НИУ, г. Челябинск

Исследование методов эквализации изображений в системах охранного телевидения

Аннотация. Исследуются технологии цифровой обработки сигналов, применяемые для повышения качества изображений в системах охранного телевидения. Представлены сравнительные результаты анализа эффективности применения методов простой, степенной и скользящей (адаптивной) эквализации реальных цифровых изображений.

Ключевые слова: цифровая обработка изображений; эквализация изображений; системы охранного телевидения.

Введение. Системы охранного телевидения являются одной из наиболее важных и необходимых составляющих обеспечения технической защиты информации на объектах [3].

Задача идентификации объектов на изображениях системы охранного телевидения сводится, к распознаванию и интерпретации зрительных образов для принятия последующих решений, что приводит к требованиям высокого качества формируемых изображений в условиях широкого изменения параметров внешней среды.

Цифровая обработка изображений начинается с этапа предварительной обработки, которая включает в себя исправление различных дефектов цифрового изображения.

Методы цифровой эквализации изображений. Самым распространенным дефектом изображений является слабый контраст (разность максимального и минимального значений яркости) [1].

В изображениях с низким контрастом содержатся только некоторые возможные значения элементов изображения (значения яркости).

Если, значения яркости группируются около больших значений, тогда изображение оказывается слишком светлым, если около малых, то слишком темным [2; 4; 5].

Для сравнения приведена гистограмма распределения яркости для малоконтрастного изображения (рис. 1, 2) и гистограмма высококонтрастного изображения, полученного методом цифровой эквализации (рис. 3, 4).

Рис. 1. Малоконтрастное изображение

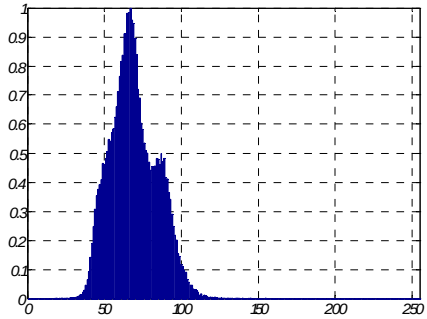


Рис. 2. Гистограмма малоконтрастного изображения

Рассмотрим разницу между двумя изображениями (рис. 1, рис. 3). До реализации процедуры эквализации изображения на рис. 1 распределение яркостей, т. е. гистограмма существенно локализована. При

этом, на рис. 4 для сравнения представлена выровненная гистограмма, которая получена после применения процедуры эквализации.

На рис. 4 видно, что гистограмма распределения яркостей стала более равномерной, а локализованные области максимальной плотности ярких участков исчезли. В свою очередь, это привело к тому, что контраст некоторых областей стал сильнее и динамический диапазон изображения стал более насыщенным, а это означает, что качество изображения стало выше.

Рис. 3. Высококонтрастное изображение

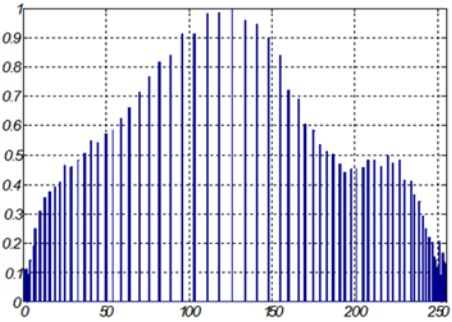


Рис. 4. Гистограмма высококонтрастного изображения

Сравнение исходного и обработанного изображений показывает, что происходящее при обработке перераспределение яркостей приводит к улучшению визуального восприятия.

В результате эквализации, в большинстве случаев существенно расширяется динамический диапазон изображения, что позволяет отобразить ранее незамеченные детали. Кроме того, стоит отметить еще одну важную особенность процедуры эквализации: в отличие от большинства фильтров и градационных преобразований, требующих настройки параметров (апертуры и констант градационных преобразований), эквализация гистограммы может выполняться в полностью автоматическом режиме без участия оператора.

Данная операция основана на том, что для каждого элемента m с координатами (x, y) в двумерной плоскости координат производится расчет по следующей формуле:

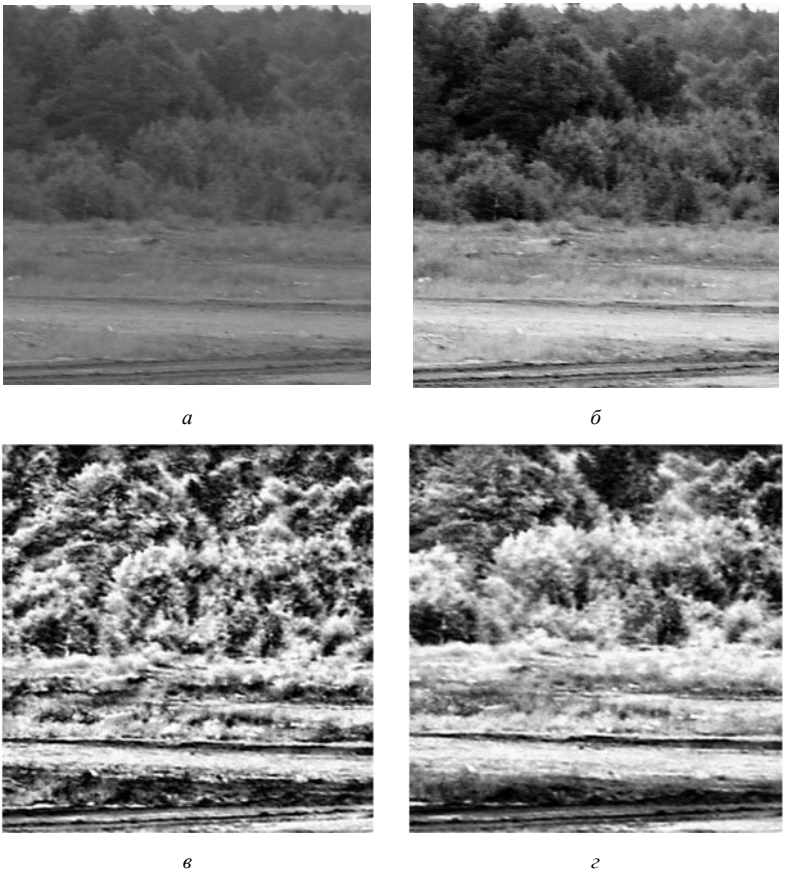
$$m = \begin{cases} \left[M \sum_{k=1}^{m} h(k) \right], m = 1, 2, ..., M - 1; \\ m = 0, \end{cases}$$

где m — квантованное значение преобразуемого сигнала; $h(k)$ — гистограмма распределения его значений; M — число уровней квантования ($M = 256$); $k = 0, 1, \ldots, M - 1$; m — преобразованное значение.

Эквализацию можно производить по всему изображению или по фрагментно, причем фрагменты изображения могут перекрываться [2; 4]. По фрагментную эквализацию изображений называют скользящей (адаптивной) эквализацией.

Различия скользящего метода эквализации и степенного метода можно наблюдать на рис. 5 (рис. 5*а* — исходное изображение, рис. 5*б* — степенная эквализация, $p = 0{,}4$, рис. 5*в* — скользящая эквализация с размером сканирующей области в виде квадрата со стороной равной 20 и $p = 0{,}4$, рис. 5*г* — скользящая эквализация с размером сканирующей области в виде квадрата со стороной равной 50 и $p = 0{,}4$) [2; 4]. Важным отличием процедуры скользящей эквализации от других видов эквализации заключается в задании различных размеров окна сканирования изображения.

Данное отличие позволяет выбирать определенную зону исследования изображения для выявления малозаметных объектов, т. е. адаптировать область эквализации в скользящем режиме в зависимости от распределения контрастности исходного изображения.



а *б*

в *г*

Рис. 5. Результат применения различных методов эквализации изображений

Заключение. Предложенные методы эквализации направлены на первичное исправление дефектов контраста изображений в условиях широкого изменения параметров внешней среды. Скользящий режим эквализации позволяет выявить пространственную неоднородность изображения, что способствует идентифицировать объекты ранее малозаметные человеческому глазу. Комплексное применение методов эквализации позволяет получить высокое качество формируемых изображений в системах охранного телевидения в условиях широкого изменения параметров внешней среды.

Библиографический список

1. *Журавель И. М.* Краткий курс теории обработки изображений. URL: https://hub.exponenta.ru/post/kratkiy-kurs-teorii-obrabotki-izobrazheniy734#72.

2. *Линдли К.* Практическая обработка изображений на языке СИ: пер. с англ. М.: Мир, 1996.

3. *Тельный А. В.* Инженерно-техническая защита информации. Системы охранного телевидения: учеб. пособие. Владимир: Изд-во ВлГУ, 2013.

4. *Яне Б.* Цифровая обработка изображений. М.: Техносфера, 2007.

5. *Ярославский Л. П.* Введение в цифровую обработку изображений. М.: Сов. радио, 1979.

А. В. Портнов, Н. С. Прытков, С. С. Лысов, А. Н. Рагозин
Южно-Уральский государственный университет — НИУ, г. Челябинск

Применение двумерной цифровой фильтрации для повышения информативности время-частотного представления звуковых сигналов в системах распознавания речи

Аннотация. Рассмотрено применение двумерных цифровых фильтров в задачах цифровой обработки время-частотных представлений звуковых сигналов в системах распознавания речи. Показана возможность повышения информативности время-частотного представления звукового сигнала и качества распознающих биометрических систем.

Ключевые слова: двумерный цифровой фильтр; время-частотное представление; звуковой сигнал.

Введение. Распознавание речи в настоящее время — технология, которая развивается быстрыми темпами. Главными критериями эффективности распознавания речи являются быстродействие и точность. Повысить эффективность обработки звукового сигнала возможно применением процедуры цифровой фильтрации. Пороговое отсечение малоинформативной части спектра звукового сигнала позволяет уменьшить время обработки сигнала, при этом увеличивая отношение сигнал/шум. Существует множество способов фильтрации звуковых сигналов, которые имеют разные характеристики по точности и скорости выполнения операций.

Метод формирования время-частотного распределения звукового сигнала. На рис. 1 изображен пример речевого сигнала. Время-частотное представление (ВЧП) сигнала содержит избыточную информацию[1]. В данном случае применяя фильтрацию можно удалить излишнюю детализацию практически без потерь в точности измерения. ВЧП

[1] *Цифровая* обработка сигналов: учеб. пособие / Ю. Н. Матвеев, К. К. Симончик, А. Ю. Тропченко, М. В. Хитров. СПб.: СПбНИУ ИТМО, 2013.

сигнала представляет собой поверхность, где по оси абсцисс располагается время, а по оси ординат — частота, высота точки поверхности (ось z) — уровень спектра звукового сигнала.

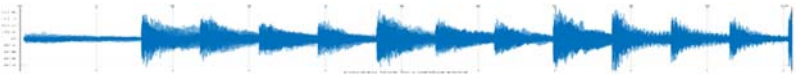


Рис. 1. Звуковой сигнал

Вид ВЧП звукового сигнала представлен на рис. 2.

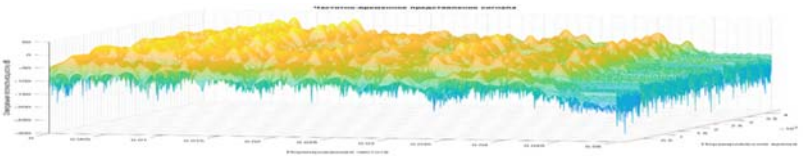


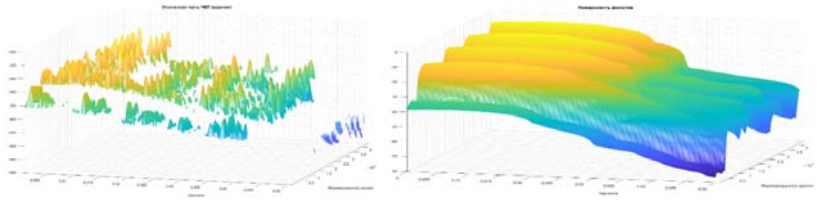
Рис. 2. ВЧП сигнала

Для выделения информативной части ВЧП сигнала используется два типа двумерных цифровых фильтров:

— усредняющий фильтр (average);

— дисковый фильтр (disk).

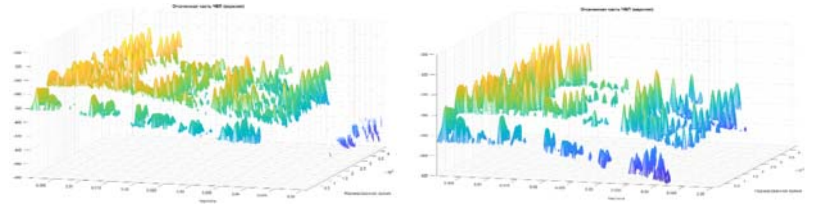
Двумерный сигнал в виде ВЧП подвергается двумерной цифровой фильтрации с использованием двумерных усредняющего и дискового цифровых фильтров, результат фильтрации изображен в виде поверхностей (отфильтрованных ВЧП), соответственно на рис. 3*а* и 3*б*.



а — усредняющего *б* — дискового

Рис. 3. ВЧП на выходе фильтров

На рис. 4*а* и 4*б* приведены изображения ВЧП в виде частей поверхности, превышающих по уровню отфильтрованные поверхности ВЧП рис. 3*а* и 3*б* соответственно.



а — усредняющего

б — дискового

Рис. 4. ВЧП, прошедшие пороговую обработку с помощью фильтра

Далее будет рассматриваться дисковый фильтр с различными значениями порядков. На рис. 5, 6 изображены виды сверху на поверхность ВЧП (см. рис. 4*б*), рассчитанных с использованием двумерных цифровых дисковых фильтров с различными величинами порядков фильтров.

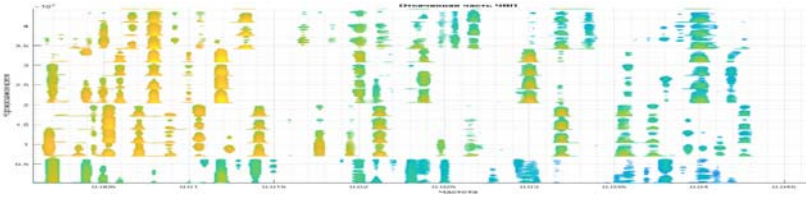


Рис. 5. Выделенная часть поверхности ВЧП
с помощью дискового фильтра (порядок 90)

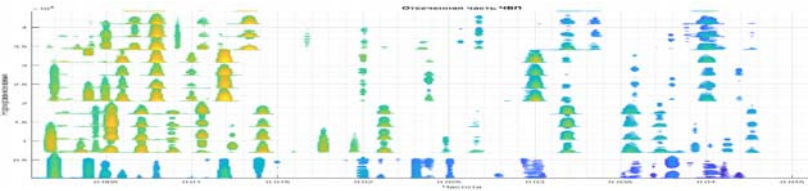


Рис. 6. Выделенная часть поверхности ВЧП
с помощью дискового фильтра (порядок 180)

Из анализа рис. 5, 6 можно сделать вывод, что применение двумерной цифровой фильтрации позволяет управлять детализацией отображения ВЧП звукового сигнала, что определяет качество обработки речевых сигналов в распознающих биометрических системах.

Заключение. Используя представленный способ двумерной фильтрации ВЧП звукового сигнала можно существенно повысить скорость и точность при реализации процедуры распознавании речи в биометрических системах.

С. Д. Субботин, Д. Н. Волчков, А. А. Забокрицкий
Уральский федеральный университет имени первого Президента России Б. Н. Ельцина, г. Екатеринбург

Обоснование актуальности разработки тестовой программы для специальных исследований интерфейса DisplayPort

Аннотация. В статье анализируются пути повышения эффективности проведения специальных исследований интерфейса DisplayPort на основе изучения характеристик для дальнейшей разработки тестовых программ. Рассмотрена возможность перехвата побочных электромагнитных излучений данного интерфейса, проведен поиск информативных сигналов от интерфейса и исследовано их затухание на различных расстояниях. Амплитудные и временные параметры информативного сигнала от интерфейса DisplayPort проанализированы в осциллографическом режиме. Обоснована актуальность разработки специальных программ.

Ключевые слова: DisplayPort; побочные электромагнитные излучения; технический канал утечки информации; специальные исследования; информативные сигналы; электрические сигналы; защита информации.

DisplayPort является современным интерфейсом для подключения мониторов и другой мультимедийной техники. Данные устройства могут участвовать в обработке информации ограниченного доступа.

В связи с этим возможность наличия технического канала утечки информации (далее — ТКУИ) за счет побочных электромагнитных излучений, возникающих при прохождении сигнала через данный интерфейс, является актуальной проблемой[1]. Для поиска информативных сигналов был собран лабораторный стенд, состоящий из ноутбука MSI GP73 LEOPARD 8RE (далее — ноутбук) и монитора Asus TUF Gaming VG259Q (далее — монитор), соединенных кабелем Ugreen Mini

[1] *Кондратьев А. В.* Техническая защита информации. Практика работ по оценке основных каналов утечки. М.: Горячая линия — Телеком, 2016.

DisplayPort — DisplayPort, версии 1.2[1]. Исследование характеристик излучений интерфейса DisplayPort осуществлялось с помощью поверенных специальных средств измерения внесенных в Государственный реестр средств измерений:

— анализатор спектра «Rohde&Schwarz FSV13»;

— антенна магнитная активная «АМА-30»;

— антенна дипольная активная «АДА-9»;

— специальное программное обеспечение «СПО-Навигатор».

Для поиска информативных сигналов измерительные антенны располагались вблизи места подключения интерфейса к монитору. Измерения проводились на каждой спектральной составляющей побочного электромагнитного излучения по магнитной составляющей в диапазоне 0,009…30 МГц и по электрической составляющей в диапазоне от 0,009…2000 МГц.

Напряженность электромагнитного поля измерялась вблизи интерфейса в два этапа. На первом — был измерен индустриальный шум при выключенных ноутбуке и мониторе. На втором — измерялась совокупность «сигнал + шум» в режиме передачи информации с ноутбука на экран монитора. В качестве тест-сигналов использовалось включение/выключение монитора от сети.

Наиболее сильный на фоне шума сигнал был обнаружен на частоте 172,79 МГц. Измеренные на данной частоте уровень шума и напряженности информативного сигнала составили 26,62 дБ (мкВ/м) и 47,03 дБ (мкВ/м) соответственно (рис. 1).

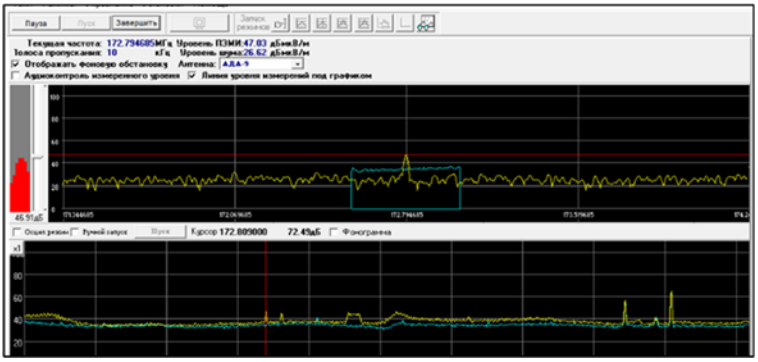


Рис. 1. Спектр информативного сигнала вблизи ПЭВМ

[1] *VESA* DisplayPort Standard Version 1, Revision 2. Github.com. URL: https://glenwing.github.io/docs/DP-1.2.pdf.

Оценивая опасность выявленного сигнала, провели измерения его характеристик на 1 метре от стенда (рис. 2).

Рис. 2. Измерение информативного сигнала
на расстоянии 1 м от монитора

В данных условиях сигнал был обнаружен. Измеренные уровни шума и напряженности информативного сигнала составили 20,37 дБ (мкВ/м) и 30,33 дБ (мкВ/м) соответственно (рис. 3).

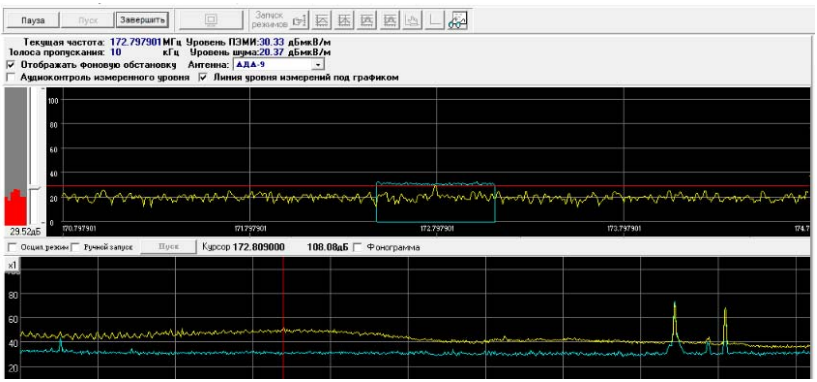


Рис. 3. Спектр информативного сигнала на расстоянии 1 м от монитора

Полученные данные свидетельствуют об опасности возникновения ТКУИ за счет побочных электромагнитных излучений при использовании интерфейса DisplayPort.

Отсутствие специальных тестов затрудняют поиск и исследование характеристик информативных сигналов.

Таким образом, актуальной задачей является разработка специальных тестов для качественного и эффективного исследования интерфейса Display-Port.

Д. В. Толстокорый, А. М. Жигарев, Р. Д. Колмогоров
Уральский государственный экономический университет, г. Екатеринбург

Анализ информационной безопасности систем видеоконференций и их сравнение

Аннотация. Рассмотрены востребованные на сегодняшний день системы видеоконференций. Проведен анализ достоинств и недостатков информационной безопасности данных решений.

Ключевые слова: анализ; видеоконференция; информационная безопасность; сравнение.

Введение. В последние месяцы сервисы групповых видеочатов, или, как их принято называть в деловом мире, видеоконференций, испытывают взрывной рост интереса пользователей. Ограничения, связанные с пандемией коронавирусной болезни, вынудили компании искать новые возможности удаленных коммуникаций между сотрудниками. И если ранее видеосовещания свидетельствовали о высоком технологическом уровне организации, то теперь использование Zoom, Cisco Webex, Slack или других решений стало насущной необходимостью. Распространение современных технологий видеосвязи не ограничивается коммерческими компаниями — их используют школы, бюджетные и государственные учреждения, спортивные клубы и досуговые центры. Из-за карантина частные лица также стали чаще прибегать к видеообщению вместо реальных встреч.

Однако возросшая популярность решений, обладающих функциями групповой видеосвязи, выявила ряд проблем, связанных с безопасностью подобного рода коммуникаций. Их можно условно разделить на четыре группы:

— неумение программ безопасно передавать конфиденциальные данные — использовать защищенные каналы и шифрование трафика;

— отсутствие защиты от несанкционированного подключения к беседе — так называемый «зумбомбинга», действий хулиганского характера, направленных на срыв видеоконференции;

— наличие в программах известных уязвимостей, которые могут эксплуатироваться злоумышленниками в кибератаках;

— нехватка правил хранения и использования накопленных персональных данных, отсутствие у пользователей возможности управлять хранением этой информации, другие недостатки политики конфиденциальности.

На основании этих критериев мы проанализировали десять решений для видеоконференций. Часть из них (Cisco Webex, Slack) ориентирована в первую очередь на бизнес-сегмент, другие, напротив, предназначены для пользовательских видеочатов (FaceTime, WhatsApp). Однако эти границы постепенно стираются: Zoom применяют и для корпоративных совещаний, и для дружеских бесед, а Google и Microsoft изменили стратегию продвижения своих разработок так, чтобы заинтересовать не только компании, но и частных пользователей.

Сквозное шифрование. Технология сквозного шифрования надежно защищает передаваемую информацию от кражи, поскольку декодирование пакетов данных происходит только на клиентском устройстве. Она скрывает данные видеочатов не только от злоумышленников, но и от государственных ведомств и самих разработчиков решения.

В отличие от обычных видеозвонков, реализация сквозного шифрования в многопользовательских видеочатах сопряжена с рядом сложностей. Возможно, именно поэтому далеко не все создатели представленных в обзоре систем реализовали ее в своих разработках. Шифрование по принципу «end-to-end» поддерживают Cisco Webex Meetings, GoToMeeting, FaceTime и WhatsApp, а создатели Zoom и Messenger Rooms планируют включить эту функциональность в будущие версии продуктов. Остальные разработчики пока ограничиваются шифрованием информации при передаче и использованием защищенных каналов связи.

Защита от несанкционированного доступа к конференциям. Использование групповых видеозвонков в бизнесе заставило внимательнее взглянуть на вопросы недопущения сторонних пользователей к беседам. Проблема не имеет единого простого решения, поскольку создателям приложений приходится искать баланс между возможностью подключения к чату внешних незарегистрированных пользователей по ссылке и борьбой с нелегитимным доступом, хулиганскими или мошенническими действиями в отношении участников беседы.

Каждый вендор выбрал свой путь. Например, в Messenger Rooms разработчики отказались от паролей на конференции, однако предоставили администраторам видеочатов большой выбор настроек доступа и вариантов видимости. Zoom, Microsoft Teams, Google Meet, Webinar Meetings и Cisco Webex Meetings имеют специальные «комнаты ожидания» для премодерации доступа к беседе. Slack жестко ограничивает возможность подключения к конференции пользователей вне рабочей

группы или корпоративного домена, WhatsApp и FaceTime ориентированы в первую очередь на общение в пределах адресной книги пользователя. В решении GoToMeeting «комнаты ожидания» присутствуют только в конференциях, которые закрыты при помощи функции MeetingLock.

Двухфакторная аутентификация. В той же плоскости лежит и вопрос применения надежных методов аутентификации пользователей. Двухфакторная, или, точнее, многофакторная аутентификация позволяет не допустить несанкционированного доступа к видеоконференции через взлом аккаунта одного из участников.

Из рассмотренных нами решений двухфакторная аутентификация отсутствует только в Zoom, однако в ряде разработок (Google Meet, FaceTime) она выполнена как функция связанной с продуктом экосистемы, а не как часть самого приложения. В этом случае, авторизовавшись в основном аккаунте, пользователь уже не проходит дополнительную проверку при входе в систему видеоконференций.

Прочие факторы. Для корпоративных и частных пользователей некоторые факторы безопасности решений для видеоконференций будут иметь разный вес. Поэтому при выборе продукта для использования в бизнесе, возможно, стоит обратить большее внимание на работу вендора с выявленными уязвимостями. Абсолютное количество найденных багов тоже имеет значение, однако для организаций важно понимать, насколько быстро и адекватно разработчики реагируют на проблемы. Для частных лиц этот вопрос также важен, однако им, возможно, интереснее будет знать, как создатели решения распоряжаются накопленными пользовательскими данными и можно ли самостоятельно управлять этой информацией.

В таблице приведены параметры, связанные с безопасностью приложений для видеоконференций.

Заключение. Разработчики продуктов для организации видеоконференций уделяют значительное внимание обеспечению безопасности своих решений, однако исповедуют разные подходы к этому вопросу. Выбор инструментов для защиты передаваемых данных и обеспечения конфиденциальности беседы зачастую зависит от сегмента рынка, на который ориентирован продукт. Приложения для общения нескольких частных пользователей уделяют большое внимание сквозному шифрованию данных, но не всегда обладают расширенными средствами контроля доступа. Системы, ориентированные на корпоративный сегмент, напротив, чаще всего имеют «комнаты ожидания», а также возможность премодерирования доступа к конференции. При этом сквозное шифрование часто заявлено как опция или реализовано с ограничениями.

Сравнение приложений для видеоконференций

Название решения	Сквозное шифрование данных	Двухфакторная аутентификация	Наличие комнаты ожидания	Возможность управления персональными данными на стороне клиента	Возможность управления персональными данными на сервере	Количество известных уязвимостей в 2019–2020 гг.
Cisco Webex Meetings	Да	Да	Да	Да	Нет	11
Google Meet	Нет	Да	Да	Да	Да	0
GoToMeeting	Да	Да	В рамках функции MeetingLock	Да	Нет	0
FaceTime	Да	В рамках IOS	Нет	Да	Да	4
Messenger Rooms	Нет	В рамках Facebook	Нет	Да	Да	0
Microsoft Teams	Нет	Да	Да	Да	Да	1
Slack	Нет	Да	Нет	Нет	Нет	6
Webinar Meetings	Нет	Нет	Да	Да	Да	0
WhatsApp	Да	Да	Нет	Да	Да	8
Zoom	Нет	Нет	Да	Да	Нет	14

Выбирая систему для видеоконференций, разумно определить, какие критерии безопасности являются для вас наиболее значимыми, а какими можно пренебречь. Сведения, собранные нами в этом материале, могут стать отправной точкой для понимания основных аспектов безопасности применительно к подобным продуктам.

Д. Э. Цибулис, А. Н. Рагозин
Южно-Уральский государственный университет — НИУ, г. Челябинск

Анализ информационных сигналов с использованием генеративно-состязательных нейронных сетей

Аннотация. Рассмотрены возможности генеративно-состязательных нейронных сетей при обработке цифровых изображений.
Ключевые слова: генеративно-состязательная нейронная сеть; цифровое изображение; информационный сигнал.

Введение. Информационный сигнал отражает физические процессы, протекающие в информационных системах. Анализ информационных сигналов позволяет формировать решения относительно характера поведения процессов информационных систем. Например: отклонение от нормального режима функционирования может быть следствием вредоносных воздействий, направленных на информационную систему.

Процессы, протекающие в информационных системах и наблюдаемые в виде информационных сигналов представимы в виде цифровых изображений, например, с использованием различных время-частотных преобразований, таких как: кратковременное преобразование Фурье, вейвлет преобразование. Обработку, таких изображений можно провести при помощи генеративно-состязательной нейронной сети, что позволит сформировать высоко-информативные признаки для принятия решений относительно характера поведения процессов, протекающих в информационных системах.

Структура генеративно-состязательной сети. Генеративно-состязательные сети — модель в области машинного обучения, умеющая имитировать заданное распределение данных. Такая модель состоит из двух нейронных сетей: генератора (Г) и дискриминатора (Д). Генератор формирует объекты из скрытого пространства признаков, а дискриминатор, обученный на реальных объектах, стремится найти отличия между настоящим и сгенерированным объектом. Структура генеративно-состязательной сети изображена на рис. 1.

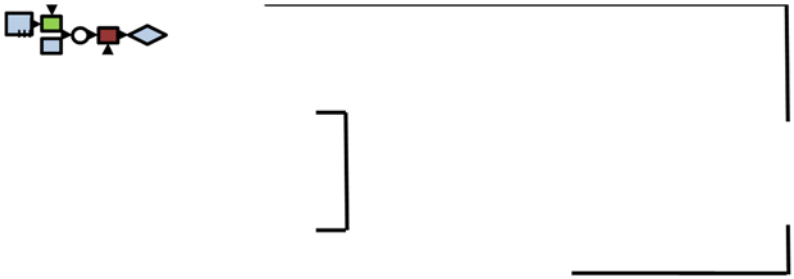


Рис. 1. Структура генеративно-состязательной сети

Генератор формирует объекты из скрытого пространства признаков, а дискриминатор, обученный на реальных объектах, стремится найти расхождения между настоящим и сгенерированным объектом. В математическом описании дискриминатор формирует на выходе вероятность того, что некий образ x относится к классу y: $p(y|x)$. Генератор формирует вероятность появления в классе y образа x: $p(x|y)$. При этом, генератор пытается повысить процент ошибок дискриминатора, который в свою очередь, старается увеличить точность распознавания.

Как и в любой нейронной сети тренировка проводится путем вычисления функции потерь (функционала ошибки) и последующей его минимизации, например, методом градиентного спуска. Функционал ошибки для генеративно-состязательной можно описать выражением [1; 2]:

$$\min_G \max_D V(G,D) = E_{XP_g}\left[\log(D(x))\right] + E_{XP_n}\left[\log(1 - D(g(z)))\right]$$

Здесь:

— x — данные из обучающей выборки;

— z — некий шум, добавляемый к входным данным;

— p_g — распределение вероятностей того, что некий образ относится к классу x;

— p_n — распределение шумовой составляющей на входе;

— $G(\theta_z)$ — дифференцируемая функция, выполненная в виде многослойного персептрона с параметром θ_z, выполняющая функцию генератора;

— $D(x,\theta_d)$ — многослойный персептрон, выполняющий функцию дискриминатора;

— $\min_G \max_G V(G, D)$ — функционал ошибки совместной работы двух нейронных сетей, по-другому обозначаемый Loss-function или L.

Обработка цифровых изображений. Рассмотрим несколько практических применений генеративно-состязательных сетей. Для обзора возьмем технологии CycleGAN [3] и StackGAN [4].

Технология CycleGAN предполагает замену одних объектов на изображении на совершенно новые, не встречающиеся на исходном изображении. В отличие от традиционной архитектуры GAN данная структура преобразует следующий функционал ошибки:

$$L(F, G, D_X, D_Y) = L_{GAN}(G, D_X, X, Y) + L_{GAN}(F, D_X, Y, X) + \lambda L_{cyc}(G, F)$$

То есть общая функция потерь состоит из трех частей:

— $L_{GAN}(G, D_X, X, Y)$ — функция потерь при тренировке генеративно-состязательной модели, обучающейся создавать образы X неотличимые от Y;

— $L_{GAN}(F, D_X, Y, X)$ — функция потерь при тренировке генеративно-состязательной модели, обучающейся создавать образы Y неотличимые от X;

— $\lambda L_{cyc}(G, F)$ — функция потерь с неким гиперпараметром λ, который отвечает за корректировку работы генераторов G и F.

Благодаря тому, что данная структура обучается генерировать объекты как в прямом, так и в обратном направлениях, получается заменять одни предметы на изображении совершенно новыми. На рис. 2 представлен пример работы такой нейронной сети.

Технология StackGAN позволяет сгенерировать изображение по заданному тексту. Структура такой сети состоит из двух компонентов: Stage-I GAN и Stage-II GAN. Сеть Stage-I GAN на основе заданного текста определяет базовые формы и цвета, которые необходимо применять, а также создает фон изображения используя скрытое пространство признаков. На выходе этой сети получается картинка с низким разрешением. Сеть Stage-II GAN занимается корректировкой изображения низкого разрешения, по деталям, которые она находит в тексте. Результат работы сети — это картинка с высоким разрешением.

Результат работы сети StackGan представлен на рис. 3.

Информационные сигналы, наблюдаемые в различных системах, представимы в виде цифровых изображений, например, с использованием различных время-частотных преобразований (кратковременное преобразование Фурье, вейвлет преобразование), что позволяет для обработки сигналов и выделения высокоинформативных признаков применять генеративно-состязательные нейронные сети, что видно из рассмотренных примеров.

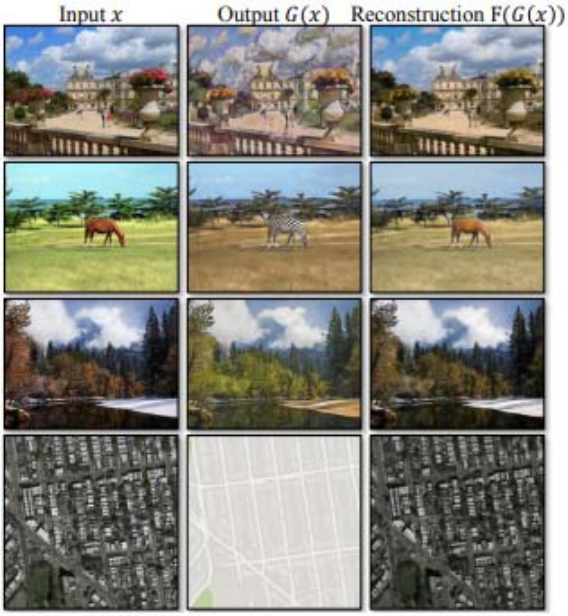


Рис. 2. Результаты работы технологии CycleGAN[1]

Рис. 3. Результат работы технологии StackGA[2]

[1] *Cornell* University arXiv.org. URL: https://arxiv.org/pdf/1703.10593.pdf.
[2] *Cornell* University arXiv.org. URL: https://arxiv.org/pdf/1612.03242.pdf.

Библиографический список

1. *Brownlee J.* Generative Adversarial Networks. URL: https://id-lab.ru/posts/developers/vvedenie-v-generativno-sostyazatelnye-seti-gan-genereative-adversarial-networks.

2. *Goodfellow I. J., Pouget-Abadie J., Mirza M., Xu B., Warde-Farley D., Ozair S., Courville A., Bengio Y.* General Adversarial Nets. URL: https://papers.nips.cc/paper/2014/file/5ca3e9b122f61f8f06494c97b1afccf3-Paper.pdf.

3. *Zhu J. Y., Park T., Isola P., Efros A. A.* Unpaired Image-to-Image Translation using Cycle-Consistent Adversarial Net-works / UC Berkeley, in ICCV. 2017. URL: https://junyanz.github.io/CycleGAN.

4. *Zhang H., Xu T., Li H., Zhang S., Wang X., Huang X., Metaxas D.* Stack-GAN: Text to Photo-realistic Image Synthesis with Stacked Generative Ad-versarial Networks. URL https://arxiv.org/pdf/1612.03242.pdf.

Э. А. Аванесян, Е. В. Радковская
Уральский государственный экономический университет, г. Екатеринбург

Моделирование развития малого и среднего предпринимательства как фактор экономической и информационной безопасности региона

Аннотация. Процесс математического моделирования рассматривается как один из факторов обеспечения экономической и информационной безопасности региона. Анализируются модели зависимости развития малого и среднего предпринимательства от различных показателей, построенные на основе статистических данных временных рядов для Свердловской области.

Ключевые слова: малое и среднее предпринимательство; регион; развитие; модель; временной ряд.

Одним из условий успешного, устойчивого развития региона, по мнению многих экономистов, является развитие малого и среднего предпринимательства. Малые и средние предприятия, как частных, так и смешанных форм собственности, не только предоставляют жителям различные товары и услуги и формируют рабочие места, но и в целом вносят довольно значительный вклад в развитие экономики региона. Более того, являясь одним из элементов обеспечения диверсификации регионального производства, к тому же — часто независимого от бюджетного финансирования и в целом государственного вмешательства, предприятия малого и среднего бизнеса образуют одну из граней каркаса экономической безопасности региона.

Безопасное в информационном плане развитие региона, безусловно, включает в себя и такой аспект, как использование обоснованных с математической точки зрения информационно-статистических моделей при разработке стратегий регионального развития [1]. В связи с этим корректная оценка уровня развития малого и среднего предпринимательства, а также разработка релевантной модели его прогнозирования, становится в настоящее время весьма важной задачей. Реализация мероприятий общерегионального экономического развития невозможна без опоры на актуальные модели и прогнозы, отражающие реальную ситуацию и отвечающие требованиям информационной безопасности — построенные по реальным статистическим данным, на основе апробированных математических методов и удовлетворяющие предпосылкам применения и признакам качественных моделей.

Одним из возможных видов экономико-математических моделей, описывающем зависимость уровня развития малого и среднего предпринимательства от различных факторов, является эконометрическая модель [2].

В качестве результирующей, зависимой, переменной в данном случае целесообразнее всего выбрать общее число малых и средних предприятий (МСП). На основе статистических данных по Свердловской области за 10 лет (2009–2018 гг.) на начальном этапе была предпринята попытка построить модель зависимости числа МСП от таких факторов как индекс бюджетных расходов; ВРП; индекс физического объема инвестиций в основной капитал; уровень безработицы в регионе; доля городского населения; затраты, направленные на развитие информационно-коммуникационных технологий; индекс производства и распределения электроэнергии, газа и воды; количество высших учебных заведений в регионе; плотность автомобильных дорог в регионе. Однако результаты выполнения корреляционного и регрессионного анализа не позволили сформировать качественную модель множественной связи в связи с незначимостью коэффициентов регрессии анализируемых факторов, несмотря на высокие значения коэффициентов парной и множественной корреляции.

Специфика статистических данных, представляющих собой временные ряды, позволила применить подход исследования данных, освобожденных от трендовых компонент. Результат пятого этапа исследования — после исключения трендовых компонент и факторов, не оказывающих влияние на зависимую переменную МСП, представлен на рис. 1.

ВЫВОД ИТОГОВ

Регрессионная статистика	
Множественный R	0,811440234
R-квадрат	0,658435254
Нормированный R-квадрат	0,560845326
Стандартная ошибка	7095,752753
Наблюдения	10

Дисперсионный анализ

	df	*SS*	*MS*	*F*	*Значимость F*
Регрессия	2	679414833,6	339707416,8	6,746959141	0,023289257
Остаток	7	352447950	50349707,14		
Итого	9	1031862784			

	Коэффициенты	*Стандартная ошибка*	*t-статистика*	*P-Значение*	*Нижние 95%*	*Верхние 95%*
Y-пересечение	-64847733,97	13062995,55	-4,964231498	0,001629774	-95736810,05	-33958657,89
Доля городского населения	-206437,6869	67865,4448	-3,041867441	0,018797373	-366913,9636	-45961,41031
Количество высших учебных заведений в регионе	4109,616463	1449,925592	2,834363698	0,025247737	681,0872447	7538,145681

Рис. 1. Результаты регрессионного анализа по данным временных рядов с исключенной трендовой компонентой

Таким образом, для Свердловской области факторами, влияющими на число малых и средних предприятий, оказываются доля городского населения и количество высших учебных заведений в регионе. При этом, если со вторым фактором связь результирующего показателя является прямой, то с первым — обратной, что объясняется, вероятно, значительной долей малых и средних предприятий, специализирующихся на внегородской деятельности — логистических, сельскохозяйственных и т.п.

Дополнительная проверка, заключающаяся в анализе первых разностей временных рядов, что позволяет говорить о зависимости между показателями без влияния временного фактора, подтверждает ранее сделанные выводы. Результат последнего этапа регрессионного анализа, проведенного по первым разностям и представляющего собой модель с удаленными незначимыми факторами, представлен на рис. 2.

ВЫВОД ИТОГОВ

Регрессионная статистика	
Множественный R	0,800171748
R-квадрат	0,640274826
Нормированный R-квадрат	0,520366434
Стандартная ошибка	12366,02488
Наблюдения	9

Дисперсионный анализ

	df	*SS*	*MS*	*F*	*Значимость F*
Регрессия	2	1633078560	816539280	5,339699898	0,046549229
Остаток	6	917511428,2	152918571,4		
Итого	8	2550589988			

	Коэффициенты	*Стандартная ошибка*	*t-статистика*	*P-Значение*	*Нижние 95%*	*Верхние 95%*
Y-пересечение	47697,28843	14343,64615	3,325325229	0,015898767	12599,65067	82794,92619
Доля городского населения	-242286,753	96144,59101	-2,520024793	0,045285579	-477544,0922	-7029,413865
Количество высших учебных заведений в регионе	6410,186528	2180,35438	2,939974614	0,025948505	1075,051556	11745,3215

Рис. 2. Результаты регрессионного анализа по первым разностям

Полученные в результате параметры уравнения трактуются как величины изменения прироста результирующей переменной МСП при единичном приросте влияющих факторных переменных.

Необходимо отметить, что полученные в ходе проведенного анализа результаты целесообразно рассматривать как промежуточные. Добавление в исходный набор независимых переменных дополнительных факторов, которые по результатам предварительного маркетингового изучения могут оказывать реальное и значимое влияние на уровень развития малого и среднего предпринимательства, вероятнее всего, расширит и углубит экономическую картину искомой зависимости, а увеличение выборки повысит достоверность модели.

Представленные модели также могут быть конкретизированы для отдельных территорий, входящих в состав Свердловской области.

Реальное прогнозирование и рекомендации по отдельным статьям развития, безусловно, стоит выполнять на основе уточненных для территорий статистических данных.

Однако верно и обратное: укрупнение блоков данных для проведения анализа позволит сделать выводы для более крупных административно-территориальных единиц, которые, несмотря на неизбежную усредненность, дадут более глобальную картину.

Применение подобных моделей может быть весьма полезно при сравнительном анализе по отраслям и сферам развития.

Библиографический список

1. *Бегичева С. В.* Применение дискретно-событийного моделирования для логистического планирования // Менеджмент и предпринимательство в парадигме устойчивого развития: материалы II Междунар. науч.-практ. конф. (Екатеринбург, 23 мая 2019 г.). Екатеринбург: Изд-во УрГЭУ, 2019. С. 53–56.

2. *Радковская Е. В., Кочкина Е. М., Дроботун М. В., Фер Т. В., Попова Н. П., Иванов И. В.* Эконометрика. Роли (Северная Каролина): Open Science Publishing, 2019.

И. И. Баранкова, А. В. Дегтярева
Магнитогорский государственный технический университет им. Г. И. Носова,
г. Магнитогорск

Анализ методологий риск-менеджмента информационной безопасности

Аннотация. Одним из важнейших факторов грамотного выбора мер и средств обеспечения информационной безопасности выступает оценка и анализ рисков ИБ. От этого зависит релевантность построения защиты информации. В статье рассмотрены основные подходы к оценке рисков, выделены преимущества и недостатки каждого подхода, проведен сравнительный анализ современных методик.

Ключевые слова: анализ рисков; информационная безопасность; качественный подход; количественный подход; оценка рисков.

С каждым годом количество атак на предприятия растет и это подталкивает компании уделять все больше внимания построению надежной защиты информации.

Чтобы организация могла создать надежную систему информационной безопасности и при этом избежать избыточных затрат, проводится оценка и анализ рисков информационной безопасности (ИБ).

В настоящее время существует два подхода к оценке рисков информационной безопасности: качественный и количественный[1]. Выбор подхода следует осуществлять индивидуально, исходя из нужд и возможностей компании. Сильные и слабые стороны каждого подхода приведены в табл. 1 и 2.

Таблица 1

Количественный подход

Достоинства	Недостатки
Получение конкретных значений объектов оценки риска	Требует больших временных затрат
Наличие численных оценок в отчетах для руководства повышает уровень доверия к отчетным документам	Требует большого количества исходных данных
	Не существует эффективного формализованного метода, позволяющего точно определить стоимости активов

Таблица 2

Качественный подход

Достоинства	Недостатки
Требует меньше временных затрат	Результаты имеют субъективный характер
Не требует большого количества исходных данных	Отсутствие наглядного понимания ущерба
Позволяет отказаться от сложных процедур определения точной стоимости актива, затрат на защитные меры, вероятности реализации угроз	

В современном мире существует множество методик оценки рисков, в рамках данной статьи проанализированы и сравнены между собой следующие методики:

— FRAP (Facilitated Risk Analysis Process)[2];

— Octave[3].

Методика FRAP описывает подход к качественной оценке рисков.

[1] *Шиляев С.* Методика оценки рисков информационной безопасности. URL: https://kontur.ru/ articles/1691.

[2] *Facilitated* risk analysis process (FRAP). URL: http://www.ittoday.info/AIMS/DSM/85-01-21.pdf.

[3] *Методология* OCTAVE для оценки информационных рисков. URL: http://www.risk24.ru/octave.htm.

Работу методики FRAP можно условно разделить на четыре этапа. 1-й этап — формирование команды (табл. 3).

Таблица 3

Формирование команды

Специалист	Ответственность
Бизнес-менеджер	Отвечают за информацию о ценности активов
Технический персонал	Отвечают за информацию о потенциальных уязвимостях системы
Член проектного офиса	Отвечают за то, чтобы члены команды общались эффективно и придерживались повестки дня
Специалист по информационной безопасности	

2-й этап — мозговой штурм. Цель данного этапа определить:

— потенциальные угрозы;

— вероятность реализации этих угроз.

Стоит отметить, что команда не пытается получить конкретные цифры, а полагается на свои знания и опыт.

3-й этап — определение мер защиты. На данном этапе выбираются меры, которые могут быть применены для снижения каждого из выявленных рисков информационной безопасности. Для удобства используются 26 типов мер защиты, определенных в методологии FRAP.

4-й этап — документирование проделанной работы и отправка отчета начальству.

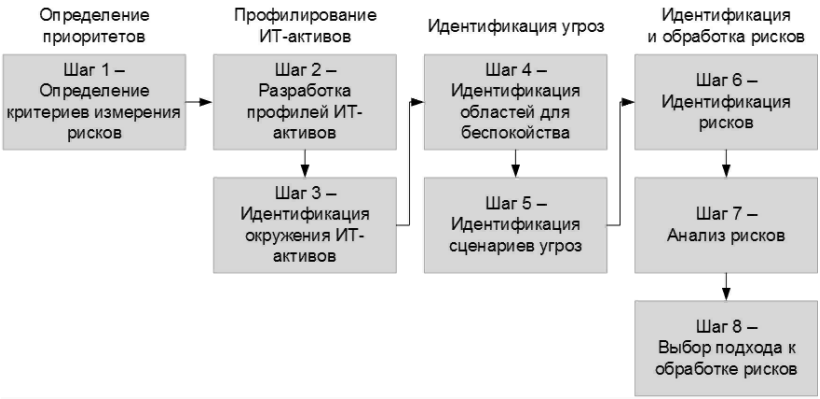
Методика FRAP наиболее распространена при качественной оценке рисков. Данную методику стоит выбирать компаниям, которым необходимо декомпозировать риски ИБ от наиболее критичных рисков верхнего уровня до рисков нижнего уровня. Метод позволят итерационно распространять процессы управления рисками на всю организацию.

Методика Octave описывает подход к количественной оценке рисков.

Для наглядности описания работы данной методики, была создана блок-схема, представленная на рисунке.

Методика Octave наиболее распространена при количественной оценке рисков. Данную методику стоит выбирать компаниям, которые впервые внедряют процесс управления рисками и не имеют достаточных ресурсов.

В рамках данной работы, была произведена упрощенная количественная оценка рисков для университета МГТУ им. Г. И. Носова, с учетом действующих СЗИ, она показала приемлемый уровень.



Методика Octave

Таким образом, каждая организация должна выбирать методику оценки рисков ИБ исходя из внутренних особенностей:

В современном мире существует множество методик оценки рисков, в рамках данной статьи проанализированы и сравнены между собой следующие методики:

— наличие временных, человеческих и финансовых ресурсов;

— особенности требований законодательства и регуляторов, применимых к деятельности организации.

Но однозначно, что каждая организация, заинтересованная в сохранении информации ограниченного доступа и финансовой прибыли, должна выбирать проактивный подход к обеспечению информационной безопасности и реагировать на инциденты с использованием рациональных методик.

М. В. Ведунова
Уральский государственный университет путей сообщения, г. Екатеринбург

О связи ортоморфизмов и преломляющих биекций с системами троек Штейнера

Аннотация. Проводится исследование преломляющих биекций систем троек Штейнера. Проверяется, могут ли преломляющие биекции быть ортоморфизмами для квазигрупп систем троек Штейнера при $v = 13$. Описана проблема, возникающая при работе с алгоритмами построения ортоморфизмов.

Ключевые слова: ортоморфизмы; преломляющие биекции; системы троек Штейнера.

Как известно, ортоморфизмы нашли широкое применение в криптографии, например, используются при построении блочных шифров, основывающихся на схемах Лая-Месси[1]. Схема Лая-Месси зависит от конечной группы G с нейтральным элементом e и ортоморфизмом G. В 2016 г. было изобретено устройство для построения ортоморфизмов, использующее парные разности, которое применяется при построении средств обработки и защиты информации, в том числе для обеспечения конфиденциальности, аутентичности и целостности информации при ее передаче, обработке и хранении в автоматизированных системах[2]. Также ортоморфизмы и полные подстановки могут применяться для построения систем ортогональных латинских квадратов [4; 5]. Известно, что системы троек Штейнера порождают квазигруппу на множестве элементов в такой системе [2]. Построенные преломляющие биекции в системах троек Штейнера являются подстановкой в квазигруппе Штейнера [1].

Прежде чем говорить о связи данных понятий, дадим определение каждому из них.

Понятие ортоморфизма впервые было опубликовано в 1961 г. учеными из Кембриджского университета [5].

Ортоморфизмом называется такое преобразование, которое при применении к квазигруппе дает квадрат, ортогональный исходному.

Под преломляющими биекциями понимаются отображения F квазигруппы в себя, удовлетворяющие условию $F(x \cdot y) \neq F(x) \cdot F(y)$ при любых $x \neq y$ [1].

Системой троек Штейнера называется система, на элементах которой построены тройки такие, что каждая пара из v элементов входит

[1] *Problem* 4. «Orthomorphisms». URL: https://nsucrypto.nsu.ru/archive/2020/round/2/task/4/#data.

[2] *Устройство* для построения ортоморфизмов, использующее парные разности. URL: https://patents.google.com/patent/RU2632119C1/ru.

в одну и только в одну тройку, где v — количество элементов, на которых построена система.

По определению, ортоморфизмом является преобразование, в результате применения которого получается квазигруппа, ортогональная исходной. Квазигруппы с таблицами Кэли $A = (a_{ij})$ и $B = (b_{ij})$ являются ортогональными, если все упорядоченные пары (a_{ij}, b_{ij}) различны[1]. В работе [3] определено, что подстановка h квазигруппы Q называется ее ортоморфизмом, если отображение f: $Q \to Q$, определенное формулой $f(x) = x - h(x)$, является подстановкой множества Q. Две квазигруппы Q_h и Q_g ортогональны тогда и только тогда, когда ортоморфизмом является отображение h-$1g$.

В работе [5] в качестве подстановок квазигруппы h выступали автоморфизмы. Под автоморфизмом понимается преобразование квазигруппы Q, отображающее квазигруппу Q на себя. В работе [3] был поставлен вопрос: существуют ли ортоморфизмы, не являющиеся автоморфизмами? Поскольку преломляющие биекции, отображающие квазигруппу Q таким образом, что $F(x \cdot y) \neq F(x) \cdot F(y)$ при любых $x \neq y$, не являются автоморфизмами, проверим для $v = 13$, может ли преломляющая биекция являться ортоморфизмом для квазигруппы Штейнера. Для проверки возьмем биекцию [4], в которой никакой элемент не преобразуется в себя:

$$g = \begin{pmatrix} 1\,2\,3 & 4\,5 & 6\,7\,8 & 9\,10\,11\,12\,13 \\ 8\,6\,10\,2\,11\,3\,11\,2\,4\,5 & 7 & 1\,3\,9 \end{pmatrix}$$

Результат применения преломляющей биекции к исходной квазигруппе приведен ниже (см. таблицу).

Поскольку в значениях столбца *«$x \cdot g(x)$»* есть повторения, то g не является ортоморфизмом квазигрупп Штейнера.

Тогда возникает естественный и важный вопрос: будут ли ортоморфизмами другие преломляющие биекции?

Для того, чтобы узнать ответ на данный вопрос, нужно также проверить все биекции. Возможно, среди них найдутся ортоморфизмы.

Для семейств троек Штейнера существует как минимум одна подстановка, являющаяся тождественным ортоморфизмом в тройках Штейнера — подстановка, при которой каждый элемент преобразуется в себя. Но такая подстановка не является преломляющей биекцией.

Для построения ортоморфизмов существуют алгоритмы, позволяющие автоматизировать данный процесс [5]. Единственная проблема,

[1] *Ортогональные* латинские квадраты. URL: https://ru.wikipedia.org.

которая возникает при работе — такие алгоритмы позволяют строить ортоморфизмы только на основе уже существующих. Поэтому открытой проблемой является автоматизация процесса построения ортоморфизмов без использования других ортоморфизмов.

Результат применения преломляющей биекции

x	$g(x)$	$x \cdot g(x)$
1	8	9
2	6	4
3	10	6
4	2	6
5	11	8
6	3	10
7	1	6
8	12	6
9	4	7
10	5	9
11	7	12
12	13	1
13	9	3

Таким образом, в данной работе было произведено исследование преломляющих биекций в тройках Штейнера.

Библиографический список

1. *Ведунова М. В., Геут К. Л., Игнатова А. О., Титов С. С.* Преломляющие биекции в тройках Штейнера // ПДМ. Приложение. 2020. № 13. С. 6–8.

2. *Ведунова М. В., Игнатова А. О., Титов С. С.* Задача блокировки троек Штейнера // Безопасность информационного пространства: сб. тр. XVII Всерос. науч.-практ. конф. студентов, аспирантов и молодых ученых (Челябинск, 29-30 ноября 2018 г.): в 2 т. Челябинск: ЧелГУ, 2018. Т. 1. С. 50–55.

3. *Глухов М. М.* О методах построения систем ортогональных квазигрупп с использованием групп // Математические вопросы криптографии. 2011. Т. 2, вып. 4. С. 5–24.

4. *Глухов М. М.* О применениях квазигрупп в криптографии // Прикладная дискретная математика. 2008. № 2(2). С. 28–32.

5. *Johnson D., Dulmage A., Mendelsohn N.* Orthomorphisms of Groups and Orthogonal Latin Squares. I // Canadian Journal of Mathematics. 1961. Vol. 13. P. 356—372.

К. Л. Геут, С. С. Титов
Уральский государственный университет путей сообщения, г. Екатеринбург

Ортоморфизмы и полные подстановки квазигрупп в криптографии и теории кодирования

Аннотация. Работа посвящена решению задачи международной олимпиады по криптографии. Последовательно строятся конструкции базисов векторного пространства двоичных векторов, содержащие все возможные покомпонентные произведения заданных параметров.

Ключевые слова: NSUCRYPTO; ортоморфизмы; базис векторного пространства; код Рида — Маллера.

На международной олимпиаде по криптографии NSUCRYPTO-2020[1] были две идейно похожие задачи. Проблема 4 была посвящена описанию ортоморфизмов, а проблема 9 — составлению базисов. Остановимся на второй задаче.

Рассмотрим векторное пространство F_2^r, состоящее из всех двоичных векторов длины r. Для любых d векторов определяется покомпонентное произведение этих векторов. Пустое произведение (когда в нем нет элемента) равно вектору всех единиц. Пусть B-базис векторного пространства F_2^r и пусть $\subseteq F_2^r$ — семейство s двоичных векторов, такое, что все возможные покомпонентные произведения до d векторов из семейства F (включая пустое произведение) образуют базис B.

Поскольку покомпонентное произведение этих векторов (определенных в условии задачи) должно быть ненулевым для того, чтобы быть вектором в базисе, и они должны быть разными, мы можем идентифицировать эти векторы как некоторые r строк в таблице истинности (табл. 1) некоторой булевой функции f, зависящей от s аргументов t^1, ..., t^s до степени d (может быть, после некоторой перестановки аргументов и значений) [1].

Таблица истинности, представляет собой расширенную матрицу системы линейных уравнений над $GF(2)$ с матрицей B и правым столбцом f. Вот почему мы получаем базис тогда и только тогда, когда существует биекция между всеми булевыми функциями f, зависящими от s аргументов t^1, ..., t^s (табл. 1) до степени d, и всем списком значений f_1, ..., f_r, на этих булевых векторах значений аргументов x^1, ..., x^s.

Для $s = d$ мы имеем $r = 2^s$ и единственное семейство всех векторов булевых векторов значений аргументов (может быть, после некоторой перестановки аргументов и значений). Искомая биекция гарантируется

[1] *International* Olympiad in Cryptography NSUCRYPTO. URL: https://nsucrypto.nsu.ru.

теоремой о АНФ (алгебраической нормальной форме, т.е. о многочлене Жегалкина).

Таблица 1

Таблица истинности

1	t^1	…	t^s	t^1t^2	…	t^1t^s	…	$t^1\ldots t^d$	…	…	f
1	…	…	…	…	…	…	…	…	…	…	…
1	x_1^1	…	x_1^s	…	…	$x_1^1 \cdot x_1^s$	…	…	…	…	f^1
…	…	…	…	…	…	…	…	…	…	…	…
1	x_r^1		x_r^s	…	…	$x_r^1 \cdot x_1^s$	…	…	…	…	f^r
…	…	…	…	…	…	…	…	…	…	…	…
…	…	…	…	…	…	…	…	…	…	…	…

Конструкция 1. Мы можем предложить некоторую конструкцию для таких базисов B с таким семейством F для всех $s > d > 1$.

Определим семейство F как набор всех строк i в таблице истинности при следующем условии: слово-вектор x_i^1, ..., x_i^s имеет вес Хэмминга, не превосходящий d.

Очевидно, что значения коэффициентов функции f определяются рекуррентно, как и в доказательстве теоремы об АНФ: коэффициент перед композицией для подмножества T (мощности не превышающей d) во множестве $\{t^1, ..., t^s\}$ аргументов определяется как сумма значений f и значений коэффициентов для всего подмножества $R \subset T$.

Утверждение 1. *Для каждого $s \geq d > 1$ существует базис, для которого существует такое семейство. Конструкция базисов описана выше.*

Для описания конкретного базиса мы можем сформировать его (без потери общности и может быть после некоторой перестановки аргументов и значений) в виде матрицы B размера $r \times r$, имеющей верхнюю строку (1, ..., 1) с номером 0, строки с номером $i = 1, ..., s$ — это векторы x^i и далее (в некотором порядке) строки для покомпонентных произведений этих векторов (вплоть до d векторов из строк с номером $i = 1, ..., s$). После некоторой перестановки столбцов можно предположить, что столбцы строк с номером $i = 1, ..., s$ упорядочены естественным порядком.

Например, в условии задачи мы имеем табл. 2 с первым вектором семейства в строке t^1 и очевидной перестановкой столбцов. Если порядок фиксирован, то базисы уникальны для $s = 2$, $d = 2$.

Таблица 2

Таблица по условиям задачи

	0	1	2	3
1 =	1	1	1	1
t_1 =	0	1	0	1
t_2 =	0	0	1	1
$t_1 \cdot t_2$ =	0	0	0	1

Для $s = 3$ и $d = 2$, $r = 7$ мы имеем следующие расчеты для нашей конструкции (табл. 3).

Таблица 3

Новые расчеты конструкции

		0	1	2	3	4	5	6	7
0		1	1	1	1	1	1	1	1
1	t_1 =	0	1	0	1	0	1	0	1
2	t_2 =	0	0	1	1	0	0	1	1
3	t_3 =	0	0	0	0	1	1	1	1
4		0	0	0	1	0	0	0	1
5		0	0	0	0	0	1	0	1
6		0	0	0	0	0	0	1	1

После удаления последнего столбца имеем квадратную матрицу 7×7 (табл. 4).

Таблица 4

Квадратная матрица

		0	1	2	3	4	5	6	7
0		1	1	1	1	1	1	1	1
1	t_1=	0	1	0	1	0	1	0	1
2	t_2=	0	0	1	1	0	0	1	1
3	t_3=	0	0	0	0	1	1	1	1
4		0	0	0	1	0	0	0	1
5		0	0	0	0	0	1	0	1
6		0	0	0	0	0	0	1	1

Чтобы описать все такие базисы, мы можем сформировать таблицу (без потери общности и может быть после некоторой перестановки аргументов и значений) как матрицу B размера $r \times r$, имеющую верхнюю

строку (1, ..., 1) с номером 0, строки с номером $i = 1, ..., s$ — векторы x^i и далее (в некотором порядке) строки для покомпонентных произведений этих векторов (вплоть до d векторов из строк с номером $i = 1, ..., s$). После некоторой перестановки столбцов можно предположить, что столбцы строк с номером $i = 1, ..., s$ упорядочены естественным порядком. Таким образом, задача состоит в том, чтобы описать все миноры размера $r \times r$ в полной матрице Рида — Маллера для булевых функций в зависимости от аргументов s до степени d [1].

Конструкция 2. Для получения таких базисов в условии задачи предлагается использовать общую аффинную группу на пространстве F^s, $F = F_2$. Хорошо известно, что общая аффинная группа является группой автоморфизмов для кодов Рида — Маллера.

Обозначим через H_d множество векторов столбцов F_s, $F = F_2$, имеющих вес Хэмминга, не превосходящий d.

Мы можем погрузить множество H_d в пространство F^r, добавив компоненты произведений [2; 3].

$$v^{\downarrow} = \begin{bmatrix} 1 \\ t^1 \\ ... \\ t^i ... t^d \\ ... \end{bmatrix} \in F_2^r \to Z^{\downarrow} = \begin{bmatrix} c^1 \\ ... \\ c^s \end{bmatrix} \in F_2^s c^{\downarrow} = \begin{bmatrix} c^1 \\ ... \\ c^s \end{bmatrix} \in F_2^s \to G = \begin{bmatrix} G_{11} ... G_{1s} \\ ... \\ G_{s1} ... G_{ss} \end{bmatrix} \in GL(s, F \mid 2)$$

$$\{0,1\} = F_2$$

$$g(Z \mid \downarrow) = \left[c^1 + t^1 + G_{11} + ... + t^3 G_{1s} \right]$$

$$g\left(v \mid \downarrow\right) =$$

Утверждение 2. *Все аффинные образы $g(H_d)$ множества H_d дают искомые базисы.*

Такие базисы можно использовать для построения кода Рида — Маллера, который определяется через порождающую матрицу, содержащую в том числе все возможные произведения 1 строк. Количество и длины этих строк определяют параметры кода.

Библиографический список

1. *Блейхут Р.* Теория и практика кодов, контролирующих ошибки. М.: Книга по требованию, 2012.

2. *Глухов М. М.* О методах построения систем ортогональных квазигрупп с использованием групп // Математические вопросы криптографии. 2011. Т. 2, вып. 4. С. 5–24.

3. *Глухов М. М.* О применениях квазигрупп в криптографии // Прикладная дискретная математика. 2008. № 2(2). С. 28−32.

А. С. Ермаков
Институт сервиса, туризма и дизайна (филиал)
Северо-Кавказского федерального университета в г. Пятигорске

Роль интегральных преобразований в специальных проверках технических средств по требованиям безопасности информации

Аннотация. Рассмотрено применение математического аппарата интегральных преобразований, используемого при проведении специальных исследований сложных сигналов с неизвестной структурой в условиях априорной неопределенности масштабных изменений сигналов.

Ключевые слова: интегральные преобразования Фурье; интегральные преобразования Меллина; специальные исследования; сложные сигналы.

Комплекс мероприятий по поиску и выявлению электронных устройств негласного съема информации, возможно внедренных в технические средства принято называть специальными проверками. В практической работе по обеспечению выполнения требований безопасности информации выполнение мероприятий по специальным проверкам играет большую роль при обнаружении электронных устройств негласного получения информации и исследования обнаруженного сигнала, расчета его мощности, диаграммы направленности и зоны разведдоступности. Для решения этих задач, в арсенале у специалистов по защите информации на данный момент находятся различные приборы, базовым из которых является анализатор спектра. Анализаторы спектра во время своей работы оказывают специалисту наглядное представление спектральных методов, основанных на интегральном преобразовании Фурье (ПФ) анализируемых сигналов.

Наибольшее распространение в современных технических средствах передачи информации получили сложные широкополосные фазоманипулированные сигналы. Среди стандартов беспроводной связи, в которых используются сложные сигналы, можно отметить все поколения стандартов Wi-Fi, WIMAX.

Если структура сложного сигнала неизвестна, то ПФ малоэффективно для измерения таких излучений, в частности, это касается фазоманипулированных широкополосных сигналов, используемых в системах

передачи данных, анализатор «размажет» по частотной составляющей спектр сигнала, не выделив его информативную составляющую. В этом случае целесообразно попытаться использовать другие базисы, например, решать задачу обнаружения сложных сигналов в базисе интегрального преобразования Меллина (ПМ).

На рис. 1 показаны спектры широкополосного фазоманипулированного (2) и узкополосного гармонических сигналов (1) в базисе интегрального преобразования Фурье (ПФ).

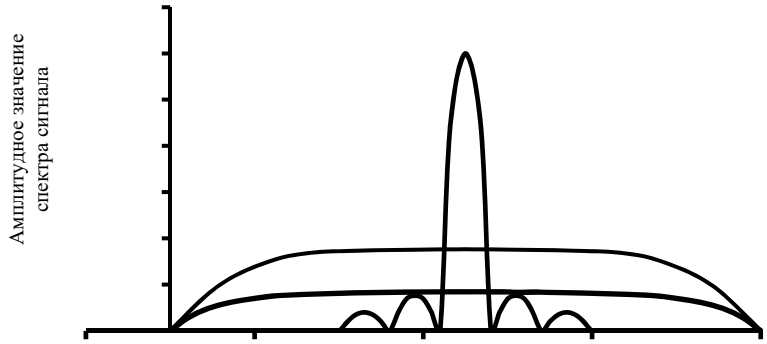


Рис. 1. Амплитудные спектры узкополосного и широкополосного сигналов в базисе преобразований Фурье

В работе рассматривается модель сигнала в виде фазоманипулированных сигналов с относительной фазовой манипуляцией. Этот класс относится к сигналам с большой фазой. Особенность их обнаружения заключается в априорном знании закона изменения фаз сложных сигналов. Если априорная информация о смене фаз известна, задача решается классическими методами, основанными на преобразованиях Фурье. При отсутствии априорной информации о законах фазовой манипуляции целесообразно воспользоваться ИП Меллина. Решение задачи основано на выводах следующей теоремы[1].

Теорема: Пусть финитная функция $S_1 t = t^{k-1} S(t)$ имеет ограниченные изменения в кольце $\sigma_1 \le k \le \sigma_2, \sigma_1, \sigma_2$ — кольца сходимости и через

[1] *Макаров А. М.* Спектральное представление гармонических сигналов в базисе интегрального преобразования Меллина // Управление и информационные технологии: межвуз. сб. Пятигорск: КМВ, 2012. С. 154–159.

равные интервалы времени τ ее огибающая изменяется на величину +1 при фазе равной π и на величину —1 при фазе равной – π, фазы изменяются по псевдослучайному закону, тогда амплитудный спектр *S_t* в базисе интегрального преобразования Меллина имеет максимум при $R_e\{S\} = 0,\ \{S\} = \sigma + ju.$

Доказательство:

Модель *S*(*t*) представим в математической записи как:

$$S(T) = \sum_{n=1}^{N} A_0[n\tau];$$

$$\forall A_0 = \begin{Bmatrix} +\text{при}\ \ \varphi = \pi \\ +\text{при}\ \ \varphi = -\pi \end{Bmatrix}\ \ n = 1, 2, ..., N.$$

Преобразования Меллина запишется в виде:

$$M(S) = \sum_{n=1}^{N}\ A_0(n\tau) \int_{(n-1)\tau}^{n\tau} t^{s-1} d(t)$$

или:

$$M(S) = \sum_{n=1}^{N}\ \frac{A_0(n\tau)\tau^S(n^S - (n-1)^S)}{S}$$

После преобразования получим реальную $R_e\{M(U)\}$ и мнимую $I_m\{M(U)\}$ составляющие *M(S)*:

$$R_e\{M(U)\} = \sum_{n=1}^{N} \frac{A_0(n\tau)\sqrt{\tau}}{0,25 + u^2}$$

$$I_m\{M(U)\} = \sum_{n=1}^{N} \frac{A_0(n\tau)\sqrt{\tau}}{0,25 + u^2}((0,5cosulnt + usinilnt)\cdot(\sqrt{n}sinulnn\tau\ -$$

$$-\sqrt{n-1}sinuln(n-1)\tau) + (0.5sinulgn - ucosuln\tau)\cdot(\sqrt{n}cosulnn\tau -$$

$$-\sqrt{n-1}scosuln(n\text{ - }1)\tau))$$

Тогда для квадрата модуля запишем:

$$|M(U)|^2 = \sum_{n=1}^{N} \frac{A_0^2(n\tau)\tau}{0,25+u^2}(R_{e_n}^2\{M(U)\} + I_{m_n}^2\{M(U)\}) +$$

$$+ \sum_{h-n=1}^{N}\sum_{h=n+1}^{N} \frac{A_n A_h \tau^2}{(0,25+u^2)}(R_{e_h}\{M(U)\}\cdot I_{m_h}\{m(U)\}) =$$

$$\sum_{n=1}^{N} \frac{A_{0\,n}^2(n\tau)\tau}{(0,25+u^2)^2} R_{e\,n}^2\{m(U)\} + \sum_{n=1}^{N} \frac{{}^{2}_{0n}(n\tau)\cdot\tau}{(0,25+u^2)^2}$$

Переходя к пределу при $u \to \infty$

$$\lim_{u\to\infty}|M(U)|^2 = \sum_{n=1}^{N} \frac{A_0^2(n\tau)\tau}{(0,25)^2} R_{e_n}^2\{M(0)\} + \sum_{n=1}^{N} \frac{A_0^2(n\tau)\tau}{(0,25)^2} I_{m_n}^2\{M(0)\}$$

$$\lim_{u\to\infty}|M(U)|^2 = 0$$

При U → 0 имеем

$$\lim_{u\to 0}|M(U)|^2 = \sum_{n=1}^{N} \frac{A_0^2(n\tau)\tau}{(0,25)^2} R_{e_n}^2\{M(0)\} + \sum_{n=1}^{N} \frac{A_0^2(n\tau)\tau}{(0,25)^2} I_{m_n}^2\{M(0)\}$$

Из этих пределов следует, что максимум спектра Меллина будет достигаться при нулевой переменной U ($U = 0$) (рис. 2).

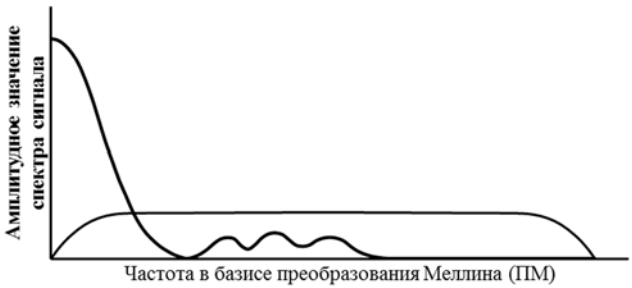


Рис. 2. Амплитудные спектры узкополосного и широкополосного сигналов в базисе преобразований Меллина

Таким образом, амплитудный спектр сигнала в базисе преобразований Меллина с фазоманипулированной фазой имеет узкополосный характер.

Из вышеприведенного можно сделать следующий вывод: одновременное использование базисов преобразования Фурье и преобразования Меллина приводит к совместной схеме обнаружения сложных сигналов в условиях априорной неопределенности масштабных изменениях сигналов, ввиду корреляционных функций шума и одновременно обеспечивает робастность решающего правила к закону фазовой манипуляции, что говорит о возможности использования данного метода как для исследования широкополосных сигналов используемых в настоящее время системами передачи данных, так и для сигналов, только разрабатываемых.

Н. А. Распопов
Уральский государственный университет путей сообщения, г. Екатеринбург

Реализация протокола Диффи — Хеллмана в не защищенном от перехвата канале

Аннотация. В статье рассматривается реализация протокола Диффи — Хеллмана в не защищенном от перехвата канале. Суть данного метода заключается в применении стеганографии для передачи открытого ключа в незащищенном канале передачи данных. Реализация протокола Диффи — Хеллмана уже давно остается актуальной, хотя и существует решение с использованием технологии инфраструктуры открытых ключей. В статье предложено новое решение данной проблемы.

Ключевые слова: асимметричная криптография; блочное шифрование; инфраструктура открытых ключей; незащищенный канал; протокол Диффи — Хеллмана; стеганография.

В 1974 г. Уитфилд Диффи и Мартин Хеллман решили проблему, остро стоявшую перед криптографией — безопасное рапределение распределение ключей шифрования. На тот момент не существовало метода, который позволил бы вырабатывать общий ключ для его использования в симметричной системе шифрования. Данный протокол основан на эксплуатации задачи вычисления дискретного логарифма [2].

При работе алгоритма каждый пользователь:

1) генерирует случайное натуральное число a — закрытый (или секретный) ключ;

2) совместно с другим пользователем устанавливает открытые параметры p и g;

3) вычисляется открытый ключ A, используя преобразования над закрытым ключом: $A = g^a \bmod p$;

4) обменивается открытыми ключами с удаленной стороной;

5) вычисляет общий секретный ключ K, используя открытый ключ удаленной стороны B и свой закрытый ключ a: $K = B^A \bmod p$.

Ключ получается равным с обеих сторон, потому что:

$B^a \bmod p = (g^b \bmod p)^a \bmod p = g^{ab} \bmod p = (g^a \bmod p)^b \bmod p = A^b \bmod p$. В практических реализациях в качестве a и b используются числа порядка 10100 и p порядка 10300. Число g необязательно должно быть большим и обычно имеет значение в пределах первого десятка.

Протокол Диффи — Хеллмана позволил решить проблему распределения ключей, но, как и у всего, у него есть недостатки. Таким недостатком является то, что невозможно однозначно установить, является ли открытый ключ, который был получен в ходе реализации протокола легальным, а не подмененным злоумышленником (рис. 1).

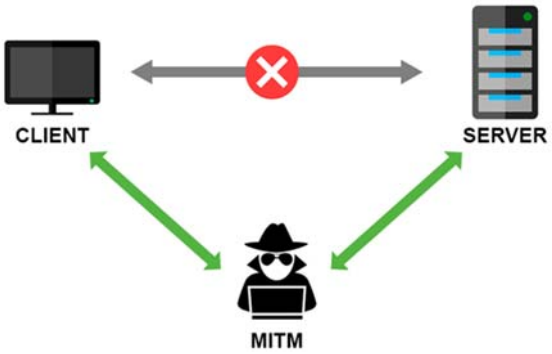


Рис. 1. Реализация атаки «человек посередине»

Атака обычно начинается с прослушивания канала связи и заканчивается тем, что криптоаналитик пытается подменить перехваченное сообщение, извлечь из него полезную информацию, перенаправить его на какой-либо внешний ресурс. Предположим, Алиса планирует передать Бобу информацию. Злоумышленник Ева обладает знаниями о структуре и свойствах используемого метода передачи данных, а также о факте планируемой передачи информации, которую она планирует перехватить. Для совершения атаки Ева «представляется» Алисе Бобом, а Бобу как Алиса. Алиса, ошибочно думая, что ведет обмен информацией с Бобом, на самом деле посылает данные Еве. Ева в своем случае совершает манипуляции с перехваченной информацией (скопировав, модифицировав) пересылает ее Бобу; Боб в своем случае полагает, что дан-

ная информация пришла от Алисы. Одним из примеров атак типа «человек посередине» является активное прослушивание, при котором злоумышленник устанавливает независимые связи с жертвами и передает сообщения между ними. Тем самым он заставляет жертв поверить, что они разговаривают непосредственно друг с другом через частную связь, фактически же весь разговор управляется злоумышленником.

На сегодняшний день известно решение данной проблемы — это инфраструктура открытых ключей Public Key Infrastructure (PKI) [1]. Основная идея PKI заключается в том, что удостоверяющий центр создает электронный документ — сертификат открытого ключа, таким образом удостоверяя факт того, что закрытый (секретный) ключ известен эксклюзивно владельцу этого сертификата, а открытый ключ (public key) свободно передается в сертификате. Недостатком данной системы является то, что сертификат может быть скомпрометирован, и тогда злоумышленник сможет под видом легального пользователя отправлять сообщения получателю. В статье предлагается метод решения проблемы уязвимости данной технологии к атаке MITM. Предлагаемое решение совмещает в себе стеганографические и криптографические методы.

Обозначим предполагаемых санкционированных участников обмена сообщениями как Алиса и Боб, а в качестве злоумышленника будет выступать Ева.

Предлагаемый алгоритм включает следующие этапы:

1. Алиса и Боб вырабатывают открытые ключи в соответствии с протоколом Диффи — Хеллмана.

2. Алиса и Боб выбирают ключи для шифрования шифром AES и публикуют их как открытую информацию. Данные ключи могут не совпадать, так как в этом случае шифрование используется исключительно для реализации «лавинного эффекта».

3. Алиса и Боб встраивают ключи в контейнер, который вмещает в себя ключ выбранной длины. Изображение-контейнер с встроенными ключами также публикуется как открытая информация.

4. Алиса и Боб обмениваются изображениями.

5. Алиса и Боб сравнивают полученные изображения с изображением, опубликованным ранее и, если изображения совпадают, то переходят к следующему этапу. Сравнение изображений происходит при помощи сканирования структуры изображений, полученных методом RGB. Если существует различие хотя бы в 1 байт, то изображение считается скомпрометированным и соединение разрывается.

6. Алиса и Боб декодируют изображение и расшифровывают свои открытые ключи при помощи ранее опубликованных ключей AES.

7. Алиса и Боб вырабатывают общий ключ, следуя протоколу Диффи — Хеллмана.

Обобщенная модель алгоритма представлена на рис. 2.

Рис. 2. Реализация алгоритма

В случае перехвата Евой изображения с встроенным в него ключом, она сможет лишь раскодировать изображение и получить открытый ключ, но, чтобы заменить его на свой, ей будет необходимо потратить значительное количество времени на подбор такого ключа, который при кодировании будет давать изображение, идентичное изображению Алисы и Боба. Также злоумышленнику необходимо скомпрометировать два изображения, а это увеличивает время работы в два раза. Обмена сообщениями между Алисой и Бобом происходит за относительно небольшой промежуток времени, любая задержка в момент обмена сообщениями может выдать злоумышленника. Это делает атаку нецелесообразной для злоумышленника, так как затраты на атаку начнут превышать ее стоимость и как следствие утратится целесообразность атаки. Также данная атака будет требовать значительного количества времени или же больших вычислительных ресурсов.

Преимущество данного алгоритма заключается в том, что пользователи являются независимыми от центров сертификации. Пользователям достаточно использовать предлагаемый алгоритм, для того чтобы выработать общий ключ. Также данный алгоритм применим в сетях, которые не используют интернет, так как в данном случае единственное, что необходимо двум абонентам для выработки общего ключа — это канал связи.

В данной статье был предложен новый метод решения проблемы реализации протокола Диффи — Хеллмана в незащищенном от перехвата канале. Также был предложен нестандартный взгляд на криптографические и стеганографические примитивы. В итоге был получен алгоритм, не требующий высокой вычислительной мощности со стороны

пользователей и являющийся простым в использовании. Были рассмотрены сферы применения, где данный алгоритм может применяться и успешно доказывать свою эффективность в сравнении с PKI.

Библиографический список

1. *Горбатов В. С., Полянская О. Ю., Шерешева М. Ю.* Основы технологии PKI. М.: Горячая линия – Телеком, 2003.

2. *Diffie W., Hellman M. E. New* Directions in Cryptography // IEEE Transactions on Information Theory. 1976. Vol. 22, no. 6. P. 644–654.

Е. А. Малыгин

Уральский государственный университет путей сообщения, г. Екатеринбург

Частные решения блок-схем Киркмана с большим порядком и их применение в защите информации

Аннотация. Приведены частные решения задачи Киркмана с большими порядками. Разработано решение для построения таких блок-схем на основе сводимости систем Киркмана с большими порядками к более малым. Приведены шаги для решения таких задач на примере задачи с порядком 63. Описано применение данных решений в прикладных и практических задачах.

Ключевые слова: блок-схемы Киркмана/Штейнера; тройки Штейнера; задача Киркмана о школьницах; решение задачи Киркмана с большим порядком.

Введение. Одной из основных задач теории блок-схем является задача классификации систем Штейнера. Впервые задача, связанная с системами троек Штейнера, была поставлена в 1844 г. Вулхаусом в [5] и имела следующую формулировку — «Определить существования различных сочетаний k-элементных множеств (блоки) из некоторого n-элементного множества, при условии, что никакие t символов, встречающиеся в некотором блоке, не встречаются ни в каком другом блоке из данного сочетания».

Частный случай этой задачи был решен и опубликован в 1847 г. Киркманом в работе [4] с параметрами $k = 3$ и $t = 2$. Задача носит название — «задача Киркмана о школьницах».

Разработанное решение задачи Киркмана на основе сводимости задачи с большим порядком к более малым.

Для начала опишем параметры блок-схемы Штейнера и условия их разрешимости. Ниже представлены формулы для расчета параметров и условия (1).

$$
\begin{aligned}
&3b = r * v \\
&r = \frac{l*(v-1)}{2} \\
&b = \frac{l*v*(v-1)}{6} \\
&g = \frac{v}{3} \\
&l*(v-1) = 0(\mathrm{mod}\,2) \\
&l*v(v-1) = 0(\mathrm{mod}\,6)
\end{aligned}
\qquad (1)
$$

где b — общее количество троек; r — количество групп троек; v — порядок системы; g — количество троек в группе.

Условие сводимости можно описать формулой (2).

$$
\begin{aligned}
&b_{L=}V_s \\
&l*v(v-1) = 0(\mathrm{mod}\,6)
\end{aligned}
\,, \qquad (2)
$$

где L — система Киркмана с большим порядком; s — система Киркмана с малым порядком.

То есть, если мы знаем решение задачи для простого V, то сможем легко найти частные решения для больших порядков, которые сводятся к этой задаче. Разработанной решение будет представлено на примере задачи Киркмана с порядком 63. Условно решение можно разбить на пять этапов.

Этап 1. Рассчитаем параметры для $v = 63$, по формулам, описанным выше. Получим следующие параметры: $v = 63$, $b = 651$, $r = 31$, $g = 21$. Далее необходимо сгенерировать базовый блок, он же будет первым блоком в нашем расписании. Первый блок мы можем заполнить в случайном порядке. Условно определим для себя ряды в блоке. Первый ряд от 0 до 60, второй от 1 до 61 и третий от 2 до 62 (рис. 1).

Этап 2. С помощью циклической перестановки второго и третьего ряда получим расписание до $r = 21$. Второй ряд необходимо сдвигать на одну ступень вниз, а третий ряд на одну ступень вверх. Ниже представлен фрагмент расписания, первые 7 блоков. Остальные блоки, до 21, заполняются по аналогичной схеме (рис. 2).

	1						
1	0	1	2	12	33	34	35
2	3	4	5	13	36	37	38
3	6	7	8	14	39	40	41
4	9	10	11	15	42	43	44
5	12	13	14	16	45	46	47
6	15	16	17	17	48	49	50
7	18	19	20	18	51	52	53
8	21	22	23	19	54	55	56
9	24	25	26	20	57	58	59
10	27	28	29	21	60	61	62
11	30	31	32				

Рис. 1. Первый базовый блок расписания

	1			2			3			4			5			6			7		
1	0	1	2	0	61	5	0	58	8	0	55	11	0	52	14	0	49	17	0	46	20
2	3	4	5	3	1	8	3	61	11	3	58	14	3	55	17	3	52	20	3	49	23
3	6	7	8	6	4	11	6	1	14	6	61	17	6	58	20	6	55	23	6	52	26
4	9	10	11	9	7	14	9	4	17	9	1	20	9	61	23	9	58	26	9	55	29
5	12	13	14	12	10	17	12	7	20	12	4	23	12	1	26	12	61	29	12	58	32
6	15	16	17	15	13	20	15	10	23	15	7	26	15	4	29	15	1	32	15	61	35
7	18	19	20	18	16	23	18	13	26	18	10	29	18	7	32	18	4	35	18	1	38
8	21	22	23	21	19	26	21	16	29	21	13	32	21	10	35	21	7	38	21	4	41
9	24	25	26	24	22	29	24	19	32	24	16	35	24	13	38	24	10	41	24	7	44
10	27	28	29	27	25	32	27	22	35	27	19	38	27	16	41	27	13	44	27	10	47
11	30	31	32	30	28	35	30	25	38	30	22	41	30	19	44	30	16	47	30	13	50
12	33	34	35	33	31	38	33	28	41	33	25	44	33	22	47	33	19	50	33	16	53
13	36	37	38	36	34	41	36	31	44	36	28	47	36	25	50	36	22	53	36	19	56
14	39	40	41	39	37	44	39	34	47	39	31	50	39	28	53	39	25	56	39	22	59
15	42	43	44	42	40	47	42	37	50	42	34	53	42	31	56	42	28	59	42	25	62
16	45	46	47	45	43	50	45	40	53	45	37	56	45	34	59	45	31	62	45	28	2
17	48	49	50	48	46	53	48	43	56	48	40	59	48	37	62	48	34	2	48	31	5
18	51	52	53	51	49	56	51	46	59	51	43	62	51	40	2	51	37	5	51	34	8
19	54	55	56	54	52	59	54	49	62	54	46	2	54	43	5	54	40	8	54	37	11
20	57	58	59	57	55	62	57	52	2	57	49	5	57	46	8	57	43	11	57	40	14
21	60	61	62	60	58	2	60	55	5	60	52	8	60	49	11	60	46	14	60	43	17

Рис. 2. Первые 7 блоков расписания

Этап 3. Исходя из расписания, составленного для первых блоков (до 21 включительно) можно заметить, что каждое значение из ряда ровно один раз встречалось со значениями из других рядов, но сами значения в одном ряду не пересекались. Выпишем каждый ряд значений из первого блока последовательно и запишем их в 22 блока (рис. 3).

	22											
1	0	3	6	8	1	4	7	15	2	5	8	
2	9	12	15	9	10	13	16	16	11	14	17	
3	18	21	24	10	19	22	25	17	20	23	26	
4	27	30	33	11	28	31	34	18	29	32	35	
5	36	39	42	12	37	40	43	19	38	41	44	
6	45	48	51	13	46	49	52	20	47	50	53	
7	54	57	60	14	55	58	61	21	56	59	62	

Рис. 3. Блок расписания для $r = 22$

Мы получили 3 блока с неповторяющимися и еще нигде непересекающимися значениями. Можно заметить, что каждый блок — это система Киркмана с параметрами $V = 21$, $b = 70$, $r = 10$, $g = 7$. Получается, если решить задачу Киркмана с порядком 21 для каждого блока, то мы получим конечное расписание для $v = 63$.

Этап 4. Итак, необходимо решить задачу с порядком 21 для каждого блока. Ниже представлено исходное расписание для $v = 21$ (рис. 4).

	1	2	3	4	5	6	7	8	9	10
1	0 1 5	3 4 9	0 7 11	1 2 3	4 5 10	1 8 9	2 0 4	5 3 11	2 6 10	18 19 20
2	4 6 12	7 8 10	9 10 14	5 7 13	8 6 11	10 11 12	3 8 14	6 7 9	11 9 13	0 3 6
3	3 10 17	1 13 14	4 8 16	4 11 15	2 14 12	5 6 17	5 9 16	0 12 13	3 7 15	1 4 7
4	8 13 15	0 16 17	2 13 17	6 14 16	1 17 15	0 14 15	7 12 17	2 15 16	1 12 16	2 5 8
5	2 9 19	2 11 20	1 6 18	0 10 19	0 9 20	2 7 18	1 11 19	1 10 20	0 8 18	9 12 15
6	7 14 20	5 12 18	3 12 19	8 12 20	3 13 18	4 13 19	6 13 20	4 14 18	5 14 19	10 13 16
7	11 16 18	6 15 19	5 15 20	9 17 18	7 16 19	3 16 20	10 15 18	8 17 19	4 17 20	11 14 17

Рис. 4. Расписание для $v = 21$

Теперь произведем замену чисел для каждого блока исходной задачи на числа из расписания для порядка 21 (выполним наложение блока на решение о 21 школьнице). Можно воспользоваться макросом (если работа ведется в MS Excel) или другими программными средствами, (рис. 5).

	22	23	24	25	26	27	28	29	30	31
1	0 3 6	3 9 39	0 45 54	3 36 18	9 6 21	3 27 39	36 0 9	6 18 54	36 12 21	60 42 51
2	9 12 15	45 27 21	39 21 48	6 45 30	27 12 54	21 54 15	18 27 48	12 45 39	54 39 30	0 18 12
3	18 21 24	3 30 48	9 27 57	9 54 33	36 48 15	6 12 24	6 39 57	0 15 30	18 45 33	3 9 45
4	27 30 33	0 57 24	36 30 24	12 48 57	3 24 33	0 48 33	45 15 24	36 33 57	3 15 57	36 6 27
5	36 39 42	36 54 51	3 12 60	0 21 42	0 39 51	36 45 60	3 54 42	3 21 51	0 27 60	39 15 33
6	45 48 51	6 15 60	18 15 42	27 15 51	18 30 60	9 30 42	12 30 51	9 48 60	6 48 42	21 30 57
7	54 57 60	12 33 42	6 33 51	39 24 60	45 57 42	18 57 51	21 33 60	27 24 42	9 24 51	54 48 24
8	1 4 7	19 10 40	1 46 55	4 37 19	10 7 22	4 28 40	37 1 10	7 19 55	37 13 22	61 43 52
9	10 13 16	46 28 22	40 22 49	7 46 31	28 13 55	22 55 16	19 28 49	13 46 40	55 40 31	1 19 13
10	19 22 25	4 31 49	10 28 58	10 55 34	37 49 16	7 13 25	7 40 58	1 16 31	19 46 34	4 10 46
11	28 31 34	1 58 25	37 31 25	13 49 58	4 25 34	1 49 34	46 16 25	37 34 58	4 16 58	37 7 28
12	37 40 43	37 55 52	4 13 61	1 22 43	1 40 52	37 46 61	4 55 43	4 22 52	1 28 61	40 16 34
13	46 49 52	7 16 61	19 16 43	28 16 52	19 31 61	10 31 43	13 31 52	10 49 61	7 49 43	22 31 58
14	55 58 61	13 34 43	7 34 52	40 25 61	46 58 43	19 58 52	22 34 61	28 25 43	10 25 52	55 49 25
15	2 5 8	20 11 41	2 47 56	5 38 20	11 8 23	5 29 41	38 2 11	8 20 56	38 14 23	62 44 53
16	11 14 17	47 29 23	41 23 50	8 47 32	29 14 56	23 56 17	20 29 50	14 47 41	56 41 32	2 20 14
17	20 23 26	5 32 50	11 29 59	11 56 35	38 50 17	8 14 26	8 41 59	2 17 32	20 47 35	5 11 47
18	29 32 35	2 59 26	38 32 26	14 50 59	5 26 35	2 50 35	47 17 26	38 35 59	5 17 59	38 8 29
19	38 41 44	38 56 53	5 14 62	2 23 44	2 41 53	38 47 62	5 56 44	5 23 53	2 29 62	41 17 35
20	47 50 53	8 17 62	20 17 44	29 17 53	20 32 62	11 32 44	14 32 53	11 50 62	8 50 44	23 32 59
21	56 59 62	14 35 44	8 35 53	41 26 62	47 59 44	20 59 53	23 35 62	29 26 44	11 26 53	56 50 26

Рис. 5. Последние блоки расписания для $v = 63$

Таким образом, будут выполнены все условия задачи и составлено итоговое расписания для порядка 63 на основе решения задачи с порядком 21.

Выводы по разработанному решению.

Если мы знаем решение для системы V_s, мы можем легко найти решение для всех:

$$V_{L=}V_S * 3^n$$
$$l * V_S(V_S - 1) = 0(\mathrm{mod}\, 6).$$

где V_L = искомый порядок системы; V_s — минимальный порядок разрешимой системы (например: v = 15, 21, 27, 33, 75); n — натуральное число.

Таким образом, мы получаем большой набор частных решений задач с большим порядком. Однако для порядков V_s данный подход неприменим, так как они в контексте данного решения являются «простейшими», соответственно данный подход не решает задачу в общем виде. Общее решение не найдено на время написания статьи, однако решения всегда есть для всех V, что доказано в работах П. Киваша [2; 3].

Применение полученных решений. Данное решение находит применение в теории кодирования, построении совершенных шифров и схемах разделения секрета. Решение применяется в прикладных задачах, таких как построение алгоритмов получения коротких сферических кодов, построение корректирующих кодов и многих других.

Также на основе разработанного решения могут быть построены крупные отказоустойчивые компьютерные сети, соответствующие всем требованиям безопасности. Подробнее о построении отказоустойчивых компьютерных сетей и систем можно прочитать в работе Г.П. Можарова [1].

Таким образом, полученные решения являются значимыми, актуальными и имеют широкое применение в области защиты информации.

Библиографический список

1. *Можаров Г. П.* Отказоустойчивые компьютерные сети, построенные на основе комбинаторных блок-дизайнов // Вестник Московского государственного технического университета им. Н. Э. Баумана. Сер.: Приборостроение. 2016. № 6(111). С. 41−53.

2. *Keevash P.* Counting designs // Journal of the European Mathematical Society. 2018. Vol. 20, issue 4. P. 903–927. DOI: 10.4171/JEMS/779.

3. *Keevash P.* The existence of designs. URL: arXiv:1401.3665.

4. *Kirkman T. P.* On a Problem in Combinations // The Cambridge and Dublin Mathematical Journal (Macmillan, Barclay, and Macmillan). 1847. Vol. II. P. 191−204.

5. *Woolhouse W. S. B.* Prize Question 1733 // Lady's and Gentlemen's Diary, 1844.

М. А. Набиулина
Уральский государственный университет путей сообщения, г. Екатеринбург

О выражении булевой функции через базовые вентили квантовых компьютеров

Аннотация. Работа посвящена применению теоремы Поста для обоснования полноты некоторого класса булевых функций. Построены таблицы истинности функций квантовых вентилей. Определена возможность выражения любой булевой функции через заданные базовые вентили квантовых компьютеров.

Ключевые слова: квантовые вентили; теорема Поста; булевы функции; Pauli-X gate; CNOT gate; CCNOT gate.

Для создания ключей шифрования, используются различные математические законы, которые изучает такая наука как математическая логика. Ее изучение начинается с алгебры высказываний или булевой алгебры, которая основывается на рассмотрении различных высказываний. Они бывают, как простые, так и составные, состоящие из логических связок. Сложные высказывания представляют собой булевы функции. Одной из проблем в области алгебры высказываний и основных логических связок является выразимость булевых функций в криптографических приложениях через заданный набор реализуемых аппаратно.

Уточним понятие квантовых вентилей:

Квантовый вентиль — это любая логическая операция с кубитами. Согласно статье Камиля Ахметовича Валиева «Квантовая информатика: компьютеры, связь и криптография»: «Квантовая система с двумя различимыми состояниями $|\mathbf{Y}_0\rangle$, $|\mathbf{Y}_1\rangle$ способная нести 1 бит информации, получила название кубит (qubit)» [1]. Следует отметить, что кубиты — это квантовая система, работающая в квантовых компьютерах.

Задачей этой работы является применение теоремы Поста для обоснования полноты различных классов булевых функций в криптографических приложениях и векторных булевых функций.

Выяснить возможность или невозможность выражения любой булевой функции через базовые вентили квантовых компьютеров: Pauli-X gate, con-trolled-NOT gate (CNOTgate), Toffoli gate (CCNOTgate).

Pauli-X gate:

$x \mid\!\rightarrow x+1$

Controlled-NOT gate (CNOT gate):

$(x,y) \mid\!\rightarrow (x,y+x)$

Toffoli gate (CCNOT gate):

$(x,y,z) \mid\!\rightarrow (x,y,z+(x \wedge y))$

Построим таблицы истинности для Pauli-X gate, CNOT gate и CCNOT gate (табл. 1−3) [3].

Таблица 1

Таблица истинности Pauli-X gate

Вход	Выход
0	1
1	0

Таблица 2

Таблица истинности CNOT gate

Вход		Выход	
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

Таблица 3

Таблица истинности CCNOT gate

Вход			Выход		
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

Рассмотрим каждую функцию в отрыве от остальных.

Pauli-X gate полностью повторяет функцию отрицания. Следовательно, проверить ее на полноту можно по теореме Поста. Для наглядности используем табл. 4, где T_0 – проверка функции на сохранение 0; T_1 — проверка функции на сохранение 1; S — проверка функции на самодвойственность; L — проверка функции на линейность; M — проверка функции на монотонность [2].

Таблица 4

Проверка Pauli-X gate на выполнение критериев теоремы Поста

	T_0	T_1	S	L	M
Pauli-X gate	–	–	+	+	–

Отсюда мы видим, что Pauli-X gate не является полным (так как является линейным и самодвойственным). Далее рассмотрим CNOT gate — обратимый логический вентиль, выполняющий операцию, схожую с классическим сложением по модулю два (или же XOR), но работающий с кубитами. На выходе он дает два значения, следовательно, нужно рассматривать оба (табл. 5).

Таблица 5

Проверка CNOT gate на выполнение критериев теоремы Поста

	*T*_0	*T*_1	*S*	*L*	*M*
Для первого значения	+	+	+	+	+
Для второго значения	+	–	–	+	–

По теореме Поста делаем вывод, что CNOT gate не является полным (в первом случае не выполняется ни один из критериев, а во втором: критерии сохранения 0 и линейности). В завершении рассмотрим CCNOT gate. Вентиль является универсальным, так как он выполняет любую из операций (NOT, AND, XOR) в зависимости от значений на входе (табл. 6).

Таблица 6

Проверка CCNOT gate на выполнение критериев теоремы Поста

	*T*_0	*T*_1	*S*	*L*	*M*
Для первого значения	+	+	+	+	+
Для второго значения	+	+	+	+	–
Для третьего значения	+	–	–	–	–

Как итог, для CCNOT gate критерии теоремы Поста не выполняются (для первого значения не выполняется ни один из критериев, для второго выполняется только один, чего недостаточно, а в последнем случае не выполняется критерий сохранения 0). Рассмотрим совокупность этих вентилей (табл. 7).

Таблица 7

Проверка совокупности вентилей на выполнение критериев теоремы Поста

	T 0	T 1	S	L	M
Pauli-X gate	–	–	+	+	–
CNOT gate (1)	+	+	+	+	+
CNOT gate (2)	+	–	–	+	–
CCNOT gate (1)	+	+	+	+	+
CCNOT gate (2)	+	+	+	+	–
CCNOT gate (3)	+	–	–	–	–

Как итог, для CCNOT gate критерии теоремы Поста не выполняются Таким образом, Pauli-X gate не сохраняет 1, 0 и имеет критерий не монотонности, CNOT gate — добавляет критерий несамодвойственности, а CCNOT gate добавляет критерий нелинейности, таким образом, для набора функций вентилей выполняются критерии теоремы Поста.

Базовые вентили квантовых компьютеров (Pauli-X gate, CNOT gate, CCNOT gate) являются полным набором, удовлетворяя теореме Поста. Отсюда следует, что через их совокупность можно выразить любую булеву функцию. (для первого значения не выполняется ни один из критериев, для второго выполняется только один, чего недостаточно, а в последнем случае не выполняется критерий сохранения 0).

Библиографический список

1. *Валиев К. А.* Квантовая информатика: компьютеры, связь и крипто-графия // Вестник Российской академии наук. 2000. Т. 70, № 8. С. 688−718.

2. *Фесенко Т. Н., Чалая Е. Ю.* Теорема Поста // Курс лекций по дискретной математике. URL: https://studfile.net/preview/2495995/page:23.

3. *Sleator T., Weinfurter H.* Realizable Universal Quantum Logic Gates // Physical Review Letters. 1995. Vol. 74, issue. 20. P. 4087–4090.

А. Н. Синадский
Уральский федеральный университет имени первого Президента России Б. Н. Ельцина,
г. Екатеринбург

Формальная модель определения классификационных признаков и аномального поведения сетевых узлов

Аннотация. Рассмотрен способ создания формальной математической модели, применяемой для определения классификационных признаков и выявления аномального поведения сетевых узлов.
Ключевые слова: классификация; аномалии; математическая модель.

Современные методы обнаружения инцидентов безопасности в телекоммуникационных сетях основываются на сигнатурном анализе сетевого трафика и методах выявления аномалий. Но перед настройкой сетевых анализаторов необходимо провести инвентаризацию существующих сетевых узлов. Предлагается для автоматизации работы по инвентаризации сетевых узлов и выявлению их аномального поведения использовать модель формирования профиля сетевого трафика узла и контроля его изменения, не требующую взаимодействия с узлами и сохраняющую целостность защищаемой системы [1; 2].

На вход модель получает сетевой трафик защищаемой системы. Набор сетевых пакетов, использующих одинаковые протоколы на всех задействованных сетевых уровнях и направленных от одного сетевого адреса к другому, назовем потоком. Поток *Flow* описывается вектором характеристик $Flow = \{feature\}_{i=0}^{numProto}$, длина которого *numProto* зависит от количества сетевых протоколов, присутствующих в пакете.

Таким образом, весь набор потоков *Flows* длиной *lenFlows* описывается набором характеристик $Flows = \{Flow\}_{i=0}^{lenFlows}$.

В качестве идентификатора каждого сетевого узла *host* из множества классифицируемых сетевых узлов *Hosts* длиной *lenHosts* используется набор адресов источника на всех *numProto* уровнях сетевой модели. Количество уровней адресации *numProto* соответствует количеству вложенных протоколов:

$$Hosts = \{host\}_{i=0}^{numHosts} = \left\{ \{host.src\}_{i=0}^{num\,\mathrm{Pr}\,oto} \right\}_{i=0}^{numHosts}$$

Основные характеристики узла — количество потоков $host.num_{flows}$, относящихся к нему, и используемые в этих потоках протоколы. Для каждого узла описывается вектор характеристик:

$$host.proto = \{frequency\}_{i=0}^{host.numKnownProto},$$

длина которого *host.numKnownProto* соответствует общему количеству известных протоколов всех уровней во всем массиве потоков, а каждый элемент frequency характеризуется числом от 0 до 1, зависящим от количества потоков, относящихся к этому узлу и имеющих в своем составе соответствующий протокол. Узел имеет набор ярлыков:

$$host.labels = \{label\}_{k}^{numTypes},$$

каждый из которых характеризует его принадлежность к одному из классов. Группы классов формируются независимо по двум признакам: роль узла (например, ПЛК, АРМ, АСО, …), операционная система (Windows XP, Windows 7, Linux Ubuntu, Linux CentOS, …).

Также узел характеризуется долей потоков, связывающих его с узлами определенных классов *host.connectedWith*.

Для описания узла в формате, пригодном для анализа моделями машинного обучения, важные характеристики сводятся в характеристический вектор узла *host.vector*. В него добавляется информация о частоте использования узлом протоколов на каждом сетевом уровне, частоте появления потоков, связывающих его с узлами различных типов, и вместе они являются профилем трафика узла *host.vector*={*host.proto, host.connectedWith*}.

В качестве дополнения характеристический вектор может расширяться за счет использования специфичных для некоторых протоколов полей.

Полученный характеристический вектор - профиль трафика узла.

Исходные данные:

$$data = \{host.vector\}_{i}^{lenHosts}$$

для модели представляются в виде набора характеристических векторов узлов.

Для обучения модели необходима априорная информация о классах узлов, поэтому необходимо задать каждый из

$host.labels = \{label\}_k^{numTypes}$. То есть дамп трафика должен состоять из набора потоков, для всех входных данных (адресов источника, для каждого узла $host_i$)в которых заранее известен ответ — тип узла *label*.

Имеющийся трафик с размеченными узлами делится на две части: тренировочную и тестовую. Сначала модель обучается на тренировочной выборке, имея в качестве ответов значения параметра *host.label*, известные для всех узлов. Затем модель выполняет распознание узлов из тестовой выборки, и по результатам сравнения предсказанных *host.labelPredicted* и заранее размеченных *host.label* классов с помощью некоторых метрик оценивается качество работы модели. Если оно удовлетворяет заданным требованиям, то модель сохраняется, в противном случае структура модели или ее гиперпараметры меняются, и цикл из обучения, тестирования и изменения модели повторяется до тех пор, пока не будет достигнуто достаточное качество предсказания.

Кроме определения классов узлов с помощью модели можно выявлять аномалии в сетевом трафике. Для этого из существующего набора потоков *Flows* выделяются характеристические вектора *host.vector*, на которых модель обучается, причем каждому узлу задается собственный класс *host.label*. Таким образом, все многомерное пространство, чья размерность равна длине характеристического вектора *host.vector,* становится разделенным на множество областей, количество которых равно количеству узлов *num.Hosts*.

При появлении новой группы потоков *Flows* характеристические вектора узлов *host.vector* обновляются и подаются на вход модели. Результаты работы модели сохраняются в свойство $host.new_{label}$ соответствующего узла и сравниваются с известными классами узлов *host.label*. Если обнаруживается расхождение ($host_i.label \neq host_i.new_{label}$), то оно считается аномалией. Потоки *Flows*, которые его вызвали (которые изменили характеристический вектор этого узла *host.vector,* считаются инициаторами аномалии, и передаются оператору как потенциально опасные, также указывается узел *host*, поведение которого было отмечено как аномальное.

Если расхождения между известными и полученными вновь классами отсутствуют ($host_i.label = host_i.new_{label}$), то модель заново обучается, используя в качестве входных данных обновленные характеристические вектора узлов *host.vector* (происходит переразметка многомерного пространства), и переходит в режим ожидания следующего набора потоков. Считается, что аномального поведения в этот раз не выявлено.

Описанная формальная модель позволяет решать задачу определения классификационных признаков и выявления аномалий в поведении сетевых узлов.

Для выбора оптимальной комплексной модели машинного обучения предполагается использование метода автоматизированного машинного обучения «Tree-based Pipeline Optimization Tool».

Метрики качества работы модели приведены в таблице.

Метрики качества работы модели

Тип класса	Точность	Полнота	F1-мера
Роли узлов (АРМ, ПЛК, Сервер, …)	0.7	0.7	0.7
Операционная система (WinXP, Win8, LinuxCentOS, ...)	0.86	0.8	0.78

Для повышения точности планируется расширить набор исходных данных, оптимизировать модель и применить метод word2vec для подготовки данных.

Библиографический список

1. *Богданов В. В., Домуховский Н. А., Лейчук Д. В., Синадский А. Н., Комаров Д. Е.* Выявление аномалий в работе информационных систем с помощью машинного обучения // Защита информации. Инсайд. 2020. № 3 (93). С. 31–35.

2. *Пырьев М. С., Синадский А. Н.* Определение характеристик сетевого узла на основе профиля сетевого трафика // Современные проблемы радиоэлектроники и телекоммуникаций: сб. науч. тр. / под ред. Ю. Б. Гимпилевича. Москва-Севастополь: Изд-ва РНТОРЭС им. А. С. Попова, СевГУ. 2020. № 3. С. 220.

А. С. Стрельникова
Уральский федеральный университет имени первого Президента России Б.Н. Ельцина, г. Екатеринбург

Математические методы криптографии

Аннотация. Рассмотрены основные математические методы криптографии, приведены некоторые криптографические алгоритмы: симметричные, асимметричные и их разновидности, с использованием формул для шифрования и расшифровки. Разобрано несколько задач.

Ключевые слова: криптоалгоритм; ключ; шифрование; подстановка; перестановка; генерация.

Криптография в данный момент разделяется на две основные области исследования: симметричная и асимметричная криптография (см. таблицу). Симметричное шифрование часто используется как синоним симметричной криптографии, а асимметричная криптография охватывает два основных варианта использования, это асимметричное шифрование и цифровые подписи [2].

Сравнение симметричных и асимметричных криптоалгоритмов

Тип алгоритма	Шифрование/Расшифрование	Скорость работы	Требования к вычислительным ресурсам	Стойкость к перехвату
Симметричные	Один ключ для шифрования и расшифрования	Высокая	Низкие	Ключ является уязвимой точкой для перехвата
Асимметричные	Два ключа (криптопара). Один ключ для шифрования, второй ключ для расшифрования	Низкая	Высокие	Открытый ключ распространяемся всем желающим, а закрытый ключ известен только Вам. Такой подход повышает стойкость к перехвату

Наиболее известными методами симметричных криптоалгоритмов являются подстановки и перестановки.

Подстановки. В прямых подстановках каждый знак исходного текста заменяется одним или несколькими знаками. Одним из важных подклассов прямых подстановок являются моноалфавитные подстановки, в которых устанавливается взаимно-однозначное соответствие между знаком e_i исходного алфавита и соответствующим знаком c_j зашифрованного текста. Все методы моноалфавитной подстановки можно представить как числовые преобразования букв исходного текста, рассматриваемых как числа, по следующей формуле [4]:

$$c \equiv (a \times e + s) \bmod K, \qquad (1)$$

где a — десятичный коэффициент; s — коэффициент сдвига; e — код буквы исходного текста; c — код зашифрованной буквы; K — длина алфавита; *mod* — операция вычисления остатка от деления выражения в скобках на модуль K.

Пример: Шифр Цезаря [4]

Рассмотрим шифрование на алфавите, состоящим и 26 латинских букв и знака пробела (пробел будем изображать знаком #). Знаку # присвоим код 0, букве A — код 1, B — код 2, … букве Z — код 26.

Исходное сообщение: WE#NEED#SNOW

Возьмем следующие параметры: $a = 1$ $s = 2$ $K = 27$

Формула для шифрования примет вид: $c \equiv (e + 2) \bmod 27$ (2)

Входной алфавит:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Выходной алфавит:

B C D E F G H I J K L M N O P Q R S T U V W X Y Z # A

(Буквы сдвигаются на две позиции: A-C B-D и т.д.)

Тогда исходное сообщение в зашифрованном виде будет выглядеть так:

YGBPGGFBUPQY

Для расшифровки (для случая, когда a = 1) используется следующая формула:

$$e \equiv (K + c - s) \bmod K. \quad (3)$$

Перестановки. Знаки исходного текста можно переставлять в соответствии с определенным правилом. В качестве примера приводится линейная перестановка.

Пример 1. Линейная перестановка [4]

Пусть необходимо зашифровать следующий текст:

ГРУЗИТЕ#АПЕЛЬСИНЫ#БОЧКАХ

Разобьем текст на группы длиной, например по 4 символа:

ГРУЗ ИТЕ# АПЕЛ ЬСИН Ы#БО ЧКАХ

Зададим следующее правило перестановки: «переставить группировки из четырех букв, находящихся в порядке 1-2-3-4 в порядок 3-1-4-2».

Получим следующий зашифрованный текст:

УГРЗ ЕИ#Т ЕАЛП ИЬНС БЫО# АЧХК

Запись исходного текста и последующее считывание шифротекста можно производить по разным путям некоторой геометрической фигуры, например, квадрата или прямоугольника.

Асимметричное шифрование основано на парах чисел, одно из этих чисел — открытый ключ, который находится в открытом доступе. С помощью этого числа любой пользователь может зашифровать сообщение, но расшифровать сообщение с помощью этого же числа не получится. Для расшифровки используется второе число — закрытый ключ, он должен быть секретным.

Открытый и закрытый ключ всегда связаны между собой алгоритмом, внутри этого алгоритма есть третье секретное число, которое связано с обоими ключами [3]. Простым примером такой асимметричного шифрования является зашифрованная электронная почта, в которой открытый ключ может использоваться для шифрования сообщений, а приватный (закрытый) ключ для их расшифровки.

Самый простой способ установить такую связь — взять два больших простых числа и перемножить их, получится еще большее число,

которое и будет лежать в основе алгоритма. Внутри этого алгоритма будет математика, которая зависит от разложения чисел на множители. Если ни одно из первоначальных простых чисел неизвестно, то разложить на множители такое число будет очень сложной задачей.

Асимметричное шифрование применяется в основном в двух случаях [1]:

— когда нужно установить защищенный канал связи в интернете. Известно, что изначально наши данные при передаче могут перехватить другие пользователи, поэтому нужно обмениваться только теми ключами, которые можно показывать другим;

— для создания цифровых подписей и сертификатов. Это позволяет проверять подлинность цифровых документов, а также убедиться, что его отправил именно владелец сертификата.

Генерация ключей. Одна из базовых проблем в реализации криптосистем — это проблема генерации случайных чисел. Только абсолютно случайное число может рассматриваться в качестве надежного ключа. Идеальным источником случайных чисел являются результаты измерения случайных физических величин. Для этого необходимо использовать физические датчики случайных чисел. В ряде случаев такие средства недоступны, и поэтому приходится использовать генераторы псевдослучайных чисел. Наиболее распространенным классом таких генераторов являются рекуррентные генераторы [1].

Библиографический список

1. *Анин Б. Ю.* Защита компьютерной информации. СПб.: БХВ-Петербург, 2000.

2. *Баричев С. Л., Гончаров В. В., Серов Р. Е.* Основы современной криптографии: учеб. курс. М.: Горячая линия - Телеком, 2001.

3. *Левин М.* Криптография: руководство пользователя. М.: Познават. книга плюс, 2001.

4. *Нечаев В. И.* Элементы криптографии: Основы теории защиты информации: учеб. пособие. М.: Высш. шк., 1999.

Н. С. Толмачев, А. А. Хегай, А. П. Черникова
Уральский государственный университет путей сообщения, г. Екатеринбург

Многообразия в образе кубической функции поля нибблов

Аннотация. Работа посвящена описанию структуры аффинных и линейных многообразий, лежащих в образе функции $F(x) = x^3+x$ поля нибблов GF(24). Представлены утверждения о конкретных случаях сдвига многообразий в образе этой функции. Результаты могут быть применимы в более общей ситуации.

Ключевые слова: конечные поля; неприводимый многочлен; аффинные многообразия; линейные многообразия; образ функции; двумерное подпространство; полином.

В работе получены некоторые закономерности в структуре аффинных многообразий, связанные со сдвигами многообразий, что может быть полезным при решении задачи «The image set» из второго тура международной олимпиады по криптографии NSUCRYPTO — 2017. Исследуется образ Image F поля $GF(16)$ под действием кубической функции $y = F(x) = x^3 + x^4$, где поле $GF(24)$ построено при помощи таблицы степеней корня неприводимого многочлена $g(x) = x^4 + x + 1$ [2]. Изучаются двумерные аффинные многообразия (четверки) — многообразия, содержащие четыре элемента конечного поля, представленные в виде подмножества $A = \{y_1, y_2, y_3, y_4\}$, таких что $y_1 + y_2 + y_3 + y_4 = 0$, лежащие в образе функции $y = F(x) = x^3 + x$, $y \in$ Image F, а также двумерные линейные многообразия (тройки) — многообразия, содержащие 4 элемента конечного поля, один из которых равен 0, представ-ленные в виде подмножества $A = \{y_1, y_2, y_3, y_4\}$, таких что $y_1 + y_2 + y_3 + y_4 = 0$, лежащие в образе функции $y = F(x) = x^3 + x$, $y \in$ Image F. Путем вычисли-тельных экспериментов получены следующие результаты.

Утверждение 1. Сдвиг двумерного линейного подпространства, лежащего в образе F, на элемент, лежащий в образе функции F, но не лежащий в этом подпространстве, дает двумерное аффинное многообразие, не лежащее в образе.

Утверждение 2. Сдвиг двумерного аффинного многообразия, лежащего в образе функции F, и не содержащего нуль, на элемент этого многообразия, дает двумерное линейное многообразие, не лежащее в образе F. Согласно автоморфизму Фробениуса, сформулируем очевидное:

Утверждение 3. При возведении в квадрат элементов двумерного аффинного многообразия, получается двумерное аффинное многообразие. Это означает, что задача поиска аффинных многообразий в образе функции F эквивалентна задаче поиска аффинных многообразий на су-

персингулярной эллиптической кривой $Y_2 + Y = X^3 + X$ [1]. Любое двумерное аффинное многообразие, лежащие в образе функции $F(x) = x^3 + x$, пересекается хотя бы по одному элементу с другим двумерным аффинным многообразием, лежащим в образе этой функции. Отсюда вытекает:

Утверждение 4. Не существует трехмерных аффинных многообразий в образе функции $F(x) = x^3 + x$.

Библиографический список

1. *Болотов А. А., Гашков С. Б., Фролов А. Б., Часовских А. А.* Элементарное введение в эллиптическую криптографию. М.: КомКнига, 2006.

2. *Фомичев В. М.* Дискретная математика и криптология. М.: Диалог-МИФИ, 2003.

Организационное и правовое обеспечение информационной безопасности

А. А. Азовцева, А. В. Иванова, Д. Н. Мазнин
Магнитогорский государственный технический университет им. Г. И. Носова,
г. Магнитогорск

Типовые ошибки в организации защиты персональных данных вуза

Аннотация. Рассмотрены основные ошибки, совершаемые вузами России при обработке, хранении и защите персональных данных студентов и абитуриентов.
Ключевые слова: обработка персональных данных; ПДн; согласие на обработку; студент; защита данных.

Хотя процесс обработки и защиты персональных данных (ПДн) носит схожий характер для различных организаций, не стоит забывать, что существуют особенности, которые не позволяют применять один и тот же подход в различных организациях. Рассмотрим типовые ошибки, которые характерны для обработки и защиты ПДн в образовательных организациях высшего образования.

Самой первой ошибкой, которая встречается в университетах России — единая форма согласия на обработку персональных данных для абитуриента и студента. Цели обработки для данных групп лиц значительно отличаются, а значит и согласия должны быть разные.

Абитуриент предоставляет данные, необходимые для поступления в университет, а именно:

— фамилия, имя, отчество;

— год рождения; месяц рождения;

— дата и место рождения, гражданство;

— адрес (место жительства и/или место фактического проживания);

— сведения об образовании (название образовательного учреждения, год окончания, специальность/направление подготовки, документ об образовании: вид, серия, номер, кем и когда выдан);

— свидетельства о результатах Единого государственного экзамена;

— документ, удостоверяющий личность (номер, серия, кем и когда выдан);

— контактный телефон, адрес электронной почты;

— сведения о родителях (фамилия, имя, отчество, контактный телефон);

— сведения об индивидуальных достижениях;

— сведения о наличии прав на льготное поступление (документы (вид документа, серия, номер, кем выдан), подтверждающие наличие особых прав приема в вузы);

— специальные категории персональных данных (справка установленного образца о состоянии здоровья).

Обработка персональных данных студентов осуществляется исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, в связи с обучением субъекта персональных данных в вузе. Для студента в согласие добавляются данные о воинской обязанности, сведения о проживании в общежитии, факультет, группа, направление подготовки, специальность, форма обучения, семейное положение и информация о детях. Кроме того, появляется пункт о передачи ПДн студента в банк, для начисления стипендии; в организации и на предприятия, предоставившие места для прохождения практики; в медицинские организации для проведения медико-профилактических обследований.

Также существует проблема в описании сроков действия согласия. В идеале оно должно быть действительно с момента подписания и до утраты правовых оснований обработки соответствующей информации или по достижению цели обработки информации. Но есть вузы, где данное согласие действительно 10 лет или «в сроки, указанные действующим законодательством Российской Федерации». В действующем законодательстве не указано никаких точных сроков действия документа по обработке ПДн, поэтому не понятно, сколько согласие студента будет действительно в университете.

Хранение данных студентов и абитуриентов должно осуществляться на разных носителях, но при одной форме согласия можно смело предположить, что при хранении данные разных групп людей смешиваются, и появляется еще одно нарушение.

Еще одна ошибка связана с публикацией ПДн студента или абитуриента в общедоступных источниках. Во многих вузах при наборе абитуриентов на сайте университета публикуется список поступающих с набранными балами за экзамены. После окончания приемной комиссии, списки поступивших студентов также размещаются на сайте и на информационных стендах. Но не во всех университетах в согласии на обработку персональных данных прописан пункт о размещении какой-либо информации об абитуриенте или студенте в общедоступных информационных ресурсах. После достижения целей обработки персональных

данных студента следует убирать данные из информационной системы, путем удаления, обезличивания, либо перемешивания. Данные передаются в архив и уходят из-под влияния № 152-ФЗ «О персональных данных».

А. О. Денисова, С. С. Титов
Уральский государственный университет путей сообщения, г. Екатеринбург

Изменения в Федеральном законе «Об электронной подписи» от 6 апреля 2011 г. № 63-ФЗ

Аннотация. Рассматриваются изменения в Федеральном законе «Об электронной подписи» от 6 апреля 2011 г. № 63-ФЗ, устанавливаются даты вступления в силу изменений. Определяются сроки внесения поправок и дальнейшая судьба рынка в области электронной подписи. Исследована возможность подключения регистрационного центра к действующему удостоверяющему центру и условия присоединения.
Ключевые слова: электронная подпись; изменения; федеральный закон; сроки; регистрационный центр; удостоверяющий центр.

В конце 2019 г. Госдума приняла поправки в Федеральный закон № 63-ФЗ «Об электронной подписи» (Федеральный закон № 63). Федеральный закон от 27 декабря 2019 г. № 476-ФЗ «О внесении изменений в Федеральный закон „Об электронной подписи“ и статью 1 Федерального закона „О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля“» был опубликован на «Официальном интернет-портале правовой информации» 28 декабря 2019 г. В июне 2020 г. сроки вступления в силу некоторых поправок перенесли — был принят Федеральный закон от 8 июня 2020 г. № 166-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в целях принятия неотложных мер, направленных на обеспечение устойчивого развития экономики и предотвращение последствий распространения новой коронавирусной инфекции». Изменения будут вступать в силу в течение двух лет и значительно поменяют функционирование действующих аккредитованных Удостоверяющих центров.

С 1 июля 2020 г. вступает группа поправок, связанная с заменой одного из основных понятий в законе об электронной подписи. В частности, изменились правила получения электронной подписи. Если раньше в законе при выдаче сертификатов предполагалось «Установление личности», то сейчас введен термин «Идентификация». Вместе с идентификацией появилась легальная дистанционная идентификация.

Иными словами, возможно провести идентификацию при личном присутствии будущего владельца сертификата или дистанционно (с помощью действующей электронной подписи или биометрических данных из загранпаспорта или единой биометрической системы). Второй момент, идентификация производится непосредственно заявителя (будущего владельца сертификата). Если раньше были возможны схемы, которые позволяли передоверить получение сертификата, и это не противоречило Законодательству РФ, то теперь в законе четко обозначено, что идентификация производится только самого заявителя. То есть сотрудник организации больше не может получить электронную подпись вместо руководителя, если подпись оформлена на руководителя.

Изменения в Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи», вступающие в силу с 1 июля 2020 г.:

1. Дистанционная идентификация (и соответствующая отметка в сертификатах о способе идентификации) — только самим УЦ.

2. Идентификация непосредственно заявителя (будущего владельца сертификата):

2.1. Запрет на получение сертификата по доверенности.

2.2. Отмена «корпоративных схем» раздачи сертификатов.

3. Недопустимость ограничения признания КЭП. Теперь невозможно не признать документ, подписанный квалифицированной электронной подписью, недействительным.

С 1 января 2020 г. начинается второй этап вступления в силу поправок в Федеральный закон № 63-ФЗ «Об электронной подписи», который предполагает:

1. Институт доверенной третьей стороны.

2. Возможность использования «облачной» электронной подписи:

2.1. Отдельные новые требования к «облачным» средствам УЦ и ЭП.

2.2. Хранение ключей только аккредитованным УЦ.

3. Дополнительные требования к аккредитации УЦ.

4. Взаимодействие УЦ с ЕИСА (информация о выданных сертификатах и безвозмездная регистрация в ЕИС).

5. Информирование о выявленных случаях приостановления технической возможности ключа.

С 1 января 2022 г. вступают в силу изменения: институт электронных подписей и новый принципиально другой порядок применений ЭП в ИС. Теперь появляются специальные отраслевые УЦ: УЦ ФНС — для всех юридических лиц и индивидуальных предпринимателей; УЦ ФНС — для финансовых организаций; УЦ Федерального казначейства — для государственных структур.

Схема подписи физического лица остается примерно такой же, как и была. Сертификат получается в АУЦ и при подписании электронного документа, документ сопровождается электронной подписью физического лица. Иногда может прикладываться документ о полномочиях, если это не те полномочия, которые определяются его представительством юридического лица, а касается чего-то другого.

Схема подписи юридического лица меняется существенно. Теперь единоличный исполнительный орган юридического лица может получить сертификат только в соответствующем УЦ (УЦ ФНС, УЦ ЦБ, УЦ ФК). После этого руководитель может использовать этот сертификат для формирования электронной доверенности на своего сотрудника, который при этом имеет сертификат физического лица. Как было отмечено ранее, с 1 января 2022 г. доверенности на представительство интересов юридического лица перестают быть разрешенные к применению при выдаче сертификатов. Соответственно, фактически остается две категории сертификатов: либо это сертификаты на генеральных директоров (ЕИО), либо на физических лиц. Если физическое лицо действует не от своего лица, а от имени юридического лица, то подписание электронного документа должно быть помимо подписи физического лица сопровождаться электронной доверенностью и КЭП ЮЛ.

После внесения изменений в Федеральный закон № 63 многие удостоверяющие центры потеряли потенциальных потребителей из других территориально населенных пунктов. После запрета выдачи квалифицированного ключа электронной подписи многие клиенты не имеют возможность приехать в УЦ и получить сертификат лично. Для выхода из этой ситуации можно воспользоваться такой привилегией, как регистрационный центр.

Регистрационный центр (РЦ) — опциональный субъект PKI, уполномоченный ПУЦ регистрировать пользователей, обеспечивать их взаимодействие с ПУЦ и проверять информацию, которая заносится в сертификат, но не подписывающий и не выпускающий сертификаты.

Оператор Регистрационного центра (Оператор РЦ)- уполномоченное лицо Регистрационного центра, ответственное за выполнение операций по регистрации пользователей, обеспечению их взаимодействия с ПУЦ и проверке информации, которая заносится в сертификат.

Обязанности регистрационного центра:

1) в целях обеспечения взаимодействия между сторонами УЦ и РЦ назначить ответственное лицо;

2) ответственное лицо РЦ обязан пройти инструктаж в учебном центре центра для осуществления деятельности, направить в Удостоверяющий центр подписанное уведомление о прохождении инструктажа

в форме бумажного или электронного документа со списком прошедших обучение с отметкой об успешной аттестации уполномоченных работников Регистрационного центра;

3) соблюдать технологию работы, предписанную УЦ;

4) строго соблюдать требования регламента Удостоверяющего центра, опубликованного на сайте (далее Регламент УЦ);

5) устанавливать личность заявителя при личном обращении заявителя за получением сертификата ключа проверки электронной подписи, проверять предоставленные заявителем документы либо их надлежащим образом заверенные копии.

А. А. Жохова, Д. А. Ярмола
Московский государственный университет им. М. В. Ломоносова, г. Москва

Актуальные проблемы правового обеспечения информационной безопасности при взаимодействии органов власти и граждан

Аннотация. Выявляются проблемы правового обеспечения информационной безопасности при взаимодействии органов власти и граждан. Предлагаются пути решения одной из поставленных проблем, затрагивающей кибербезопасность при обращении граждан в органы власти посредством социальных сетей.

Ключевые слова: информационная безопасность; правовое обеспечение, взаимодействие органов власти и общества.

Актуальность правого обеспечения информационной безопасности в современном мире связана с появлением новых видов взаимодействия органов власти и граждан посредством информационно-коммуникационных технологий. Помимо очевидных преимуществ (появление новых каналов обратной связи; отсутствие временного лага; и т.п.), новые информационные технологии, повсеместно использующиеся при взаимодействии граждан с органами власти, могут быть и источниками новых угроз. Ежедневно порталы государственных и муниципальных органов власти подвергаются хакерским атакам, поэтому для решения проблемы правого обеспечения информационной безопасности ставится цель выявления угроз и слабых мест в этой системе, а также их устранение, для того чтобы исключить использование порталов третьими лицами. Такая информационная защита сегодня без сомнений является одним из важнейших приоритетов государственной деятельности, а, следовательно, необходима выработка и применение государством единой политики в сфере информационной безопасности на всех уровнях.

Наиболее значимым нормативно-правовым актом, освещающим проблемы кибербезопасности, является Доктрина информационной безопасности Российской Федерации, утвержденная указом Президента России от 5 декабря 2016 г. № 646. В данном нормативно-правовом акте закреплены стратегические приоритеты и главные направления деятельности государственных органов в сфере информационной безопасности. Однако, помимо этого, в Доктрине информационной безопасности отмечается, что развитие и применение информационных технологий должно подкрепляться одновременным обеспечением кибербезопасности с целью минимизирования риска проявления информационных угроз.

Одна из наиболее значимых проблем связана с таким явлением как сайты-зеркала. Данные виды сайтов, несмотря на разный веб-адрес, имеют одинаковый контент на своих страницах. Законодательно данная проблема была частично решена при принятии Федерального закона от 1 июля 2017 г. № 156-ФЗ «О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации“». С помощью данного нормативно-правового акта зачастую носителям исключительных прав удается добиться блокировки зеркал пиратских сайтов, которые незаконно публикуют какой-либо контент, что наносит удар по его правообладателям. При этом, зачастую после блокировки сайтов, создается его зеркало с другим доменом, а для блокировки нового адреса требуется некоторое время на подачу заявления в суд. Решением суда сайт блокируется, однако, в случае изменения его адреса, он вполне может продолжать свое функционирование до следующего правового решения. Более того, сайты-зеркала могут создаваться в качестве порталов органов власти или банков с целью извлечения персональных данных и другой информации от невнимательных пользователей. Но также они могут служить источником межнациональной и другой розни, дезинформации, публикуя соответствующие новости.

Важной проблемой кибербезопасности в контексте государственного управления является процесс работы с обращениями граждан, поступающих из социальных сетей. До 2006 г. в Российской Федерации существовала проблема использования технических средств информационных систем, которые размещались на территории иностранных государств, что не позволяло должным образом обеспечить безопасность персональных данных российских пользователей. Однако в ч. 2.1 ст. 13 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» были определены требования к обеспечению информационной безопасности, которые установили, что «технические средства информационных систем, используемых государственными органами, органами местного само-

управления, государственными и муниципальными унитарными предприятиями или государственными и муниципальными учреждениями, должны размещаться на территории Российской Федерации». Данные требования запрещают для государственных органов власти и органов местного самоуправления использование облачных вычислительных мощностей иностранных государств для работы сайтов, так как в таком случае возникает сложность с определением физического местонахождения таких мощностей, что делает обеспечение информационной безопасности довольно затруднительным. Для решения такой проблемы, была поставлена задача в развитии собственных вычислительных мощностей и облачных технологий внутри российского государства.

Однако с активным развитием социальных сетей органы власти начали использовать их как новую площадку для взаимодействия с гражданами, что породило новую проблему в области правового обеспечения информационной безопасности. Сервера большинства социальных сетей находятся на территории иностранных государств, в связи с чем возможна утечка персональных данных граждан. Речь идет о таких персональных данных, как паспортные данные граждан, фотографии документов и т.д. Например, сервера социальной сети Facebook находятся на территории Силиконовой Долины, то есть, в области Санта-Клары, а также в Вирджинии и Европе. Помимо этого, один из важнейших серверов располагается за пределами США в Швеции[1]. Социальная сеть Instagram до 2012 г. хранила данные на публичном облаке Amazon Web Services, однако после приобретения сети Facebook, данные были перенесены в ее дата-центры[2]. Обеспечение кибербезопасности является важным условием при осуществлении взаимодействия власти и граждан посредством социальных сетей в связи с проблемой утечки персональных данных пользователей.

В данный момент, обозначенные проблемы правового обеспечения информационной безопасности при взаимодействии органов власти и граждан остаются неразрешенными и малоизученными. Данный вопрос требует куда более тщательной проработки действий органов власти в сфере защиты авторских и смежных прав, а также борьбы с сайтами, имеющими противозаконный контент. Возможно выделить несколько путей решения одной из поставленных проблем, связанной с кибербезопасностью в социальных сетях при обращении граждан в органы власти. Первым путем решения данной проблемы может быть использование социальных сетей для взаимодействия с гражданами, основные

[1] *Сервера* и дата-центр Фейсбука — секреты. URL: http://7facebook.ru/2019/08/11/serve7.

[2] *Где* хранятся страницы социальных сетей? URL: https://madspark.ru/data-centers.

мощности которых располагаются в Российской Федерации. На сегодняшний день основные вычислительные мощности популярной российской социальной сети «ВКонтакте» располагаются в Санкт-Петербурге[1]. Однако такие социальные сети, как Instagram, Facebook и Twitter до сих пор отказываются перенести часть серверов, содержащих персональные данные российских пользователей, на территорию Российской Федерации[2]. Это может привести к утечке персональных данных, которые находятся не под контролем органов власти РФ. Вторым путем решения данной проблемы может стать законодательное ограничение публикации персональных данных пользователями при взаимодействии с органами власти.

Таким образом, несмотря на значимое количество преимуществ взаимодействия власти и населения посредством информационно-коммуникационных технологий существует ряд проблем, снижающих его эффективность. Даже с принятием властью различных решений для правового обеспечения информационной безопасности остается множество угроз, связанных с утечкой личных данных и распространением дезинформации.

А. А. Заведенская, Т. Ю. Зырянова
Уральский государственный университет путей сообщения, г. Екатеринбург

Соотнесение мер защиты информации, указанных в ГОСТ Р 57580.1-2017, с мерами защиты из приказа ФСТЭК России от 18 февраля 2013 г. № 21

Аннотация. При построении систем защиты информационных систем персональных данных финансовыми организациями должны применяться меры защиты, определенные как Банком России, так и ФСТЭК России. В статье приводится анализ соотнесения мер защиты ГОСТ Р 57580.1-2017 и приказа ФСТЭК России от 18 февраля 2013 г. № 21.

Ключевые слова: защита информации; система защиты; персональные данные; Банк России; ФСТЭК России; ГОСТ Р 57580.1-2017.

На момент написания статьи, в нормативном поле требований по обеспечению информационной безопасности финансовой сферы можно выделить несколько основных видов финансовых организаций:

— кредитные организации (КО);

[1] *Дата-центр* «ВКонтакте».. URL: https://vk.com/blog/datatsentr-vkontakte.

[2] *Суд* оштрафовал Facebook и Twitter на 4 млн р. каждую за отказ переносить серверы с данными в РФ. URL: https://habr.com/ru/news/t/488248.

— некредитные финансовые организации (НФО);

— субъекты национальной платежной системы (НПС).

Так 26 марта 2019 г. официально было опубликовано Положение ЦБ РФ от 9 января 2019 г. № 672-П «О требованиях к защите информации в платежной системе Банка России» (далее — 672-П). Затем 21 мая 2019 г. официально были опубликованы Положение ЦБ РФ № 683-П от 17 апреля 2019 г. «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента» (683-П) и Положение ЦБ РФ от 17 апреля 2019 г. № 684-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций» (684-П). 672-П определило требования по защите информации для субъектов НПС, 683-П — для КО, а 684-П — для НФО. Согласно упомянутым ранее Положениям Банка России субъекты НПС, КО и НФО должны обеспечить реализацию уровней защиты информации, определенных ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер» (ГОСТ Р 57580.1-2017).

Таким образом, финансовые организации обязаны применять организационные и технические меры, перечисленные в ГОСТ Р 57580.1-2017. Данный ГОСТ устанавливает три уровня защиты информации (см. рисунок). По сути, применяя подход аналогичный приказам ФСТЭК России № 17/21/31/239, когда от уровня защиты информации зависит базовый состав мер. Уровень определяется в зависимости от размеров и направления деятельности организаций[1].

Уровни защиты информации, определенные ГОСТ Р 57580.1-2017

[1] *Заведенская А. А.* Обзор изменений в законодательстве за май 2019. URL: https://www.ussc.ru/news/novosti/obzor-izmeneniy-v-zakonodatelstve-za-may-2019.

На основании ГОСТ Р 57580.1-2017 финансовой организации необходимо определить совокупность мер защиты информации, входящих в состав системы защиты информации и системы организации и управления защитой информации, применяемых совместно в пределах контура безопасности для реализации политики защиты информации организации. При этом в ГОСТ Р 57580.1-2017 для финансовых организаций установлена процедура соотнесения уровней защиты информации к уровням защищенности персональных данных (ПДн) при их обработке в информационных системах персональных данных (ИСПДн):

— для обеспечения соответствия четвертому уровню защищенности ПДн при их обработке в ИСПДн рекомендуется использовать требования, установленные ГОСТ Р 57580.1-2017 для уровня 3 — минимальный;

— для обеспечения соответствия третьему и второму уровням защищенности ПДн при их обработке в ИСПДн рекомендуется использовать требования, установленные ГОСТ Р 57580.1-2017 для уровня 2 — стандартный;

— для обеспечения соответствия первому уровню защищенности ПДн при их обработке в ИСПДн рекомендуется использовать требования, установленные ГОСТ Р 57580.1-2017 для уровня 1 — усиленный.

Выбор и применение финансовой организацией мер защиты по ГОСТ Р 57580.1-2017 включает в себя этап дополнения при необходимости адаптированного (уточненного) состава и содержания мер защиты информации, определенных ГОСТ Р 57580.1-2017, мерами, обеспечивающими выполнение требований к защите информации, установленных нормативными правовыми актами в области обеспечения безопасности и защиты информации. Таким образом в случае наличия в контуре безопасности финансовой организации ИСПДн необходимо применять также меры по обеспечению безопасности ПДн при их обработке в ИСПДн, определенные приказом ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (приказ ФСТЭК России № 21).

По ГОСТ Р 57580.1-2017 меры защиты информации разделяются «попроцессно», а в приказе ФСТЭК России № 21 выделяются группы мер по обеспечению безопасности ПДн с соответствующими идентификаторами. В таблице приведено сопоставление процессов, определенных ГОСТ Р 57580.1-2017 и мер по обеспечению безопасности ПДн приказа ФСТЭК России № 21.

Соотнесение мер защиты ГОСТ Р 57580.1-2017 и приказа ФСТЭК России № 21

Меры защиты информации согласно ГОСТ Р 57580.1-2017		Меры по обеспечению безопасности ПДн согласно приказу ФСТЭК России № 21
Процесс 1 «Обеспечение защиты информации при управлении доступом»	Управление учетными записями и правами субъектов логического доступа	Управление доступом субъектов доступа к объектам доступа
	Идентификация, аутентификация, авторизация (разграничение доступа) при осуществлении логического доступа	Идентификация и аутентификация субъектов доступа и объектов доступа
	Защита информации при осуществлении физического доступа	Защита технических средств
	Идентификация, классификация и учет ресурсов и объектов доступа	Управление конфигурацией информационной системы и системы защиты ПДн
Процесс 2 «Обеспечение защиты вычислительных сетей»	Сегментация и межсетевое экранирование вычислительных сетей	Защита информационной системы, ее средств, систем связи и передачи данных
	Защита информации, передаваемой по вычислительным сетям	
	Защита беспроводных сетей	
	Выявление сетевых вторжений и атак	Обнаружение (предотвращение) вторжений
Процесс 3 «Контроль целостности и защищенности информационной инфраструктуры»		Обеспечение целостности информационной системы и персональных данных
		Ограничение программной среды
		Обеспечение доступности ПДн
Процесс 4 «Защита от вредоносного кода»		Антивирусная защита
Процесс 5 «Предотвращение утечек информации»		Защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные
		Защита информационной системы, ее средств, систем связи и передачи данных
		Регистрация событий безопасности
Процесс 6 «Управление инцидентами защиты информации»	Мониторинг и анализ событий защиты информации	Регистрация событий безопасности
		Контроль (анализ) защищенности персональных данных
	Обнаружение инцидентов защиты информации и реагирование на них	Выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы

Окончание таблицы

Меры защиты информации согласно ГОСТ Р 57580.1-2017		Меры по обеспечению безопасности ПДн согласно приказу ФСТЭК России № 21
		и (или) к возникновению угроз безопасности ПДн, и реагирование на них
Процесс 7 «Защита среды виртуализации»		Защита среды виртуализации
Процесс 8 «Защита информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств»		Защита информационной системы, ее средств, систем связи и передачи данных

Примечание. Составлено по: *ГОСТ* Р 57580.1-2017. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер; *Об утверждении* Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных: приказ ФСТЭК России от 18 февраля 2013 г. № 21.

Как видно из проведенного анализа, регуляторы используют общие подходы к защите информации, выбирая примерно одинаковый перечень направление обеспечения информационной безопасности. При этом в ГОСТ Р 57580.1-2017 определены и способы реализации мер: организационные или технические средства, а для технических средств даются примеры рекомендуемых классов решений специализированных средств защиты информации. Приказ ФСТЭК России № 21 позволяет оператору ИСПДн самостоятельно определить способ реализации мер защиты информации. Также стоит отметить, что исходя из проведенного соотнесения, в случае если финансовой организацией для ИСПДн ранее уже были реализованы требования приказа ФСТЭК России № 21, то приведение ИСПДн в соответствие ГОСТ Р 57580.1-2017 не потребует больших затрат.

Е. Ю. Иванова
Финансовый университет при Правительстве РФ, г. Москва

Основные исследовательские подходы к детектированию инсайдерских угроз

Аннотация. Внутренняя угроза стала одной из основных проблем в кибербезопасности. Такие угрозы требуют специальных систем, методов и инструментов, позволяющих облегчить точное и быстрое обнаружение внутреннего нарушителя. В статье представлены основные подходы к детектированию инсайдерских угроз, выявлены их преимущества и недостатки.

Ключевые слова: кибербезопасность; кража данных; инсайдерские угрозы; стратегии детектирования инсайдерских угроз.

Антропогенные уязвимости, угрозы, атаки и риски имеют больший вес по сравнению с техногенными и наносят значительный ущерб организациям, и минимизация их на основе комбинированного применения разных методов исследования является новой и актуальной научной задачей с ожидаемым положительным эффектом. Поэтому крайне важно минимизировать негативное влияние инсайдеров на бизнес организации путем своевременного их обнаружения, адекватного реагирования, предотвращения утечки информации и применения к ним дисциплинарных и правовых мер пресечения. Однако, есть много ограничений, таких как отсутствие реальных случаев, предвзятость в выводах, а также недостаточное количество статистических данных, описывающих действия пользователей в системах.

Внутренняя угроза — это проблема безопасности, которая возникает от лиц, имеющих доступ к корпоративной сети, системам и данным, например, сотрудников и доверенных партнеров. Хотя внутренние угрозы возникают нечасто, размер ущерба от них больше, чем от внешних вторжений. Согласно исследованию института Ponemon стоимость инцидентов, зависит от размера организации. Большие организации (с численностью персонала от 25 000 до 75 000 чел.) потеряли в среднем 17,92 млн долл. США за последний год, в то время как малые организации (с численностью персонала ниже 500) потратили в среднем 7,68 млн долл. для устранения инцидентов, связанных с действиями инсайдеров. Наибольший рост инсайдерских угроз был отмечен в следующих отраслях: розничная торговля (рост на 38,2% за два года) и финансы (рост за два года на 20,3%)[1].

[1] *Cost* of Global report. URL: https://cdw-prod.adobecqms.net/content/dam/cdw/on-domain-cdw/brands/proofpoint/ponemon-global-cost-of-insider-threats-2020-report.pdf.

Выделяют следующие типы инсайдеров[1]:

— неосторожный работник: это сотрудник, который не соблюдает требования Политики информационной безопасности организации, действия которого могут включать нарушение политик доступа, использование нецелевых инструментов и установку сторонних приложений, которые могут стать причиной возникновения уязвимостей в организациях;

— внутренний агент: это инсайдер, к которому обращаются внешние злоумышленники и используют его как часть более крупной схемы. Злоумышленники вербуют или подкупают уязвимых инсайдеров для кражи информации от их имени. Также, злоумышленник может атаковать скомпрометированного инсайдера, собирая его учетные данные при помощи социальной инженерии, а затем получить доступ к организационным активам, что может привести к краже интеллектуальной собственности организации;

— злонамеренный инсайдер: инсайдер, имеющий доступ к корпоративным активам и использующий существующие привилегии для доступа к информации в своих личных целях, например, кражи информации и последующей ее перепродажи;

— поставщики услуг/деловые партнеры: и сторонние организации, которые ставят под угрозу безопасность из-за неправильного использования, небрежности или несанкционированного использования активов компании.

Эффективный способ борьбы с внутренними угрозами - мониторинг действий пользователей и выявление аномалий поведения, которые могут иметь злонамеренный характер. Существует три основных исследовательских стратегии для обнаружения внутренних угроз: создание набора правил, обнаружение аномалий на основе графового метода, построение моделей машинного обучения[2]. Преимущества и недостатки указанных стратегий описаны в таблице.

Первая стратегия — создание набора правил. Группа экспертов создает набор правил для выявления злонамеренных действий инсайдеров. Затем поведение каждого пользователя записывается в журнал и проверяется, чтобы определить, соответствует ли оно какому-либо из заранее разработанных правил.

---

[1] *Маркова Т. И., Захарова К. В.* Классификация инсайдеров // Вестник Волжского университета им. В.Н. Татищева. 2010. № 15. С. 29−34.

[2] *Impact* and Key Challenges of Insider Threats on Organizations and Critical Businesses. URL: https://www.researchgate.net/publication/344686225_Impact_and_Key_Challenges_of_Insider_Threats_on_Organizations_and_Critical_Businesses.

Сравнительные характеристики стратегий детектирования инсайдеров

Стратегия	Преимущества	Недостатки
Создание набора правил	Простота реализации. Возможность детализации правил применительно к конкретным кейсам	Зависимость от экспертных знаний. Необходимость регулярных обновлений правил экспертной группой
Обнаружение аномалий на основе графов	Анализ взаимосвязи между данными. Анализ качества данных	Высокая сложность реализации. Высокий процент ложных срабатываний
Построение модели машинного обучения	Автоматическая идентификации пользователей, которые совершают необычные действия среди всех пользователей на основе данных из различных источников. Непрерывное обновление моделей на основе статистических данных. Отсутствие зависимости от экспертных оценок	Зависимость от качества данных. Необходимость выбора оптимальной модели

Вторая стратегия — построение графа для выявления подозрительных пользователей или злонамеренного поведения путем отслеживания изменений в структуре графа. Выявление инсайдерских угроз на основе графового метода не только анализирует ценность самих данных, но также анализирует взаимосвязи между данными.

Третья стратегия — построение модели машинного обучения. На основе обучающей выборки на основе статистических данных. Обнаружение внутренних угроз с использованием методов машинного обучения направлено на разработку метода автоматической идентификации пользователей, которые совершают необычные действия среди всех пользователей без предварительных знаний или правил.

Инсайдерские угрозы являются одними из самых серьезных угроз безопасности и главной проблемой организации любого размера. На основе сравнительного анализа обнаружения внутренних угроз, а также выделены их преимущества и недостатки. Для обнаружения угроз, которые связаны как с техническими характеристиками, так и с поведением человека, построение моделей машинного обучения, является лучшим методом для получения результатов.

А. В. Кириченко, Н. В. Ганженко
Уральский государственный университет путей сообщения, г. Екатеринбург

Влияние цифрового следа на обеспечение конфиденциальности информации

Аннотация. Освещаются проблемы обеспечения конфиденциальности информации при растущем объеме цифрового следа, оставляемого пользователями в сети Интернет. Обозначаются возможности их разрешения и предлагаются рекомендации по снижению негативного влияния цифрового следа на конфиденциальность информации.
Ключевые слова: цифровой след; конфиденциальность; информационная безопасность; персональные данные.

Стремительное развитие информационных технологий приводит к тому, что человечество начинает использовать все большее их количество в своей повседневной жизни. Потребность в окружении себя технологиями является базовой для современного человека. В своей повседневной жизни человек генерирует огромное количество цифровой информации, большую часть которой составляет информация о самом себе. Посты в социальных сетях, комментарии к таким постам, история посещений сайтов — вся эта информация может быть использована для того, чтобы отследить пользователя в Сети. Цифровой след пользователя — одно из самых опасных явлений в информационном пространстве.

Итак, цифровой след — это информация, которая остается в Сети после действий пользователя. Следы миллионов пользователей по всему миру представляют собой большие данные (Big Data), и являются целью обработки многих организаций, начиная монопольными гигантами вроде Amazon и Google и заканчивая рекламными компаниями.

Цифровой след бывает активным и пассивным. Активный след — это сознательные действия пользователя в Сети — посты в социальных сетях, комментарии, фотографии, переписка, лайки и т.д. Пассивный же след — это непредумышленно оставленные данные — геолокация мобильного устройства, история посещений сайтов, IP-адрес устройства, с которого пользователь выходил в сеть. На основе цифрового следа фильтруется и отбирается интересующий пользователя контент во Всемирной Паутине. Рекламные компании идут тем же путем — анализируя деятельность пользователя в Сети, они составляют его портрет как потребителя, и предлагают те товары и услуги, что заинтересуют потребителя с большей вероятностью. Несомненно, фильтрация контента и таргетированная реклама очень облегчает жизнь пользователя в сети. С другой стороны, интернет-площадки могут менять цены на свою продукцию в зависимости от истории покупок пользователей, повышать цены

при увеличении количества заказов и наоборот, уменьшать цены при отсутствии заказов.

Чтобы понять, как именно возникает цифровой след, необходимо разобрать цифровую информацию по составу. Большая часть цифровой информации визуальна: ее составляют фотографии, видеоролики, данные с камер видеонаблюдения, телевизионный сигнал. На втором месте находится текстовая информация — электронная почта, электронные документы, переписки пользователей. Следом за текстовой информацией идет голосовая информация — различные виды телефонной связи. И, наконец, логи — временные записи каждого действия каждого пользователя на каком-либо ресурсе — самая недолговечная информация, которая автоматически удаляется через определенные промежутки времени[1].

Визуальная информация — фотографии и видеоролики с участием пользователя — практически невозможно удалить из Сети, если они были туда загружены. Постоянное архивирование баз данных сетевых ресурсов гарантируют постоянное присутствие загруженных материалов в сети.

Текстовая информация — посты в социальных сетях, записи в блогах, переписки в мессенджерах — также могут быть архивированы и останутся в сети. Посты и записи можно удалить со своей страницы, но это не гарантирует того, что кто-то не сохранит пост до момента его удаления. Личные переписки могут оставаться в сети довольно долгое время, становясь частью резервной копии интернет-ресурса. Также, к личной или рабочей переписке может получить доступ посторонний человек — с помощью взлома аккаунта или от собеседника пользователя.

Голосовая информация (телефонные переговоры) сохраняется операторами связи в течение какого-то времени. Разговоры абонентов время от времени записываются с целью настройки и тестирования алгоритмов предотвращения преступной деятельности, и эта информация также может быть использована против пользователя, если доступ к ней получит злоумышленник.

Все эти данные могут быть использованы недоброжелателями и злоумышленниками. Фото-, видео- и голосовые материалы могут быть использованы для уничтожения репутации одного человека или группы людей либо компрометации их тайной личной жизни. Текстовая информация из переписок может использоваться для тех же целей. Рабочие же переписки и документы, которые были получены путем несанкциониро-

[1] *Цифровая* тень и цифровой след // ИнтернетБезопасность.РФ. URL: https://inetsafety.ru/cifrovaja-ten-i-cifrovoj-sled.

ванного доступа к учетной записи работника организации с использованием его цифрового следа могут привести к серьезным убыткам организации.

Но даже без использования средств связи человек оставляет довольно значительный цифровой след. Перемещаясь из точки А в точку Б, человек обязательно попадает под прицел видеонаблюдения. Камеры расположены во всех местах скопления людей, на входах в банки, магазины, заведения общественного питания, торговые центры. Данные с этих камер видеонаблюдения подвергаются длительному хранению и многократному копированию. В случае какого-либо инцидента запись тут же будет обнародована, и удалить ее из сети будет практически невозможно.

Банковские операции — еще один источник достаточно большого пласта информации. При совершении операции банк получает точную информацию о местоположении магазина или другого заведения, наименование и стоимость товара или услуги. Анализ этих данных может привести к компрометации адреса проживания, работы, уровня доходов, статей расходов и даже медицинских данных. Учитывая, как часто происходят утечки баз данных банковской информации — довольно опасная информация в руках злоумышленников. Многим людям сразу после получения кредита или крупного перевода поступают звонки от мошенников, представляющихся службой безопасности банка и обманом пытающихся завладеть чужими средствами.

На совокупности использования всех этих данных разработана и введена Система социального кредита в Китае. Анализируя большие данные из сотен источников, система создает социальный портрет каждого гражданина, и на основе его проступков инициализирует применение к нему различных санкций — от запрета работы в государственных учреждениях до отказа вбронировании номеров в отелях и даже отказа в социальном обеспечении, и наоборот — поощрений в случае образцового поведения. У этой системы есть противники, которые обвиняют правительство Китая в попытке установки тотального контроля за гражданами, однако система уже начала приносить свои плоды, и уровень преступности и недостойного поведения в тестируемых населенных пунктах начал снижаться[1].

Еще одна новая разработка — фитнес-трекеры. Небольшой браслет на руке и приложение в телефоне — и у пользователя есть карманный фитнес-тренер, который подскажет правильный режим пробежек и тренировок. Эти данные также отправляются на сервера приложений для

[1] *Китайская* система социального кредита — так ли страшен черт? // Хабр. URL: https://habr.com/ru/post/453850.

статистики. Но кроме жизненных показателей в течение дня фитнес-трекер постоянно передает информацию о геолокации браслета. Так, в ноябре 2017 г. компания Strava, занимающаяся разработкой приложения, контролирующего физическую активность пользователей, создала «тепловую карту», на которой отобразила географическую активность пользователей по всему миру. Целью этой карты было показать более удобные маршруты для пробежек. Но спустя 2 месяца сиднейский студент Натан Русер обнаружил «перегретые» участки карты с повышенной беговой активностью как раз в местах расположения американских военных баз. Так, на первый взгляд безобидные данные о пробежках пользователей поставили под угрозу национальную безопасность целого государства[1].

Так, цифровой след человека в информационной сфере является серьезным инструментом воздействия. Все больше данных о человеке оказывается в открытом доступе, и на основе этих данных можно как безобидно выдать пользователю таргетированную рекламу об акции в гипермаркете через дорогу, так и полностью уничтожить репутацию человека или целой организации. Генерация огромного объема информации о действиях пользователей ставит под угрозу конфиденциальность как свойство информации.

Есть несколько правил, при соблюдении которых можно существенно снизить негативное влияние цифрового следа на успешную жизнедеятельность. Первое, и самое главное, — стараться не участвовать в сомнительных мероприятиях, в которых можно оставить очередную порцию личных данных или получить ущерб репутации. Второе правило — внимательно относиться к безопасности всех своих учетных записей: от банковских аккаунтов до аккаунтов в социальных сетях и на тематических форумах. И третье правило — пытаться поддерживать положительную репутацию в окружении. Высокий кредит доверия позволит выдержать пару ударов по репутации, которые могут возникнуть при недобросовестном использовании цифрового следа.

[1] *Цифровые* следы: как интернет учит нас ответственному поведению // РБК. URL: https://www.rbc.ru/opinions/technology_and_media/02/03/2018/5a96ba709a79475e2e9688cb.

А. М. Киселева
Финансовый университет при Правительстве РФ, г. Москва

Информационные и экономические риски российских компаний в условиях цифровой экономики

Аннотация. С развитием цифровых технологий увеличился уровень угрозы появления различных видов киберпреступлений, которые несут в себе отрицательный характер для общества. В статье рассматриваются информационные и экономические риски компаний и меры по их минимизации.

Ключевые слова: информационные и экономические риски; цифровая безопасность; цифровая экономика; российские компании.

Тенденции глобальной информатизации общества присущи современной экономике. Сегодня одним из важнейших ресурсов, которые определяют конкурентоспособность и эффективность деятельности экономических субъектов, в том числе предприятий, стала информация. Но одновременно с этим она очень уязвима и потому необходимо заботиться об информационной и экономической безопасности и искать эффективные методики управления рисками для предотвращения утечки внутренних данных компании [2, с. 143].

Для повышения уровня ознакомления и владения цифровыми технологиями государство осуществляет политику по развитию цифровой экономики в стране (см. таблицу). Несмотря на некоторые высокие показатели, Российская Федерация значительно отстает в развитости цифровой экономики от стран, сопоставимых по уровню образования и качества человеческого капитала [3, с. 119].

В свою очередь, развитие цифровых технологий порождает определенные возможности для увеличения числа киберпреступлений, поэтому на сегодняшний день одним из наиболее актуальных направлений является обеспечение информационной и экономической безопасности. Это означает принятие мер по защите информации на различных уровнях управления, что должно обеспечиваться как компаниями и ее сотрудниками, так и на законодательном уровне. Также важно обеспечение стабильного функционирования и качественного использования ресурсов для предотвращения угроз. Наиболее эффективное использование корпоративных ресурсов предприятия достигается путем достижения функциональных целей:

— достижение высокой конкурентоспособности;
— обеспечение высокой финансовой эффективности и устойчивости;
— достижение высокой эффективности менеджмента;
— обеспечение качественной правовой защищенности [2, с. 145].

Структура цифрового сектора России по величине добавленной, % [3, с. 120]

Цифровой сектор России	2011	2012	2013	2014	2015	2016	2017
Телекоммуникации	49	47	45	44	36	35	38
ИТ и прочие информационные услуги	18	22	21	22	28	28	33
Производство ИКТ-оборудования	13	14	15	18	19	20	11
Оптовая торговля ИКТ-товарами	6	5	7	7	6	7	7
Издательская деятельность	4	4	4	3	3	3	3
Деятельность в области производства	10	8	8	7	7	8	7

Информационные риски — это возможные события, которые оказывают непосредственное влияние на информацию (о предприятии): ее удаление, искажение, нарушение ее конфиденциальности или доступности. Данные риски также можно назвать информационными угрозами, которые, в свою очередь, можно разделить на различные виды (см. рисунок).

Для минимизации рисков такого характера используется комплекс инструментов: обучение сотрудников правилам работы в условиях цифровизации и информатизации, внедрение и применение электронной цифровой подписи, биометрические технологии и другие [1, с. 43].

Если переходить от теории к практике, то в настоящее время действительно случаются различные киберпреступления. Например, уже дважды в СМИ сообщалось о некой утечке личных данных клиентов «Сбербанка»: 20 тыс. записей в октябре 2019 г. и данные 60 млн кредитных карт в феврале 2020 г. Правда, этих данных недостаточно, чтобы напрямую списывать деньги, обычно мошенники представляются сотрудниками банка и пользуются наивностью клиентов, которые сами рассказывают свои пароли и CVC-код.

В свою очередь, ПАО «Сбербанк» уверяет, что данные клиентов хорошо защищены. Если и действительно происходит утечка данных клиентов, то это дело рук не каких-то мошенников, а самих сотрудников банка, решивших заработать легкие деньги путем продажи конфиденциальной информации банка.

Естественно, такой персонал немедленно увольняется, и ПАО старается усовершенствовать систему минимизации человеческого фактора в такого плана ситуациях[1].

[1] *СМИ* обнаружили новую утечку данных клиентов Сбербанка. URL: https://clck.ru/RygKc.

Информационные угрозы [1, с. 44]

Можно сделать вывод: в условиях цифровизации экономики появляются новые виды рисков, требующие стратегии устранения.

В целях минимизации и предотвращения экономических и информационных рисков необходимо:

— разработать международные правовые нормы, способные регулировать рынок труда;

— внутри компании обеспечить взаимодействие всех подразделений организации в обеспечении экономической и информационной безопасности, а также в решении уже существующих проблем и информационных угроз;

— бороться с асимметрией информации между экономическими субъектами;

— развивать технологии для обеспечения безопасности внутренних данных компании;

— разработать системы обучения сотрудников навыкам и правилам работы в условиях развитой информационной среды.

Библиографический список

1. *Благих И. А.* Бизнес-правила компаний и обеспечение защиты информации в условиях цифровой экономики в России // Вестник ТИСБИ. 2018. № 4. С. 41–48.

2. *Герасимова В. В.* Экономические и социальные риски в условиях становления и развития цифровой экономики // Экономика и предпринимательство. 2019. № 6. С. 141–144.

3. *Кот М. К., Белозерова О. А., Шпанагель Ф. Ф.* Цифровая экономика и правовые и экономические риски предпринимателей в РФ // Проблемы развития предприятий: теория и практика. 2018. № 4. С. 117–122.

А. Д. Кубарев, А. В. Потапов, С. В. Поршнев
Уральский федеральный университет имени первого Президента России Б. Н. Ельцина, г. Екатеринбург

Вопросы управления стратегией аудита информационной безопасности предприятия государственного сектора

Аннотация. Рассмотрены проблемные вопросы управления аудитом информационной безопасности типового предприятия государственного сектора. Акцент сделан на управляющей функции по отношению к вопросам аудита информации, содержащей сведения конфиденциального характера.

Ключевые слова: аудит; конфиденциальная информация; подразделения информационной безопасности; инцидент; управление.

Сегодня проблема информационной безопасности имеет достаточно большую актуальность. Это связано с увеличением объема защищаемой информации, а также с появлением дополнительного технического оснащения средств разведки. Предприятия государственного сектора не являются исключением — процессы, протекающие в них, часто имеют отношение к информации закрытого характера. Для проверки соответствия предъявляемым требованиям по защите информации проводится процедура аудита. Эту процедуру проводят специальные подразделения по защите информации, либо уполномоченные сотрудники. Стоит сказать, что к защите информации, которая содержит сведения, содержащие государственную тайну, предъявляются особенные требования, но существует и служебная информация, не имеющая грифа секретности, но общедоступность которой недопустима. И методики защиты такой информации, и методики аудита систем защиты определяются локальными нормативными актами, чаще всего, не имеющими достаточной степени проработанности. В данной статье понятие «аудит информационной безопасности» обозначает проверку соответствия обращения с информацией ограниченного распространения заданным требованиям.

Цель данной статьи — рассмотрение процессов управления аудитом информационной безопасности на предприятии государственного сектора. Актуальность статьи заключается в определении проблемных моментов, возникающих на этапе управления аудитом информационной

безопасности в отношении сведений, не составляющих государственную тайну, но необходимых к защите.

Необходимо отметить, что к информации ограниченного распространения может относиться информация с ограничительной пометкой «для служебного пользования». Текущее законодательство Российской Федерации не предусматривает понятие «служебная тайна», оно было выведено из оборота еще в 2006 году. Но обращение с подобной информацией требует внимания. Аудиторы, проводящие проверки информационной безопасности, часто уделяют максимальное количество внимания защите информации, содержащей государственную тайну, а вопросы конфиденциальной информации с ограничительной пометкой или без таковой, остаются без должной проработки. Как следствие, необходимо управленческое решение и воздействие на подразделения аудита либо отдельных сотрудников, уполномоченных на проведение аудита. На рисунке приведена схема выработки и реализации управленческого решения, направленного на определение задач подразделению аудита информационной безопасности.

Схема выработки и реализации управленческого решения по аудиту

Стоит отметить, что управленческая задача руководства предприятия государственного сектора является важной и неотъемлемой частью аудита информационной безопасности. Руководитель предприятия, как ответственное за обеспечение информационной безопасности лицо,

определяет политику защиты информации, содержащей сведения конфиденциального характера. Данная политика носит обобщенный характер, в ней указываются основные линии работы. Следующая управленческая роль — работа по направлению заместителя руководителя предприятия государственного сектора, им определяется и вырабатывается стратегия защиты информации ограниченного распространения, при необходимости определяется, на каких участках работы предприятия может циркулировать данная информация, какие именно сведения относятся к ней, а также какие меры по защите информации необходимо принимать. Нижестоящий орган управления — подразделение информационной безопасности или уполномоченное лицо, это непосредственно аудиторская функция. В его функции входит: непосредственная проверка, на каких участках циркулирует защищаемая информация, проверка знаний работников по обращению с информацией ограниченного распространения, разработка и подача для рассмотрения и утверждения руководству предприятия планов по проведению аудита на период, анализ аудиторской работы за прошедший период и составление отчетности. Особенное внимание на всех уровнях управления необходимо уделять обучению сотрудников, так как меры контроля не могут быть достаточными при неграмотном обращении исполнителей с информацией ограниченного распространения.

В настоящей статье была поднята научная проблема управления аудитом информационной безопасности. Рассмотрены вопросы выработки управленческих решений на различных уровнях управления для обеспечения эффективного процесса аудита информации, не составлявшей государственную тайну, но требующей ограниченного распространения. Рассмотрена типовая структура предприятия государственного сектора. Данная структура представлена с точки зрения аудита информационной безопасности. Основная идея статьи — обозначить проблему управления аудитом информационной безопасности, проводимым в интересах защищаемой информации, не содержащей сведений, составляющих государственную тайну.

А. Д. Кубарев, А. В. Потапов, С. В. Поршнев
Уральский федеральный университет имени первого Президента России Б .Н. Ельцина,
г. Екатеринбург

Анализ функциональных подсистем центров обработки данных

Аннотация. Проведен анализ и описаны основные функции подсистем центров обработки данных.

Ключевые слова: сервер; кластер; центр обработки данных; подсистема; компонента; эксплуатация; хранение; обработка данных; система обнаружения атак.

Сегодня, в эпоху цифровых технологий, данные являются основой любой стороны деятельности человеческого общества. Чаще всего, данные передаются, обрабатываются и хранятся в электронном виде, на базе серверных технологий. Хотя многие организации пытаются произвести подсчеты, какое именно количество информации существует в электронном виде, определение точного количества не представляется возможным ввиду большого количества стохастических и детерминированных процессов, происходящих в области цифровых данных в каждый момент времени. Серверы объединяют в центры обработки данных, к которым предъявляются дополнительные требования. Обеспечение надежности, достоверности и целостности, доступности в любое время пользовательских данных — основные задачи серверных платформ.

Цель статьи — рассмотреть архитектуру центров обработки данных с точки зрения функционирования подсистем и выделить вопросы информационной безопасности.

Настоящая статья будет посвящена обзору основных характеристик и определению требований, необходимых для построения центров обработки данных. В рамках написания статьи концептуально будут рассмотрены инженерные вопросы, касающиеся эксплуатации систем обеспечения работоспособности вычислительных машин центров обработки данных и непосредственно организации их работы. Актуальность данной темы велика, так как если при построении центра обработки данных будут упущены некоторые моменты, такие, как вопросы информационной безопасности, они могут стать негативным или критическим фактором в вопросах управления процессами, связанными с пользовательскими данными.

Центры обработки данных имеют определенную архитектуру[1].

В большом количестве научных источников для описания архитектуры центров обработки данных используется многоуровневый подход.

[1] *ГОСТ Р* 53111- 2008. Устойчивость функционирования сетей связи общего пользования. Требования и методы проверки.

В рамках данной статьи будет применен подход разделения на функциональные подсистемы. Среди них можно перечислить следующие: серверная подсистема, подсистема хранения данных, подсистема информационной безопасности, подсистема эксплуатации и обеспечения, подсистема передачи данных.

Серверная подсистема является одной из основных подсистем центра обработки данных. В серверную подсистему включаются специализированные вычислительные машины, обладающие достаточным объемом вычислительных мощностей для обработки поступающих транзакций.

Подсистема хранения данных является своеобразным ядром всей системы, реализованной на базе центра обработки данных. Данная подсистема обеспечивает непосредственное хранение данных на промышленных машинных носителях.

Подсистема информационной безопасности является основной подсистемой обеспечения. Она предназначена для достижения необходимого уровня надежности хранения данных с точки зрения противодействия угрозам, связанным с несанкционированными действиями различного рода нарушителей. Данная подсистема является одной из наиболее сложных компонент с точки зрения функционирования. Построение данной подсистемы базируется на применении аппаратно-программных, инженерно0технических и организационно-правовых подходов [1].

Подсистема эксплуатации является подсистемой обеспечения жизнедеятельности центра обработки данных. Она необходима для обеспечения правильной работы вех подсистем в части, касающейся требований к оборудованию, определяемому его производителем.

Подсистема передачи данных — транспортная среда, благодаря которой центр обработки данных связан с внешней телекоммуникационной инфраструктурой, а также при помощи которой осуществляется взаимодействие подсистем центра обработки данных.

На рис. 1 приведена схема построения центра обработки данных. Стоит отметить, что правильная организация всех систем при построении центра обработки данных — основная задача, так как дальнейшее администрирование, возможность масштабирования и балансировка нагрузки будут невозможны, если на этапе построения не будут учтены некоторые вопросы. Важность любой подсистемы сложно переоценить — несмотря на то, что часть подсистем являются основными, а часть — подсистемами обеспечения, их роль однозначно высока. Основными считаются подсистемы, работающие с данными непосредственно, а не наиболее важные.

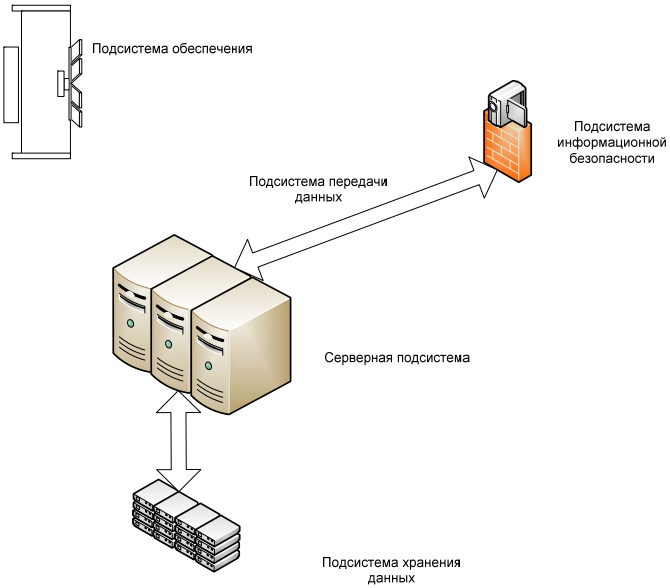


Рис. 1. Схема организации центра обработки данных

На данном этапе необходимо рассмотреть ряд моментов, связанных со спецификой вышеописанных подсистем [2].

Начать стоит с серверной подсистемы. Серверная подсистема может включать в себя совершенно разные серверы — это и серверы приложений, серверы представления информации, серверы информационных ресурсов и служебные серверы.

Серверы приложений — это группа вычислительных машин, которая непосредственно обрабатывает пользовательские данные, циркулирующие в подсистеме хранения.

Серверы предоставления информации отвечают за интерфейс, благоприятный для пользователя при отображении данных, получаемых от серверов приложений.

Серверы информационных ресурсов отвечают за обработку данных и предоставление их серверам приложений.

Служебные серверы — это вспомогательная группа, обеспечивающая биллинг, авторизацию, мониторинг и хранение статистических данных.

Данный многоуровневый принцип построения серверной подсистемы является наиболее целесообразным, так как при таком подходе

может быть достигнута максимальная простота при модернизации и замене в случае неисправности отдельных элементов. При реализации данного принципа необходимо резервирование на всех уровнях по узловому принципу, когда во время выхода из строя одного из элементов без перерыва действия сервиса начинает функционировать резервный элемент. На рис. 2 представлена иллюстрация серверной подсистемы.

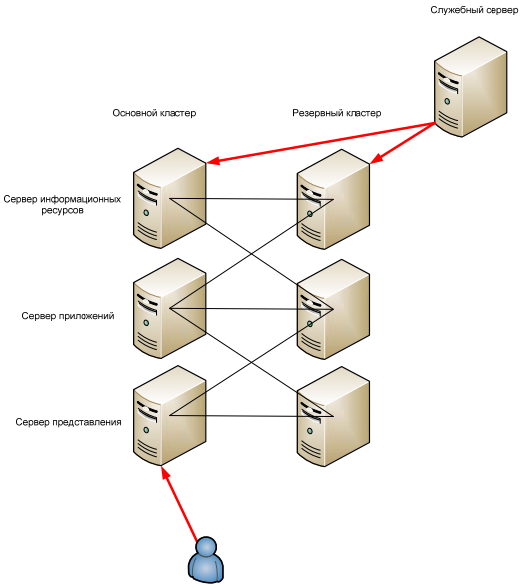


Рис. 2. Организация серверной подсистемы

Подсистема хранения данных — одна из подсистем, к организации которой проявляется особое внимание при проектировании и эксплуатации центров обработки данных. Данная подсистема состоит из ряда компонент. Первая — устройства хранения данных, в качестве которых используются дисковые массивы и ленточные блоки хранения данных, но в настоящее время внедряется и технология Fiber Channel, базирующаяся на волоконно-оптических технологиях. Также среди компонент можно выделить компоненту резервного копирования и резервирования данных. Здесь применяются технологии многоуровневого копирования типа RAID. Необходимо отметить, что в концепции организации центра обработки данных необходимо предусматривать такие механизмы, как

ежедневное резервное копирование на отдельные аппаратные компоненты. Создание так называемого back-up кластера позволит при серьезной техногенной аварии, при которой не будет эффективна система RAID, подобный кластер поможет восстановить данные с некоторой потерей от контрольной точки [2].

Подсистема информационной безопасности — одна из наиболее сложных, как уже было сказано ранее. Подобная система должна быть построена для противодействия и внешним, и внутренним нарушителям. Данная подсистема может состоять из множества компонент, причем эти компоненты могут быть интегрированы в другие подсистемы. При использовании той или иной компоненты необходимо оценивать целесообразность ее использования в каждом конкретном случае. К компонентам относятся: контур охранного видеонаблюдения, против пожарная сигнализация, система контроля и управления доступом, система обнаружения атак на телекоммуникационную инфраструктуру (типа SNORT или СОПКА). Также необходимо внедрять систему межсетевого экранирования и организовывать межсетевое экранирование.

Подсистема эксплуатации — это и компоненты вентиляции и кондиционирования, а также компоненты резервного электропитания. Все компоненты обеспечения необходимы для поддержания режимов штатного функционирования. Отдельно необходимо анализировать микроклимат в помещении центра обработки данных, так как перегрев — наиболее распространенное явление, в результате которого наблюдается выход их строя аппаратуры и оборудования [3].

Подсистема передачи данных строится на базе технологий передачи данных Ethernet различных модификаций.

Необходимо отметить, что организация сетевой инфраструктуры очень важный этап и центры обработки данных могут быть удалены друг от друга на значительные расстояния от нескольких сот метров до десятков километров.

Если на это не обращать должного внимания, то можно нанести серьезный урон и данным, и бизнес-приложениям во время передачи важной информации от сервера к пользователю, либо во время операции создания резервных копий.

В результате написания статьи и проведения исследования были рассмотрены вопросы организации современных центров обработки данных. В исследовании предложено описание структуры центра обработки данных с точки зрения подсистем, каждая из которых была рассмотрена достаточно детально. Цель исследования достигнута и задачи решены.

Библиографический список

1. *Ахо А. В., Хопкрофт Дж. Э., Ульман Дж. Д.* Структуры данных и алгоритмы: учеб. пособие / пер. с англ. и ред. А. А. Минько. М.: Вильямс, 2007.

2. *Крэйг Х.* TCP/IP. Сетевое администрирование: пер. с англ. 3-е изд. СПб.: Символ-Плюс, 2007.

3. *Поляк-Брагинский А. В.* Сеть своими руками. 2-е изд., перераб. и доп. СПб.: БХВ-Петербург, 2004.

С. С. Салтыш, Г. А. Юткин, К. Л. Стойчин, С. В. Поршнев
Уральский федеральный университет имени первого Президента России Б. Н. Ельцина, г. Екатеринбург

Современные проблемы обеспечения информационной безопасности документооборота на предприятии

Аннотация. Рассмотрены основные принципы документооборота на предприятии. Приведена классификация защищаемой в Российской Федерации информации, обозначена актуальность и значимость научной проблемы информационной безопасности документооборота, указаны основные источники угроз, определены носители информации, приведены меры, направленные на защиту информации, циркулирующей в системе документооборота. Описаны возможные угрозы электронному документообороту.

Ключевые слова: документооборот; защищаемая информация; коммерческая тайна; несанкционированный доступ; информационная безопасность; угрозы безопасности информации.

В настоящее время на любом предприятии существуют определенные принципы документооборота. Объем информации, который обрабатывается на современных предприятиях сегодня, велик. Исходя из этого, формируется проблема защиты информации, циркулирующей в данном документообороте. Подобная проблема имеет высокую актуальность, так как несанкционированный доступ к информации предприятия может иметь негативные последствия, вплоть до критических, в результате которых может быть поставлен вопрос о существовании предприятия в целом.

В начале исследования необходимо отметить, что защищаемая информация имеет классификацию с точки зрения законодательства Российской Федерации. Информация, содержащая сведения, составляющие государственную тайну, регулируется отдельными нормативно-правовыми актами, в настоящем исследовании аспекты по ее защите рассматриваться не будут. Помимо нее существуют сведения, составляющие

персональные данные (ПДн) и сведения, составляющие коммерческую тайну [1].

Если в случае сведений, составляющих ПДн, законодательно определены требования по их защите, изложен порядок защиты информации, содержащей сведения, составляющие ПДн в информационных системах обработки персональных данных (ИСПДн), то в отношении коммерческой тайны жесткого регулирования нет. Следовательно, владелец информации, наделивший ее статусом «коммерческая тайна», может применять все возможные и разрешенные законодательством способы к ее защите. Встает вопрос об их необходимом и целесообразном объеме [3].

Цель настоящего исследования — структурирование направлений по защите информации и обеспечению информационной безопасности документооборота на предприятии. Актуальность исследования заключается в определении направлений, по которым необходимо проводить работы по защите информации, циркулирующей в системе документооборота типового предприятия. Результаты исследования могут быть применены в рамках разработки концепции информационной безопасности современного предприятия научно-исследовательского или производственного сектора.

Необходимо помнить, что информация не существует без носителя информации. Информация может быть представлена:

1) в электронном виде и храниться на физических носителях;

2) в виде аналогового или цифрового сигнала и передаваться по каналам и линиям связи, а также циркулировать в рамках корпоративных сегментов вычислительных сетей;

3) в физическом виде на физических носителях;

4) в акустическом или визуальном виде и распространяться при помощи акустических волн или визуального изображения.

На сегодняшний день стандарты защиты информации в основном распространяются на защиту информации в системах электронного документооборота.

На рис. 1 представлена концепция реализации схемы защищенного электронного документооборота на предприятии. На данном рисунке представлен выделенный сегмент, в котором циркулирует защищаемая информация в системе защищенного электронного документооборота. В нем представлены клиентские устройства, являющиеся оконечными пользовательскими терминалами, оборудование коммутации, сервер системы защищенного электронного документооборота, а также некоторое оборудование, являющееся программно-аппаратной защитой и устанавливаемое на границе защищенного контура [4].

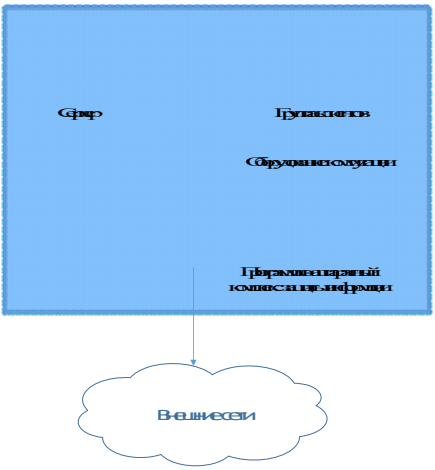


Рис. 1. Концепция реализации схемы
защищенного электронного документооборота на предприятии

На данном этапе исследования необходимо рассмотреть способы защиты системы документооборота в целом и системы электронного документооборота в частности. Существует несколько мер:

1) аппаратно-программные;
2) инженерно-технические;
3) организационно-правовые.

Сейчас целесообразно рассмотреть, каким образом может быть оказано воздействие на систему документооборота предприятия, при котором возникнет инцидент информационной безопасности. Начать следует с физических носителей. При недостаточном внимании к физическим носителям они могут быть похищены либо подменены, поэтому ко всем физическим носителям необходимо применять меры по их учету, также необходимо вводить охранно-режимные меры, благодаря которым хищение не будет возможным. Эти действия относятся к организационно-правовым мерам по защите информации, в частности, циркулирующей в системе документооборота предприятия [5].

Необходимо акцентировать внимание на аппаратно-программных мерах, которые призваны защитить информацию (в основном, при помощи применения криптографии) в электронной системе документооборота и при передаче документов, содержащих конфиденциальную информацию, по каналам и линиям связи. Среди таких мероприятий можно назвать: контроль подключаемых устройств к ресурсам корпоративной

сети, контроль за распечатыванием документов на бумажных носителях из корпоративной сети.

Также стоит обращать внимание на информацию, циркулирующую в акустическом и визуальном виде на объекте защиты. При определенных обстоятельствах она может быть перехвачена устройствами технической разведки. Следует обращать внимание на подобные моменты при планировании концепции информационной безопасности документооборота на предприятии [2]. Возможные угрозы электронному документообороту предприятия приведены на рис. 2.

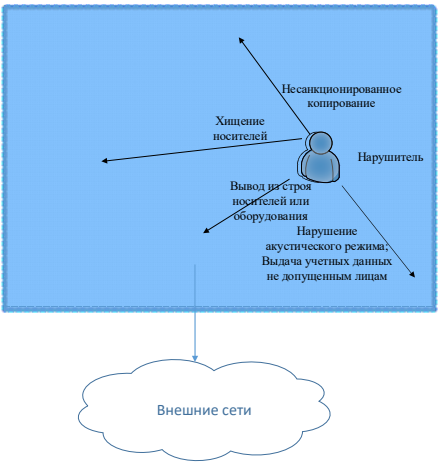


Рис. 2. Возможные угрозы электронному документообороту

В результате написания статьи были затронуты моменты, касающиеся защиты информации документооборота на предприятии. Определена цель и актуальность исследования, сформировано направление дальнейших научных исследований. В настоящей статье были рассмотрены аспекты, затрагивающие в основном информационную безопасность систем электронного документооборота, но общая концепция обеспечения безопасности информации документооборота предприятия является более глобальной научной проблемой, требующей научной проработки.

Библиографический список

1. *Гриняев С. Н.* Поле битвы — киберпространство: теория, приемы, средства, методы и системы ведения информационной войны. Минск, 2004.

2. *Информационная* безопасность: кол. монография / Д. Н. Шакин, Е. Г. Бунев, С. М. Доценко и др. М.: Оружие и технологии, 2009.

3. *Манойло А. В., Петренко А. И., Фролов Д. Б.* Государственная информационная политика в условиях информационно-психологической войны. М., 2009.

4. *Машкин К.* Современные способы и средства распространения материалов информационно-психологического воздействия в ВС США. Часть 1 // Зарубежное военное обозрение. 2009. № 10. URL: http://pentagonus.ru/publ/sovremennye_sposoby_i_sredstva_rasprostranenija_materialov_informacionno_psikhologicheskogo_vozdejstvija_v_vs_ssha_ch1/11-1-0-403.

5. *Прокофьев В. Ф.* К проблеме формирования основных понятий в области информационной безопасности. URL: https://flot.com/publications/books/shelf/safety/18.htm.

М. Р. Кужаева, А. Л. Золкин
Поволжский государственный университет телекоммуникаций и информатики,
г. Самара

Проблемы информационной безопасности в компьютерных сетях

Аннотация. Рассмотрено понятие информационной безопасности, которое может относиться как к отдельным пользователям вычислительной техники, так и к корпорациям. Выяснено, что радикальное решение проблем электронной защиты информации может быть получено только на основе использования криптографических методов, позволяющих решать важнейшие задачи безопасной автоматизированной обработки и передачи данных. Отмечается, что в Республике Казахстан существует законодательная и нормативно-правовая база в области информационной безопасности, основой которой выступает система «Киберщит Казахстана». Даны рекомендации по обеспечению информационной безопасности, которые должен соблюдать каждый сотрудник, имеющий доступ к той или иной информации, так как потеря данных одной информационной цепочки может привести к взлому всей сети. В то же время в Казахстане недостаточно кадров, способных расследовать киберпреступления.

Ключевые слова: информационная безопасность; вычислительная техника; компьютер; криптографический метод; защита информации; информация.

Широкое использование компьютерных технологий в автоматизированных системах обработки информации и управления обострило проблему защиты информации, циркулирующей в компьютерных системах. Защита информации в компьютерных системах имеет ряд особенностей, связанных с тем, что информация не привязана к электронным носителям, она может быть легко и быстро скопирована и передана по каналам связи.

Радикальное решение проблем электронной защиты информации может быть получено только на основе использования криптографиче-

ских методов, позволяющих решать важнейшие задачи безопасной автоматизированной обработки и передачи данных. [1, с. 133]. Проблемы, возникающие с безопасностью передачи информации при работе в компьютерных сетях, можно разделить на три основных типа:

1. Перехват информации — целостность информации сохраняется, но ее конфиденциальность нарушается.

2. Модификация информации — исходное сообщение изменяется или полностью заменяется другим и отправляется получателю.

3. Смена авторства информации. Эта проблема может иметь серьезные последствия. Например, кто-то может отправить письмо от чужого имени (этот тип обмана обычно называется спуфингом) или веб-сервер может выдать себя за электронный магазин, принимать заказы, номера кредитных карт, но не отправлять товары. [2, с. 101].

С развитием информационных коммуникаций одновременно появляется возможность повреждения информации, хранящейся и передаваемой с их помощью, в связи с чем проблема информационной безопасности существующих систем хранения, передачи и обработки информации сейчас актуальна для общества [3, с. 92].

Информационная безопасность в Республике Казахстан подразумевает защиту информации и всей организации от преднамеренных или случайных действий, ведущих к причинению вреда ее владельцам или пользователям, при этом обеспечение информационной безопасности должно быть направлено в первую очередь на предотвращение рисков, а не на устранение их последствий.

Законодательные меры в сфере информационной безопасности направлены на создание в стране законодательной базы, которая рационализирует и регулирует поведение субъектов и объектов информационных отношений, а также определяет ответственность за нарушение установленных норм.

Существует следующая законодательная база в этой области: законы Республики Казахстан в области информационной безопасности: «О национальной безопасности», «Об информатизации», «О государственных секретах», «О персональных данных и их защите», «Об электронном документе и электронной цифровой подписи», «О связи», Уголовный кодекс Республики Казахстан, Кодекс Республики Казахстан «Об административных правонарушениях», Единые требования в области информационно-коммуникационных технологий и обеспечения информационной безопасности, Концепция кибербезопасности («Киберщит Казахстана»)[1].

[1] *Об утверждении* Концепции кибербезопасности («Киберщит Казахстана»). URL: http://adilet.zan.kz/rus/docs/P1700000407.

Таким образом, информационная безопасность — это прежде всего безопасность информационного пространства, которая включает в себя защиту прав и интересов человека и гражданина, общества и государства в информационной сфере от реальных и потенциальных угроз[1].

Тем не менее, проведя анализ общедоступной информации в интернете, было выявлено, существуют различные проблемы, связанные с информационной безопасностью жителей Казахстана, самая частая — утечка информации. Пользователи интернета часто попадаются на уловки мошенников, которые крадут реквизиты банковских карт, пароли и т.д. Основная причина — низкая осведомленность населения по поводу информационной безопасности.

Проблемы информационной безопасности затронули и крупные компании Казахстана, так, например, 28 октября 2020 г. на казахстанский банк «Каспи» была совершена кибератака. Хакерам удалось украсть 78 млн тенге. Преступники нашли уязвимости на сайте и в мобильном приложении банка, что позволило списать данную сумму со счетов. Помимо кражи денег, хакерская атака приостановила работу всех информационных ресурсов банка. Мобильное приложение не работало около суток.

27 марта 2017 г. с подобной атакой столкнулся и Нурбанк, но сотрудники по информационной безопасности очень быстро среагировали, что позволило избежать потерь как со стороны банка, так и со стороны его клиентов.

Одним из самых популярных методов информационной атаки на физических лиц в Казахстане является фишинг банковских карточек. С недавнего времени большинство банковских карт имеют возможность оплачивать покупки через Wi-Fi. Мошенники используют специальные устройства, которые могут воровать на определенном расстоянии данные карт, что позволяет им воровать денежные средства.

Специалисты утверждают, что внутренние органы не до конца готовы бороться с данной проблемой, если физические и юридические лица заявляют о информационном преступлении, то в большинстве случаев правоохранительные органы не знают в каком направлении решать проблему. В результате, проблема либо решается очень поздно, либо ее вовсе не удается решить.

Защита информации в сетях и вычислительных средствах с помощью технических средств осуществляется на основе организации доступа к памяти [4, с. 91]. Для того чтобы обезопасить народ от утечки

[1] *Как* в Казахстане обеспечивают кибербезопасность. URL: https://zakon-kz.turbopages.org/zakon.kz/s/4959961-kak-v-kazahstane-obespechivayut.html.

личной информации, платежных реквизитов, паролей и т.д., уполномоченные органы Республики Казахстан по информационной безопасности должны предоставлять все необходимую информацию населению, люди должны знать, как обезопасить себя от мошеннических действий в сети интернет, а также уметь надежно защищать личную информацию, которая хранится на компьютерах, смартфонах и другой цифровой технике.

Также Казахстану необходимы специалисты в правоохранительных органах, способные решать вопросы по информационной безопасности за короткие промежуток времени.

Основной проблемой является нехватка персонала, который разбирается в информационной безопасности в правоохранительных органах. Необходимо использовать международный опыт расследования преступлений. Так, например, в США 7 из 10 преступлений, связанных с киберпреступностью, раскрываются. Для сравнения, в Казахстане — 2 из 10.

В связи с широким использованием современных информационных технологий, криптография становится незаменимым инструментом защиты информации. Использование электронных платежей, возможность передачи секретной информации через открытые сети связи, а также решение большого количества других задач информационной безопасности в компьютерных системах и информационных сетях основаны на криптографических методах.

Республике Казахстан необходимо обеспечение необходимыми кадрами, которые способны расследовать подобные преступления, так как на данный момент полиция работает с информационными преступлениями не должным образом, раскрытие преступлений в области информационной безопасности имеет очень низкий уровень, в сравнении со странами Запада, где существуют специализированные отделы по борьбе с киберпреступностью.

Библиографический список

1. *Аутентификация.* Теория и практика обеспечения безопасного доступа к информационным ресурсам: учеб. пособие для вузов / А. А. Афанасьев, Л. Т. Веденьев, А. А. Воронцов и др.; под ред. А.А. Шелупанова, С.Л. Груздева, Ю.С. Нахаева. 2-е изд., стер. М.: Горячая линия – Телеком, 2012.

2. *Васильков А. В., Васильков И. А*. Безопасность и управление доступом в информационных системах. М.: Форум, 2015.

3. *Запечников С. В., Милославская Н. Г., Толстой А. И., Ушаков Д. В.* Информационная безопасность открытых систем: в 2 т. М.: Машиностроение, 2016. Т. 1. Угрозы, уязвимости, атаки и подходы к защите.

4. *Ярочкин В. И.* Безопасность информационных систем. М.: Ось-89, 2016.

Д. А. Москаленко, Ю. Ю. Чернышов
Уральский государственный университет путей сообщения, г. Екатеринбург

Актуальная угроза информационной системы

Аннотация. В некоторых случаях злоумышленникам не требуется взламывать информационный ресурс для получения полезной информации. Это могут сделать легитимные пользователи с помощью такого инструмента, как фишинг. В статье отмечается отсутствие актуальных инструментов защиты против данной угрозы.

Ключевые слова: фишинг; УБИ.17; социальная инженерия; информационная безопасность; защита информации.

Актуальной угрозой любой информационной системы является фишинг, в силу того, что одной из составляющих частей информационной системы является человек. И этот человек выступает в качестве отмычки к системе безопасности информационной системы для получения полезной информации.

С каждым годом данная угроза набирает популярность у злоумышленников. В 2020 г. это особенно ярко выраженно из-за пандемии. Это объясняется тем, что для реализации данной угрозы не нужно быть технический подкованным, а достаточно понимать психологию человека, его интересы, работу и окружение. Злоумышленнику проще сблизиться с жертвой, чем искать уязвимости в системе безопасности.

Всего за I квартал 2020 г. защитные решения обнаружили 49 562 670 вредоносных почтовых вложений, что практически идентично показателю прошлого отчетного периода: в IV квартале 2019 г. было выявлено на 314 862 вредоносных вложений больше. Количество вредоносного вложения можно наглядно увидеть на рис. 1.

В I квартале 2020 г. с помощью системы «Антифишинг» предотвращено 119 115 577 попыток перехода пользователей на мошеннические страницы. Процент уникальных атакованных пользователей составил 8,8% от общего количества пользователей продуктов «Лаборатории Касперского» в мире.

По оценке аналитиков Group-IB, только по Российской Федерации в сумме составляет 510 млн руб. за период со второй половины 2018 г. по первую половину 2019 г., не говоря уже про репетиционный ущерб, а если рассмотреть мировые масштабы, то суммы доходят до миллиардов долларов. Как можно заметить на рис. 2, фишинг хотя и имеет наименьшую среднюю сумму одного хищения, но общее число успешных атак, а также количество группировок, занимающихся им, наибольшее.

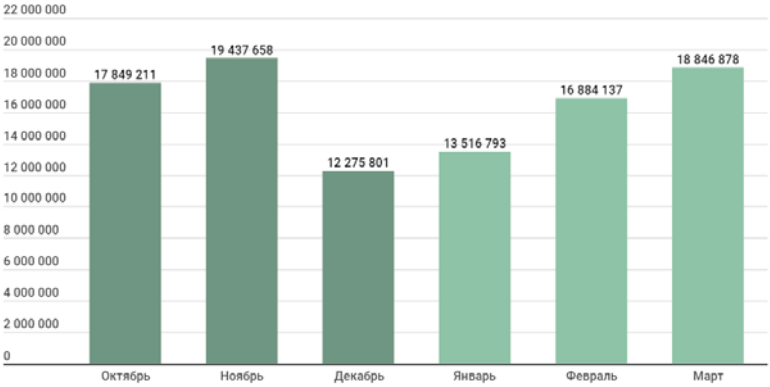


Рис. 1. Семейства вредоносных программ

Рис. 2. Оценка Group-IB рынка высокотехнологичных преступлении в финансовой отрасли России

В 2020 г. начиная с середины марта киберпреступники запустили множество тематических фишинговых и вредоносных атак COVID-19 против работников, учреждений здравоохранения и недавно безработных. Количество фишинговых сайтов, обнаруженных в первом квартале 2020 г., составило 165 772, по сравнению с 162 155, наблюдаемыми в четвертом квартале 2019 г. Теперь злоумышленники более качественные подделки. Некоторые случаи фишинга, о которых сообщают крупные хостинг-провайдеры, могут оставаться без внимания в течение нескольких месяцев.

Все риски по банковским картам связаны с различными механизмами их использования. Это усложняется тем, что с каждым годом злоумышленники придумывают новые мошеннические схемы кражи денежных средств. В классической схеме (рис. 3) злоумышленник отправляет сообщение пользователю сети Интернет с предложением перейти на фишинговый сайт, визуально напоминающий оригинальный известный сайт. Пользователь вводит на поддельном сайте свои персональные данные. Далее злоумышленник для получения одноразового пароля, который приходит пользователю на телефон, звонит пользователю, представляясь сотрудником банка, с просьбой сообщить одноразовый пароль.

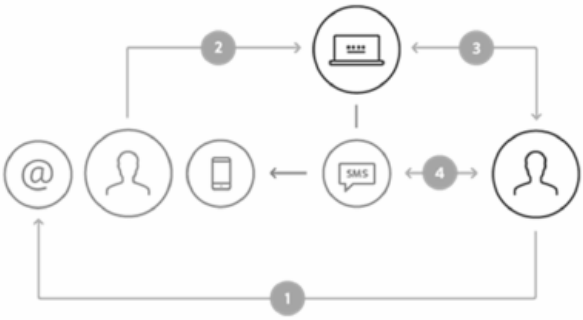


Рис. 3. Классическая схема фишинга

Похитив все данные, злоумышленник получает полный доступ к личному кабинету пользователя. Во втором случае, вирусное ПО заражает мобильное устройство пользователя таким образом, что при переходе на сайт банка вирус перенаправляет пользователя на фишинговый сайт, имитирующий сайт банка (рис. 4). На фишинговом сайте пользователю предлагается ввести персональные данные, необходимые для входа

в личный кабинет, а также предлагается скачать приложение от банка, которое после установки будет пересылать все данные злоумышленнику.

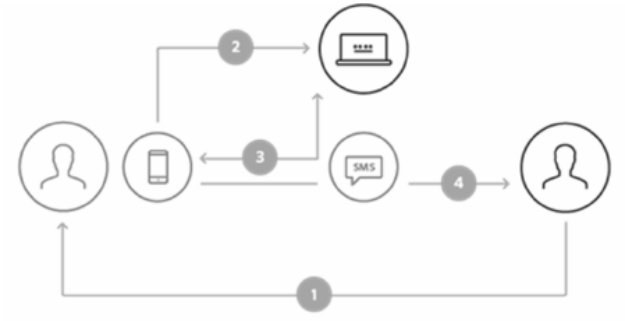


Рис. 4. Фишинг для мобильных устройств

Количество предоставления банковских услуг только растет, в том числе выпуск банковских карт (рис. 5), различные механизмы взаимодействия производителя и потребителя. Поэтому для избегания реализации перечисленных рисков не только производителю стоит принимать меры по минимизации рисков, но и потребителю стоит стремится соблюдать рекомендации производителей по безопасной эксплуатации своих продуктов и услуг.

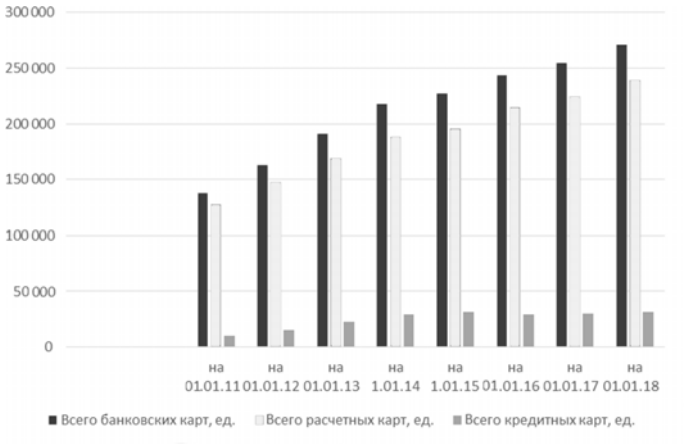


Рис. 5. Динамика выпущенных банковских карт, тыс. ед.

На сегодняшний день компания Google разместила объявление о фишинге на их почтовом сервисе. В объявлении сообщается, что ежедневно сервис блокирует около 18 млн электронных сообщений, которые связаны с новой коронавирусной инфекцией и содержат в себе фишинговые ссылки.

На сегоднейшний день единственное упоминание фишинга в законодательстве РФ присутствует только в банке данных угроз ФСТЭК — УБИ.175, которое не дает достаточное понимание угрозы за счет неполноты ее раскрытия. Согласно описанию угрозы:

Данная угроза заключается в возможности неправомерного ознакомления нарушителем с защищаемой информацией, в том числе идентификация и аутентификация пользователя путем убеждения его с помощью методов социальной инженерии.

Существует несколько видов фишинговых атак:

1) посылка целевых писем (spear-phishing attack), с помощью звонков с вопросом об открытии вложения письма;

2) имитация рекламных предложений (fake offers);

3) различные приложения (fake apps).

Все эти методы предполагают, что дискредитируемый пользователь зайдет на поддельный сайт (выглядящий одинаково с оригинальным), на котором от дискредитируемого пользователя требуется ввести защищаемую информацию или открыть зараженное вложение в письме.

Разработано множество способов защиты против фишинга: различного рода инструкции, ответственность и многое другое. Но никакого рода организационные меры не помогут защититься от злоумышленника, если он действительно заинтересован в этом. Т.е. есть фишинг осуществляется не на «случайную жертву» сети Интернет, а на конкретное лицо или группу лиц. В ходе исследования рынка по защите информации было выделено несколько действующих способов.

Использовать встроенное ПО, которое будет осуществлять сканирование URL-ссылок, а также проверку их на фишинг в случае обнаружения данной угрозы, и блокировать их.

Другой метод — автоматизация процессов. Он подразумевает разбить ИС на сегменты и защищать каждый по отдельности. Тем самым у каждого сегмента будет своя группа администраторов и свой уровень доступа к каждому сегменту. Также данный метод подразумевает автоматизацию процессов с помощью «идеальных инструментов». Под «идеальными инструментами» понимается некоторый инструмент, который не требует вмешательства человека в процесс. С помощью такого метода можно явно отследить, где произошла утечка информации и кто

это допустил, так как логирование и мониторинг происходит во всех сегментах ИС по отдельности.

Е. П. Пономарева, А. Л. Золкин
Поволжский государственный университет телекоммуникаций и информатики,
г. Самара

Анализ вопросов обеспечения безопасности корпоративных коммуникационных систем и мер по предотвращению утечки информации

Аннотация. Рассмотрены основные причины и методы несанкционированного проникновения в корпоративную сеть. Проведен анализ мер обеспечения безопасности коммуникационных систем, рассмотрены меры по обеспечению защиты от утечки информации.

Ключевые слова: корпоративные вычислительные сети; информационная безопасность; киберпреступление; хакер; программное обеспечение.

Система обеспечения информационной безопасности — неотъемлемая часть корпоративной компании, защищающая интересы собственников и пользователей. Разглашение конфиденциальной информации может стать причиной множества трудностей организации. Для обеспечения безопасности информации необходимо иметь представление о возможных инцидентах утечки информации. Ущерб может быть нанесен не только в связи с несанкционированным доступом к информации сторонним недоброжелателем, но также и сотрудниками компании.

Существует несколько методов взлома корпоративных вычислительных сетей, а также несколько способов предотвращения утечки информации.

Чтобы взломать корпоративную сеть, необходимо получить доступ к узлу, подключенному к внутренней сети. Причинами несанкционированного проникновения могут стать следующие уязвимости:

— дефекты в области управления учетными записями и паролями;

— незащищенность веб-приложений;

— дефекты фильтрации трафика;

— дефекты управления уязвимостями и обновлениями;

— неосведомленность пользователей в вопросах информационной безопасности;

— дефекты конфигурации и разграничения доступа.

В отдельных пентестах хотя бы одна из вышеперечисленных уязвимостей могла стать причиной взлома корпоративной вычислительной сети.

Существует множество сценариев, согласно которым недоброжелатели могут получить доступ к сети. Рассмотрим следующие из них[1]:

— подбор учетных данных;

— эксплуатация веб-уязвимостей;

— эксплуатация известных уязвимостей;

— социальная инженерия;

— открытые данные.

Существуют следующие основные способы предотвращения утечки информации.

1. В целях предотвращения сценария по подбору учетных данных следует применять авторизацию по приватному ключу. Необходимо осуществить настройку по ограничению доступа к узлам подключения по протоколам удаленного управления. Это значит, что нужно разрешать подключения лишь из внутренней сети и лишь определенному количеству администраторов. В целях исключения вероятности по установлению элементарных паролей требуется утвердить парольную политику. VPN лучше всего применять в случае необходимости администрирования ресурсов в удаленном режиме[2].

2. В целях предотвращения сценария по эксплуатации веб-уязвимостей кроме введения парольной политики, рекомендуется вводить белые списки для проверки файлов, которые загружаются на сервер. Для того, чтобы защитить код приложения от эксплуатации уязвимостей нужно фильтровать пересылаемые пользователями сети данные. Эти данные следует фильтровать на уровне кода приложения. Межсетевой экран уровня приложения (webapplicationfirewall) также хорошо послужит для предотвращения сценария по эксплуатации веб-уязвимостей[3].

3. В целях предотвращения сценария по эксплуатации известных уязвимостей можно использовать частое обновление ПО, обновление безопасности для ОС и применять трудные для взлома пароли. Кроме того, интерфейсы не должны быть общедоступны из внешних сетей. Информация по версии веб-серверов должна быть закрыта.

4. В целях предотвращения сценария по социальной инженерии следует отметить, что сотрудники могут самостоятельно выявлять часть производимых атак. Главное условие — это внимательность сотрудни-

---

[1] *Гнедин Е.* Сценарий для взлома. Разбираем типовые сценарии атак на корпоративные сети. URL: https://xakep.ru/2017/04/10/hacking-attack-types/#toc03.

[2] Публичная страница. URL: https://forum.antichat.ru/forum113.html — Форум АНТИЧАТ > Безопасность и Уязвимости > Беспроводные технологии/Wi-Fi/Wardriving.

[3] *Варлатая С. К., Рогова О. С., Юрьев Д. Р.* Анализ методов защиты беспроводной сети Wi-Fi от известных способов взлома злоумышленником // Молодой ученый. 2015. № 1 (81). С. 36–37.

ков компании. В этом случае сотрудники самостоятельно могут проверять адрес отправителя и не заходить на сомнительные ссылки и прилагающиеся к письмам файлы. Помимо этого, большую роль сыграет неразглашение сотрудников компании своих учетных данных даже сотрудникам службы безопасности и администраторам.

5. Еще одним вариантом решения проблемы становится назначение в компании доверенного лица, от которого могут присылаться письма.

6. Несомненно, использование антивирусов тоже в силах помочь в решении данного вопроса.

7. В целях предотвращения сценария по открытым данным администраторы систем должны осуществлять наблюдение за тем, какие данные доступны на страницах веб-ресурсов. Они также должны обеспечивать разграничение доступа к директориям на серверах и файлам, которые могут быть доступны из внешних сетей.

В заключение необходимо сделать вывод о том, что невозможно описать все возможные сценарии атак злоумышленниками, хотя они, безусловно, основываются на вышеперечисленных принципах. Утечка информации — серьезная проблема для большинства организаций[1].

По проведенному исследованию также можно сделать вывод о том, что любой вид атаки можно предотвратить вышеперечисленными методами:

1) авторизация по приватному ключу;
2) введение парольной политики;
3) частое обновление ПО, обновление безопасности для ОС и применение трудных для взлома паролей;
4) неразглашение сотрудниками компании своих учетных данных;
5) использование антивирусов;
6) назначение доверенного лица;
7) наблюдение и разграничение доступа к серверу администраторами.

[1] *Способы* предотвращения утечки информации. URL: https://searchinform.ru/analitika-v-oblasti-ib/utechk.

К. М. Саматов
Уральский государственный экономический университет, г. Екатеринбург

Типовые ошибки в реализации закона о безопасности критической информационной инфраструктуры

Аннотация. Рассматриваются основные ошибки, которые возникают у субъектов в ходе реализации закона о безопасности критической информационной инфраструктуры (КИИ) и создании системы безопасности значимых объектов КИИ.

Ключевые слова: критическая информационная инфраструктура; безопасность; система обеспечения безопасности.

С момента вступления в законную силу Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»[1] прошло уже более двух лет, но далеко не все организации могут похвастаться успехами в его выполнении. На практике, специалисты, занимающиеся обеспечением безопасности объектов критической информационной инфраструктуры, рисуют приблизительно следующую картину (дорожную карту) по выполнению требований действующего законодательства в указанной сфере (см. рисунок).

Первое, что сразу бросается в глаза при анализе дорожной карты, это то, что категорирование объектов КИИ разделяется на два самостоятельных этапа. На практике, большинство субъектов КИИ действительно так и делают: создают комиссию, начинают процедуру категорирования, а затем выясняют, что к субъектам КИИ они не относятся.

По мнению автора, приступать к реализации 187-ФЗ необходимо с анализа учредительных документов и определения функционирует ли организация (государственный орган, учреждение) в одной из перечисленных в законе сферах. Иными словам, первым этапом будет не категорирование, а «самоидентификация» в качестве субъекта КИИ, уже после которой создание комиссии и проведение процедуры категорирования объектов КИИ. Если в ходе «самоидентификации» установлено, что организация функционирует в одной из 12 сфер[2], целесообразно разработать дорожную карту по реализации в организации требований 187-ФЗ[3].

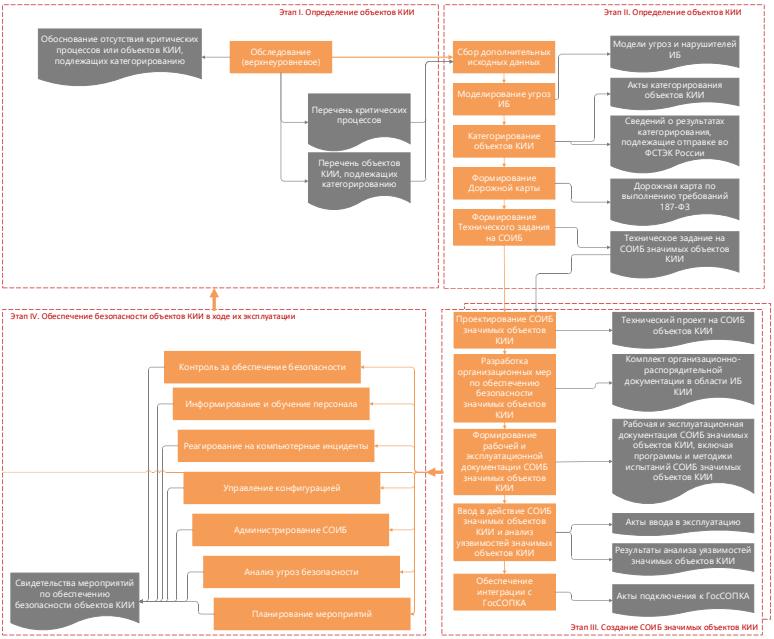
---

[1] Далее по тексту вместо полного названия Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» используется сокращение «187-ФЗ», вместо критическая информационная инфраструктура используется сокращение «КИИ».

[2] Порядок ведения реестра значимых объектов КИИ (утв. приказом ФСТЭК России от 6 декабря 2017 г. № 227) выделяет 12 сфер.

[3] С учетом принятых во исполнение данного Федерального закона подзаконных нормативно-правовых актов.

Следует отметить, что дорожная карта не является планом проекта, а представляет собой некий прогноз действий, могущих привести к достижению цели, а, следовательно, разрабатывается именно в начале пути, а не в середине, как указано на рисунке.



Дорожная карта глазами субъекта КИИ

После же проведения процедуры категорирования целесообразно разработать план проекта по созданию системы обеспечения информационной безопасности (СОИБ) объектов (значимых объектов) КИИ с указанием результата, сроков и ресурсов.

Еще одной характерной ошибкой, является разработка моделей угроз на этапе категорирования. На этапе категорирования происходит анализу угроз безопасности и возможных действий нарушителей (см. пп. «г», «д» п. 14 Правил категорирования объектов критической информационной инфраструктуры Российской Федерации (утв. постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 127), результаты которого отражаются в разделе 6 Сведений о результатах присвоения объекту критической информационной инфраструктуры одной

из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий.

Разработка же моделей угроз, осуществляется на этапе создания СОИБ объектов (значимых объектов) КИИ (см. п. 11 Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации (утв. приказом ФСТЭК России от 25 декабря 2017 г. № 239)), который начинается с установления требований к обеспечению безопасности объекта (значимого объекта) КИИ (см. п. 10 Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации) и формирования технического задания. На основе технического задания, с учетом моделей угроз и нарушителей, производится проектирование СОИБ (технический проект), а также разработка рабочей (эксплуатационной) документации.

На этом заканчивается техническое проектирование и начинается внедрение организационных и технических мер СОИБ: установка и настройка средств защиты информации, разработка организационно-распорядительных документов, предварительные, опытные и приемочные испытания, ввод в эксплуатацию.

Отдельным этапом, по мнению автора следует выделить взаимодействие с Государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА), так как:

— его обязаны осуществлять в том числе и те субъекты, у которых нет значимых объектов КИИ и которые приняли решение не создавать СОИБ (субъект КИИ может принять решение о создании СОИБ в том числе и для объектов КИИ не имеющих категории значимости);

— оно может осуществляться и без интеграции с технической инфраструктурой Национального координационного центра по компьютерным инцидентам (на сегодняшний день);

— набор мероприятий может быть различным: от простого внесения изменений в регламент по реагированию на инциденты информационной безопасности, до создания целой структуры — корпоративного (ведомственного) центра ГосСОПКА.

Поэтому, взаимодействие с ГосСОПКА необходимо рассматривать как отдельный этап, идущий параллельно созданию СОИБ.

Следующим этапом в реализации требований 187-ФЗ является обеспечение безопасности объекта (значимого объекта) КИИ в ходе его эксплуатации. На данном этапе заканчивается проект по созданию СОИБ и начинаются процессы по обеспечению ее функционирования,

а, соответственно, меняются и подходы. Так, Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации обязуют субъекта КИИ применять модель «Планирование (Plan) - Осуществление (Do) - Проверка (Check) - Действие (Act)» (PDCA) для обеспечения безопасности в ходе эксплуатации объекта (значимого объекта) КИИ. Иными словами, субъект КИИ должен внедрить (интегрировать в бизнес-процессы организации) данные процессы в соответствии с требованиями утвержденными приказами ФСТЭК России от 21 декабря 2017 г. № 235 и от 25 декабря 2017 г. № 239 (см. таблицу).

Процессы по обеспечению функционирования СОИБ

Наименование процесса	Описание основных действий
Планирование	Ежегодное планирование мероприятий по обеспечению информационной безопасности. Отдельное планирование мероприятий по повышению осведомленности персонала (рекомендация автора)
Осуществление	Реализация мероприятий в соответствии с планом
Проверка (мониторинг и контроль)	Мониторинг состояния информационной безопасности (постоянный). Периодические аудиты (не реже чем раз в три года, лучше раз в год)
Действие (совершенствование)	Совершенствование процессов обеспечения информационной безопасности, повышение их зрелости

Нельзя не отметить также, что на рисунке полностью отсутствует этап вывода объекта КИИ из эксплуатации. Психологически это понятно, стоит задача что-то создать (построить), а не ликвидировать. Но для целостного видения картины учесть данный этап необходимо.

М. А. Хохлов
Финансовый университет при Правительстве РФ, г. Москва

Анализ организационного и правового обеспечения информационной безопасности в Российской Федерации

Аннотация. Рассматриваются основные аспекты организационного и правового регулирования информационной безопасности, выделяются направления и функции организационного обеспечения данной сферы.

Ключевые слова: информационная безопасность; организационное обеспечение; правовое регулирование; доктрина информационной безопасности РФ.

Развитая информационная структура является одним из важнейших факторов функционирования современного общества. Информация проникает во все сферы деятельности государства и несет в себе самое разное выражение. Это обусловливает актуальность обеспечения информационной безопасности РФ, так как защита информации — это одно из приоритетных направлений национальной политики.

Государственная политика РФ, направленная на обеспечение информационной безопасности, может быть реализована посредством законотворчества, правоохранительной деятельности и участия государства в развитии правосознания и правовой культуры граждан. В публикации свода законов СССР 1970-х гг. было систематизировано 29 тыс. действующих законов и более миллиона подзаконных актов и нормативных актов, при этом 120 профсоюзных министерств и ведомств издали до 300 таких актов в год. За последние 10 лет в России было принято более 1000 законов, что намного выше, чем предыдущий уровень законотворчества. В последние годы российское законодательство существенно обновлено [2].

Одним из основных документов в области обеспечения информационной безопасности является «Доктрина информационной безопасности Российской Федерации о состоянии и совершенствовании правовых отношений в информационной сфере», которая представляет собой документ, содержащий официально принятую в Российской Федерации систему взглядов на проблемы по обеспечению информационной безопасности, средства и методы защиты жизненно важных интересов общества, личности, государства в информационной сфере [1].

В системе безопасности Российской Федерации определены следующие основные направления информационной безопасности[1]:

[1] *Доктрина* информационной безопасности Российской Федерации о состоянии и совершенствовании правовых отношений в информационной сфере. URL: URL: http://www.scrf.gov.ru/documents/6/5.html.

— разграничение уровней правового регулирования проблем обеспечения информационной безопасности на законодательном уровне — существуют уровень субъекта федерации, федеральный уровень и уровень местного самоуправления;

— создание нормативной базы для того, чтобы развивать систему страхования информационных рисков, которая будет обеспечивать страховую защиту не только пользователей информационных услуг, но и организаций, которые данные услуги предоставляют;

— закрепление на законодательном уровне приоритета развития отечественных сетей связи и производства спутниковой связи;

— разработка национальной программы развития общедоступных компьютерных сетей, которая включает в себя правовое регулирование деятельности провайдеров интернет-услуг, защиту русского языка в сети Интернет, а также предоставление в сети информации о том, как работают государственные органы и т.д.;

— создание правовой базы для функционирования на отечественном пространстве системы региональных центров с целью обеспечения информационной безопасности.

Согласно «Доктрине информационной безопасности Российской Федерации о состоянии и совершенствовании правовых отношений в информационной сфере», основными функциями системы организационного обеспечения информационной безопасности являются:

— разработка основных положений нормативной правовой базы в данной сфере;

— создание оптимальных условий и организационных мероприятий для выполнения реализации прав общественных объединений и граждан на разрешенную законом Российской Федерации деятельность в информационной сфере;

— необходимость поддержания баланса между потребностями граждан в свободном использовании информации и ограничениями, направленными на ее распространение;

— оценивание состояния сферы информационной безопасности в РФ с целью выявления определенных источников разнообразных угроз информационной безопасности для того, чтобы найти приоритетные направления по их предотвращению и нейтрализации;

— организация и координация деятельности федеральных органов государственной власти и других государственных органов, которые решают задачи по обеспечению информационной безопасности в Российской Федерации;

— организация контроля за тем, как осуществляется деятельность органов государственной власти субъектов Российской Федерации и фе-

деральных органов государственной власти, государственных и межведомственных комиссий, решающих задачи обеспечения информационной безопасности;

— организация разработки федеральных и региональных программ по обеспечению информационной безопасности и выполнение координации деятельности по их реализации;

— обеспечение предупреждения, выявления и пресечения правонарушений, которые связаны с посягательствами на законные интересы граждан Российской Федерации, государства и общества в информационной сфере, на выполнение судопроизводства по делам, связанным с преступлениями в области информационной безопасности;

— организация фундаментальных и обеспечение прикладных научных исследований в области организации обеспечения информационной безопасности;

— осуществление мероприятий по единой технической политике в области обеспечения информационной безопасности;

— развитие и совершенствование целостной системы по подготовке кадров, которые необходимы в области обеспечения информационной безопасности;

— развитие не только российской информационной инфраструктуры, но также и индустрии информационных средств, работа над повышением их конкурентоспособности на рынке ИТ;

— выполнение обеспечения мероприятий по контролю над созданием и использованием средств необходимых для защиты информации посредством реализации программ обязательного лицензирования выполняемой деятельности в сфере обеспечения информационной безопасности и сертификации средств защиты информации;

— защита государственных информационных ресурсов;

— международное сотрудничество в сфере обеспечения информационной безопасности.

Правовое регулирование всех органов, входящих в состав системы, осуществляется при помощи федеральных законов и нормативно-правовых актов Президента и Правительства РФ. Функции данных органов определяются посредством отдельных нормативно-правовых актов РФ.

Таким образом, можно сказать, что информационная безопасность определяется возможностью нейтрализации воздействия в отношении к опасным факторам.

В заключение следует сказать, что информационная безопасность РФ — основная составляющая национальной безопасности страны, что напрямую влияет на эффективность работы органов государственной власти и является важнейшим фактором борьбы с мировым терроризмом и организованной преступностью.

Внедрение современных технологий и законодательной базы для защиты государственных секретов должно стать мощным звеном в укреплении вертикали власти в России и ее становлении как экономически и политически сильного государства на мировой арене.

Библиографический список

1. *Партыка Т. Л., Попов И. И.* Информационная безопасность: учеб. пособие. М.: Форум, 2012.

2. *Петров С. В., Слинькова И. П., Гафнер В. В.* Информационная безопасность: учеб. пособие. М.: АРТА, 2012.

Г. А. Юткин, С. А. Булатов, К. Л. Стойчин, С. В. Поршнев

Уральский федеральный университет имени первого Президента России Б. Н. Ельцина, г. Екатеринбург

Проблемы защиты телекоммуникационной структуры интернет-провайдера от внешних угроз

Аннотация. Описана архитектура, схема атак и угрозы, влияющие на функционирование корпоративной сети.

Ключевые слова: корпоративная сеть; архитектура; трафик; сервер; коммутатор; межсетевой экран; демилитаризованная зона.

Сегодня корпоративные сети — основа современного общества. Благодаря сетевым технологиям у сотрудников появилась возможность совместно работать над проектами в много пользовательском режиме, у студентов — дистанционно обучаться, у близких людей — общаться с использованием видеосвязи ультравысокого качества. При помощи технологий связи, являющихся основой корпоративных сетей, клиент банка может сделать перевод, не выходя из дома. И это далеко не все преимущества сетей связи и корпоративных сетей.

Организация корпоративных сетей — одна из приоритетных задач любой организации, желающей осуществлять эффективную деятельность и быть конкурентоспособной. Но наряду с огромным количеством преимуществ существует также и ряд недостатков. Одним из наиболее ярким из них являются проблемы безопасности корпоративных сетей. Настоящая статья будет посвящена обзору основных характеристик и определению требований, необходимых для обеспечения безопасности сетей. Актуальность данной статьи достаточно велика, так как при недооценке угроз безопасности корпоративной сети может произойти

успешный инцидент атаки на данную сеть, и злоумышленник получит нелегитимный доступ к ее ресурсам или режимам работы.

Современные корпоративные сети имеют определенную архитектуру. На данном этапе исследования необходимо проанализировать ее. Сама корпоративная сеть — это совокупность устройств различного уровня эталонной модели взаимодействия открытых систем (ЭМ ВОЗ) и среды передачи данных. В качестве устройств могут выступать: на втором уровне — коммутаторы, на третьем — маршрутизаторы, на четвертом — межсетевые экраны. Корпоративные сети имеют адресацию устройств, подавляющее большинство данных сетей строятся по следующим принципам: на канальном уровне работает протокол Ethernet и адресация идет в соответствии с физическим адресом оборудования (MAC-адресом). Далее, на следующем уровне, сетевом, работает протокол IP, и, соответственно, происходит IP-адресация устройств. Современные корпоративные сети имеют определенную систему адресации. Например, существуют сети, работающие в одноранговом диапазоне (когда все адреса подсети принадлежат одной сети). Также существуют сети, которые требуют маршрутизации между подсетями (неодноранговые сети). На рис. 1 приведен пример одноранговой сети, имеющей в своем составе коммутаторы, пользовательские компьютеры и серверы.

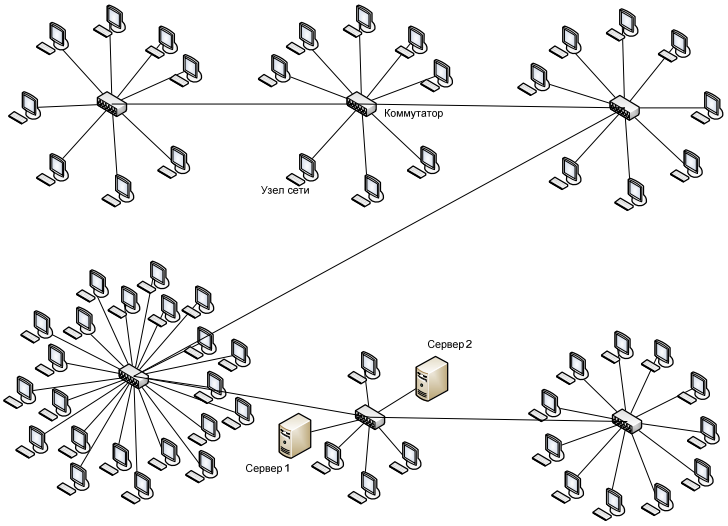


Рис. 1. Одноранговая корпоративная сеть

В рамках применения корпоративной сети происходит разделение коммутаторов на коммутаторы доступа, ядра сети и агрегации. В настоящем исследовании данные понятия рассматриваться не будут, так как любой коммутатор имеет одни и те же уязвимости вне зависимости от принадлежности [1].

Маршрутизатор стоит на границе сегмента корпоративной сети, он содержит таблицы маршрутизации и вычисляет адресата доставки информации. Защита трафика корпоративной сети — задача межсетевого экрана. Подобные устройства очень часто стоят на границе демилитаризованной зоны и общедоступной сети «Интернет». Часто встречается случай, когда для построения корпоративной сети используется архитектура с двумя межсетевыми экранами, одни из которых имеет более жесткие настройки, а второй — менее жесткие.

В корпоративных сетях очень часто используется такая площадка, как демилитаризованная зона. Это пространство, которое содержит общедоступные сервисы, например, web-сайт, реализованный на базе web-сервера. Демилитаризованная зона создается при использовании такого принципа, как построение сети на базе двух межсетевых экранов. На рис. 2 приведен пример демилитаризованной зоны[1].

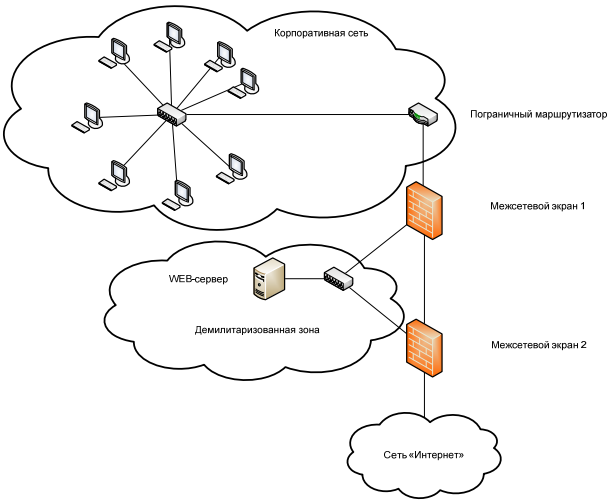


Рис. 2. Демилитаризованная зона корпоративной сети

[1] *Безопасность* WEB. Риски и их предотвращение // Системы безопасности. 2015. № 2.

Необходимо понимать, что пользователи, действующие с целью похищения данных, могут работать удаленно. Также удаленно могут осуществлять деятельность и инсайдеры. Основной атакой инсайдера может стать пользовательский терминал или сервер. При получении доступа к этим ресурсам инсайдер может работать с информацией или менять конфигурацию сети так, как ему это необходимо. На рис. 3 приведена схема атак нарушителей из внешней или внутренней телекоммуникационной среды.

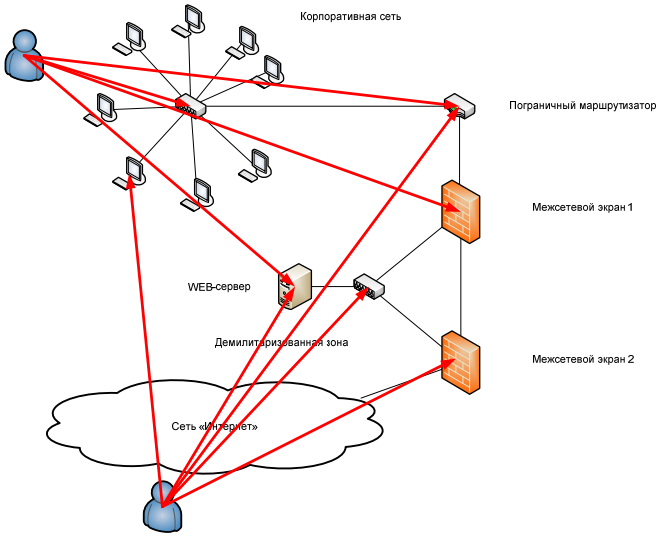


Рис. 3. Схема атак на участке корпоративной сети

Данные атаки можно классифицировать таким образом:

Из внешней или внутренней среды — на межсетевые экраны (для изменения их политики фильтрации трафика), на маршрутизатор (для изменения таблицы маршрутизации), на коммутатор (для получения доступа к транспортной среде) на локальную рабочую станцию или сервер (для получения доступа к информации, хранящейся или обрабатывающейся на них). Также на все устройства может быть оказано воздействие для получения отказа в обслуживании (когда устройство перестает обрабатывать запросы легитимных пользователей)[1]. В результате

[1] Веб-серверы, развитие технологий. Бизнес-результаты // Каталог «Системы безопасности» — 2017.

проведения исследования были рассмотрены аспекты построения современных корпоративных сетей, рассмотрено оборудование данных сетей, проведен анализ атак и угроз, влияющих на безопасность корпоративных сетей. Дальнейшие научные интересы сводятся к анализу существующих и подбору оптимальных решений для обеспечения безопасности функционирования современного сегмента корпоративной сети.

Библиографический список

1. *Кузьменко Н.* Компьютерные сети и сетевые технологии. М., 2009.
2. *Основы* защиты информации: учеб. пособие / А. А. Шелупанов, А. П. Зайцев, Р. В. Мещеряков и др. Томск: В-Спектр, 2016. Ч. 2.

Н. В. Калязин, П. К. Шаврина, В. Ю. Бердюгин
Южно-Уральский государственный университет – НИУ, г. Челябинск

Разработка игровой модели программной защиты информации в целях повышения осведомленности персонала

Аннотация. Описывается метод повышения осведомленности сотрудников объектов критической информационной инфраструктуры (КИИ) в области обеспечения безопасности КИИ. Для решения данной задачи предлагается использовать деловую игру. Приводится описание игры, оценка ее эффективности.

Ключевые слова: корпоративная сеть; архитектура; трафик; сервер; коммутатор; межсетевой экран; демилитаризованная зона.

Законодательство в сфере защиты информации на объектах КИИ совершенствуется с каждым годом. Особенно активно оно стало развиваться с 2017 г., с принятия Федерального закона № 187-ФЗ «О безопасности КИИ Российской Федерации[1]», который определил объекты КИИ, которые относятся к значимым и должны защищаться в соответствии с требованиями подзаконных нормативных документов.

В 2017 г. вышли и приказы ФСТЭК[2], которые содержали эти требования.

[1] О безопасности критической информационной инфраструктуры Российской Федерации: федер. закон от 26 июля 2017 г. № 187-ФЗ.

[2] Об утверждении требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования: приказ ФСТЭК России от 21 декабря 2017 г. № 235; Об утверждении требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации: приказ ФСТЭК России от 25 декабря 2017 г. № 239.

Одними из важнейших пунктов требований к созданию системы информационной безопасности (далее ИБ) является проведение разъяснительной работы с персоналом и повышение его осведомленности об угрозах безопасности.

Согласно данным компании InfoWattch, более 95% инцидентов, связанных с внутренним нарушителем, были непреднамеренными, и происходили по ошибке сотрудников.

Как отмечают авторы исследования, утечки, совершенные по неосторожности, происходят чаще всего в организациях тех отраслей, где уделяют недостаточно внимания вопросам цифровой грамотности, а направление ИБ совершенствуется медленнее.

За последние несколько лет большинство случайных инцидентов, связанных с ИБ, происходили в сфере медицины, образования, в государственных и силовых структурах[1], т.е. в сферах, предприятия которых, являются субъектами КИИ.

Широко распространены случаи, когда документы или технику, содержащую секретные сведения, выбрасывают[2], выставляют на продажу[3], оставляют в общественном транспорте[4] или же просто в заброшенных зданиях[5]. Такие случаи фиксируются как в России, так и за рубежом.

Повышение осведомленности персонала – это один из важнейших этапов внедрения системы обеспечения ИБ, который направлен на обучение персонала и поддержание его знаний в актуальном состоянии. Обучение персонала компании по вопросам ИБ – залог высокой эффективности всей системы безопасности в целом. Кроме того, большую часть инцидентов ИБ можно не допустить, поскольку более половины всех инцидентов порождают работники по незнанию требований и правил ИБ [1].

Сегодня большинство предприятий проводят занятия по повышению осведомленности в виде лекций. В ходе этой работы был рассмотрен новый, более качественный подход к этому вопросу. Актуальность работы состоит в том, чтобы создать эффективный способ повышения

---

[1] *Большинство* утечек данных из организаций за пять лет происходили из-за ошибок персонала или сбоев в системах обработки информации // Аналитический центр InfoWatch. URL: https://www.infowatch.ru/company/presscenter/news/15197.

[2] *На Урале* местный житель нашел на помойке секретные документы МВД // РИА Новости. URL: https://ria.ru/20181001/1529670405.html.

[3] *В Сети* купили ноутбук с военными секретами Германии // Аналитический центр InfoWatch. URL: https://www.infowatch.ru/analytics/data-loss-cases/21993.

[4] *Большинство* утечек данных из организаций за пять лет происходили из-за ошибок персонала или сбоев в системах обработки информации // Аналитический центр InfoWatch. URL: https://www.infowatch.ru/company/presscenter/news/15197.

[5] *В заброшенном* отделе полиции в Москве забыли «кубометры» документов россиян // Новости РИА URA.RU. URL: https://ura.news/news/1052346986.

осведомленности персонала объектов КИИ в вопросах ИБ, проверить его эффективность и сравнить ее с эффективностью других форм обучения.

Современная психология выделяет три основные категории методов обучения:

— к пассивным методам обучения относится лекция, в ходе которой лектор является основным действующим лицом, а обучаемые выступают в роли пассивных слушателей;

— к активным методам относят семинары, мастер-классы, кейсы. Общим их признаком является взаимодействие обучаемого и обучающего;

— интерактивные методы, такие как деловые игры, круглый стол и др., направлены на еще более плотное взаимодействие обучающихся.

Согласно последним исследованиям психологов, именно интерактивные методы дают наиболее ощутимый результат. Поэтому было принято решение разработать деловую игру, которую можно было использовать для повышения осведомленности персонала в области угроз информации на объектах КИИ [3].

Для того чтобы сделать игру более эффективной, мы воспользовались стандартом ISO/IEC 27002:2013[1], в котором, помимо прочего, выделены рекомендации по содержанию программы повышения осведомленности:

— целью программы повышения осведомленности должно являться ознакомление сотрудников с их обязанностями, касающихся вопросов ИБ, и средствами выполнения этих обязанностей;

— программа должна планироваться с учетом роли сотрудников в организации;

— деятельность в рамках программы повышения должна быть запланирована в течение долгого времени и регулярно повторяться;

— программа должна включать в себя осведомительные мероприятия, такие как выпуск буклетов, новостной рассылки, проведение специальных тематических дней и т.п.;

— при составлении программы повышения осведомленности, важно не только сосредоточиться на «что» и «как», но и «почему» (важно, чтобы сотрудники понимали цели ИБ);

— в конце курса повышения осведомленности должна быть проведена оценка понимания сотрудниками переданных им знаний;

— программа повышения осведомленности также должна регулярно обновляться, в соответствии с изменениями в организационных

[1] *ISO*/IEC 27002:2013 Information technology – Security techniques – Code of practice for information security con-trols.

политиках, а также она должна быть построена на уроках, извлеченных из инцидентов ИБ [2].

Разработанная игра является карточной командной соревновательной настольной игрой, состоит из четырех раундов, в каждом из которых игрокам предстоит обеспечить безопасность объекта КИИ, применив необходимые меры противодействия компьютерным атакам.

Первый раунд является тестовым. В ходе него участникам предоставляется возможность ознакомиться с угрозами и мерами противодействия им.

С каждым раундом участникам предстоит обеспечивать безопасность объектов КИИ все более высокой категории. Увеличивается число потенциальных угроз, количество возможных мер, уменьшается время на принятие решения.

Для повышения интереса участников и увеличения эффективности обучения в деловой игре используются виртуальные деньги. За правильное применение мер игроки получают виртуальную премию, за неправильное же применение мер защиты, участники могут потерять деньги, а также получить виртуальный штраф. Чтобы повысить шансы на победу, были введены дополнительные меры.

В начале каждого раунда участники получают комплект карточек мер защиты, карточки раунда и угроз. Определив актуальные угрозы и выбрав меры для их предотвращения, ответы заносятся в программу для автоматического подсчета результатов.

На основе «Банка данных угроз безопасности информации»[1] представленном на официальном сайте ФСТЭК, исследований НКЦКИ, и «Решений компании Cisco Systems по обеспечению безопасности корпоративных сетей»[2] был сформирован список актуальных для объектов КИИ компьютерных атак.

Такой метод группировки позволяет в наилучшей степени понимать возможные потери предприятия, позволяет принять наиболее эффективные меры защиты, а также упрощает процесс понимания смысла самих угроз.

Далее был сформулирован список наиболее значимых угроз для объектов КИИ. Данный список является краткой версией «Состава мер по обеспечению безопасности для значимого объекта соответствующей категории значимости»[3]. Сокращение было необходимо для упрощения

---

[1] *Банк* данных угроз безопасности информации // Официальный сайт ФСТЭК России. URL: https://bdu.fstec.ru/threat.

[2] *Решения* компании Cisco Systems по обеспечению безопасности корпоративных сетей // Официальный сайт компании Cisco Systems. URL: https://www.cisco.com/c/dam/global/ru_ru/assets/ downloads/security.pdf.

[3] *Об утверждении* требований к созданию систем безопасности значимых объектов КИИ Российской Федерации: приказ ФСТЭК России от 25 декабря 2017 г. № 239.

восприятия однотипной информации. Кроме того, такой метод группировки позволяет принимать наиболее эффективные методы предотвращения атак.

Также для повышения сложности были добавлены несколько мер защиты, принятие которых не требуется или, вовсе, вредит безопасности объектов. Для разных раундов было принято решение взять абстрактные объекты КИИ разных категорий значимости. После проведения игры проводился опрос участников, в ходе которого участники подтверждали, что данный способ повышения осведомленности намного интереснее и эффективнее лекций. Представленную игру можно уже сейчас применять как способ повышения уровня знаний в области ИБ.

Библиографический список

1. *Писаренко И.* Повышение осведомленности пользователей по вопросам ИБ // Information Security / Информационная безопасность. 2013. № 1. URL: http://itsec.ru/articles2/control/povyshenie-osvedomlennosti-polzovateley-po-voprosam-ib.

2. *Раковская А. С., Бердюгин В. Ю.* Повышение осведомленности сотрудников в области защиты персональных данных // Наука ЮУрГУ: материалы 68-й науч. конф. секции технических наук. Челябинск: Изд. центр ЮУрГУ, 2016. С. 627–635.

3. *Хайулин В. Р.* Использование деловой игры для повышения осведомленности персонала в отношении требований обеспечения информационной безопасности // Безопасность информационного пространства: сб. тр. XVIII Всерос. науч.-практ. конф. студентов, аспирантов и молодых ученых. (Магнитогорск, 28–29 ноября 2019 г.). Магнитогорск: Изд-во Магнитогорск. гос. техн. ун-та им. Г. И. Носова, 2019. С. 163–167.

Программно-аппаратные средства защиты информации, компьютерная безопасность

Н. С. Алпатов, М. П. Воронов, В. П. Часовских
Уральский государственный экономический университет, г. Екатеринбург

Обзор современных технологий настройки и администрирования беспроводной сети

Аннотация. Статья посвящена обзору технологий администрирования в беспроводных сетях. На основе анализа литературных источников приведены классификация беспроводных сетей, способы защиты беспроводных каналов, рекомендации по обеспечению безопасности беспроводных устройств.

Ключевые слова: информационные технологии; беспроводные сети; администрирование сетей.

В современном мире все большее распространение получают беспроводные сети. Это гораздо удобнее и позволяет быть независимым от проводных телефонов, компьютерных сетей. Именно поэтому существует огромное количество технологий и стандартов беспроводной передачи данных.

Обычно беспроводные сети классифицируют по нескольким критериям. Одним из основных является — максимальный радиус действия [4].

— WWAN (Wireless Wide area network) — в основном это сети сотовой связи, их радиус действия составляет десятки километров.

— WMAN (Wireless Metropolitan Area Network) — это беспроводные сети масштаба города. Радиус действия таких сетей несколько километров.

— Wireless LAN (Wireless Local Area Network) — это беспроводная локальная вычислительная сеть. Радиус действия составляет несколько сотен километров.

— WPAN — применятся для связи различных устройств. Радиус связи составляет несколько десятков метров [7].

Кроме этого, важным критерием является роль протоколов при определении уровней модели OSI. Стек OSI предусматривает 7 уровней, разработанных Международной организацией по стандартам:

1) физический;
2) канальный;
3) сетевой;
4) транспортный;

5) сеансовый;

6) представления данных;

7) прикладной.

Wi-FI — создан в 1991 г. NCR Corporation в Нидерландах — Wireless Fidelity — беспроводная точность. Схема сети содержит не менее одной точки доступа и не менее одного клиента. Возможно подключение двух клиентов в режиме точка-точка, когда точка доступа не используется, а клиенты соединяются посредством сетевых адаптеров «напрямую». Точка доступа передает свой идентификатор сети SSID с помощью специальных сигнальных пакетов на скорости до 10 Мбит/с каждые 100 мс. Поэтому 0,1 Мбит/с — минимальная скорость передачи данных для W-FI [1].

Так как технологии беспроводного доступа к сети в большей частности являются сетями общего пользования то, следует рассмотреть аспект безопасности. Несмотря на то, что на сегодняшний день для защиты Wi-Fi применяются сложные алгоритмы, проблема доступа третьих лиц к информации является существенной. И если не настроить сеть правильно, то злоумышленник может:

— заполучить доступ к ресурсам и дискам пользователей Wi-Fi-сети, а через нее и к ресурсам LAN;

— подслушивать трафик, извлекать из него конфиденциальную информацию;

— искажать проходящую в сети информацию;

— воспользоваться интернет-траффиком;

— атаковать ПК пользователей и серверы сети;

— внедрять поддельные точки доступа;

— рассылать спам, и совершать другие противоправные действия от имени вашей сети [2].

Чтобы разобраться в способах обеспечения безопасности нужно сначала изучить процесс аутентификации [6].

Существует несколько механизмов обеспечения безопасности. Протокол шифрования передаваемых данных WEP — основная функция этого протокола — шифрование. Еще один механизм защиты WEP2 — улучшенный механизм шифрования и поддержка метода шифрования Cerberos V. В 2003 г. был представлен стандарт безопасности IEEE 802.1X, использующий динамические 128-разрядные ключи шифрования. Основой этого стандарта является протокол WPA. Главной особенностью которого является использование технологии динамической генерации ключей [6].

Способы защиты беспроводных каналов с помощью разных способов от слабого к сильному:

1) Sin Seguridad;

2) MAC Auth;
3) WEP 64;
4) WEP 128;
5) WPA-PSK;
6) WPA2-TKIP;
7) WPA2-AES [8].

Сети использующие низкие ключи шифрования наиболее уязвимы. 64-битный ключ взламывается перебором. Фактическая длина секретного ключа составляет 40 бит, следовательно, достаточно перебрать всего лишь 549 755 813 888 комбинаций. При скорости перебора в сто миллионов ключей в секунду атака займет около часа [5]. По возможности стоит применять алгоритм шифрования WPA2, так как WEP устарел и существует огромное количество способов проникновения [3]. Рекомендации обеспечения безопасности беспроводных устройств:

1) запретить настройку используя соединение по радиосигналу;
2) использовать WPA;
3) не использовать в названии наименования, позволяющие идентифицировать принадлежность к владельцу или организации;
4) не использовать без необходимости DHCP;
5) включить фильтрацию MAC-адресов;
6) использовать длинные ключи доступа [9].

Библиографический список

1. *Андреев Ф. И., Трегубов С. В.* Как работает Wi-Fi // StudNet. 2020. № 3. С. 380–386.

2. *Белов Э. В.* Обзор безопасности беспроводных сетей семейства 802.11 // Научно-технический вестник информационных технологий, механики и оптики. 2006. № 29. С. 205–208.

3. *Зарешин С. В., Сильнов Д. С.* Комплексный анализ защищенности беспроводных сетей НИЯУ МИФИ // Современные информационные технологии и ИТ-образование. 2016. № 4. С. 90–96.

4. *Коптев Д. С., Щитов А. Н., Шевцов А. Н.* Сравнительный анализ наиболее перспективных стандартов беспроводных сетей связи // Международный журнал гуманитарных и естественных наук. 2016. № 1. С. 185–191.

5. *Куценко И. О., Жайворонок Д. А.* Анализ уязвимостей беспроводных сетей // Вестник ВИ МВД России. 2007. № 4. С. 140–143.

6. *Лабутин Н. Г.* Инновационные способы защиты беспроводных компьютерных соединений в целях обеспечения экономической безопасности // Юридическая наука и практика: вестник Нижегородской академии МВД России. 2010. № 1 (12). С. 221–226.

7. *Разиньков С. Н.* Основные направления развития и базовые технологии создания систем радиосвязи со сверхширокополосными сигналами // Воздушно-космические силы. Теория и практика. 2019. № 11. С. 38–44.

8. *Скрыпников А. В., Денисенко В. В., Евтеева К. С.* Защита данных при передаче по беспроводным каналам связи // Международный журнал гуманитарных и естественных наук. 2019. № 8-2. С. 35–38.

9. *Старцев С. С.* К вопросу защиты беспроводных сетей на базе технологии Wi-Fi // Вестник НГУ. Сер.: Информационные технологии. 2012. Т. 10, вып. 1. С. 63–72.

И. Ю. Антосик, А.В. Вершицкий
Крымский федеральный университет им. В.И. Вернадского, г. Симферополь

Опыт импортозамещения ИКТ в государственных органах власти

Аннотация. Рассмотрен опыт применения отечественного программного обеспечения в органах государственной власти. Проведен анализ преимуществ и недостатков информационно-коммуникационных технологий, в частности программ по импортозамещению.

Ключевые слова: импортозамещение; программное обеспечение; государственные органы; информационно-коммуникационные технологии.

В XXI в. почти все организации используют информационно-коммуникационные технологии (ИКТ) для эффективного управления своей деятельностью, чтобы менеджеры могли принимать наиболее рациональные и правильные решения, тем самым достигая конкурентные позиции во внешней среде, для облегчения внутренней среды со своими сотрудниками, клиентами, партнерами и другими заинтересованными сторонами. Использование «больших данных», позволяющих аккумулировать в себе архивы и поисковые системы, торговые и аналитические платформы, бизнес и государственные базы различного рода облегчают поиск информации при принятии решений, способствуют достижению высокого уровня развития гражданского общества в нашей стране. А искусственный интеллект, разработанный на основе умственных способностей человека, благодаря быстрому запоминанию информации и умению обрабатывать ее в больших количества в кратчайшие сроки, позволяет найти правильный вариант решения проблемы[1].

В рамках реализации национальной программы «Цифровая экономика Российской Федерации» утвержденная протоколом заседания президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам от 4 июня 2019 г. № 7. Из

[1] *Вершицкий А. В.* Технологическая трансформация государственного управления и переход к когнитивному правительству // Оптимизация системы управления социально-экономическим развитием региона: теория и практика: материалы XIV Междунар. науч.-практ. конф. (Симферополь, 25–27 октября 2018 г.). Симферополь: Полиграфинт, 2018. С. 10–11.

шести направлений реализации программы, два: «Цифровое государственное управление» и «Информационная безопасность» взаимодополняют друг друга.

Среди ключевых показателей данных направлений, которые планируется достигнуть к 2024 году, является:

1) обеспечение устойчивой и безопасной информационной инфраструктуры, конкурентоспособности отечественных разработок и технологий информационной безопасности;

2) выстроение эффективной система защиты прав и законных интересов личности, бизнеса и государства от угроз информационной безопасности;

3) 90% автоматизация внутри- и межведомственного электронного документооборота, а также устранения отставания РФ на международном уровне.

Необходимо отметить значимое событие, в ноябре 2020 г., согласно приказу Министерства цифровового развития, связи и массовых коммуникаций (Минкомсвязи) произошел переход некоторых государственных органов на отечественный софт — в рамках импортозамещения иностранного ПО 26 госорганов исполнительной власти России, где вместо операционной системы Windows будет установлена Astra Linux[1]. Первым субъектом, в котором применится данный опыт в аспекте государственного управления, стала Ивановская область. Интересно, что уже давно Astra Linux и с успехом используется на предприятиях «Ростеха», «Росатома», «Роскосмоса», а также в МВД, ФСБ и ФСИН. Например, в Федеральной службе судебных приставов в 2014 г. была внедрена многопользовательская система Гослинукс (GosLinux), которая используется до сих пор. При создании продукта делался акцент на безопасности обрабатываемых данных и особенностях служебной деятельности судебных приставов-исполнителей[2]. О совместимости своих продуктов с ГосЛинуксом уже заявили различные разработчики ПО, в том числе «Ред Софт», «Крипто-Про», «ИнфоТеКС», «Лаборатория Касперского» и «Доктор Веб». Разработчики GosLinux признают наличие ряда проблем совместимости с некоторыми широко востребованными в госструктурах приложениями и подчеркивают, что в этом направлении специалистами ведомства и партнерскими организациями ведется активная работа.

---

[1] *Об утверждении* методических рекомендаций по переходу государственных компаний на преимущественное использование отечественного программного обеспечения, в том числе отечественного офисного программного обеспечения: приказ Минкомсвязи России от 20 сентября 2018 г. № 486.

[2] *Официальный* сайт национальной программы «Цифровая экономика». URL: https://digital.ac.gov.ru.

Выбор операционной системы линейки Astra Linux определили несколько факторов, среди которых доступность, безопасность и простота освоения, также имеет значение то, что продукты Astra Linux входят в реестр отечественного ПО при Минкомсвязи. ОС Astra Linux принята в стандарт федеральных органов исполнительной власти и госкорпораций, кроме того, она имеет полный набор сертификатов Минобороны России, ФСТЭК (Федеральная служба по техническому и экспортному контролю) и ФСБ (Федеральная служба безопасности). Помимо обеспечения ПО вендор, то есть компания, которая разработала программу, обязуется оказывать всестороннюю консультационную поддержку при переходе на отечественную операционную систему. Перевод ИТ-систем госорганов потребует настройки корректного взаимодействия обновленных ИТ-систем с теми решениями, что уже есть у заказчиков, и со всеми ресурсами, с которыми работают пользователи. Чтобы обеспечить полноценное функционирование инфраструктур под управлением Astra Linux, предстоит подобрать совместимые отечественные аналоги продуктов и обучить пользователей и администраторов работе с ними.

Персонал госорганов обучится применять новое ПО в учебном центре Astra Linux, который открыт на базе Ивановского государственного университета. Причем курсы будут не только для администраторов различных уровней, но и для пользователей. Группа Astra Linux участвует в проектах импортозамещения и безопасности КИИ (критической информационной инфраструктуры). Компания по итогам 2019 г. поставила почти 24 тыс. лицензий на свою фирменную ОС в российские медицинские учреждения. ОС Astra Linux сегодня существует в двух версиях — Common Edition и Special Edition. Первая предназначена для потребителей, а также для среднего и малого бизнеса, образовательных учреждений. Она находится в свободном доступе и может быть скачана с официального сайта проекта. Special Edition разработана для государственных и военных предприятий и не распространяется в свободном доступе. Сборки Astra Linux Special Edition выпускаются под архитектуры «Эльбрус» (релиз «Ленинград»), IBM System Z («Мурманск»), POWER («Керчь), MIPS («Севастополь»), ARM («Новороссийск») и x86-64 («Смоленск»). Каждый из релизов имеет различные сферы применения: к примеру, «Новороссийск» пригоден для мобильных устройств и встраиваемых компьютеров, а «Ленинград» — для вычислительных комплексов «Эльбрус». Стоит отметить, о стоимости лицензии от 15 тыс. до 50 тыс., которая зависит от аппаратных платформ и срока техподдержки.

ОС Astra Linux гарантирует высочайший уровень информационной безопасности, подходит для использования в IT-системах, обрабатывающих такую конфиденциальную информацию, как персональные

данные и государственная тайна. Немаловажными факторами являются импортонезависимость решения, а также то, что приобретение лицензий и обеспечение поддержки ОС Astra Linux требуют меньшего финансирования, чем аналогичные продукты и услуги Microsoft. Внешне ОС схожа с Windows и проста в использовании. Однако среди вышеперечисленных возможностей и перспектив ОС Astra Linux присущ недостаток — большое отставание по версиям пакетов программ в официальных репозиториях.

Таким образом, появление на рынке отечественных производителей программного обеспечения становиться достойной альтернативой известным продуктам западных вендоров, особенно в государственных ведомствах и организациях. Важно поддерживать со стороны государства данные разработки, и использовать в органах власти с целью сохранения безопасности данных.

В. А. Бочарова, М. П. Воронов, В. П. Часовских
Уральский государственный экономический университет, г. Екатеринбург

Обзор сетей хранения данных (SAS, NAS, SAN)

Аннотация. Статья посвящена анализу сетевых архитектур SAS, NAS, SAN. Приводится описание, масштаб применения, особенности, преимущества каждой из архитектур.
Ключевые слова: информационные технологии; телекоммуникационные сети; SAS; NAS; SAN; администрирование сетей.

Часто в компаниях возникает задача хранения большого объема данных с определенной степенью надежности. Для этого используют сетевые хранилища данных.

Технологии хранения данных находятся в постоянном развитии. Оптимальным будет выбор решения, в котором учитываются все потребности организации.

В настоящее время четкой квалификации сетевых хранилищ не сформировалось, поэтому приведем одну из квалификаций, где устройства структурируются по типу подключения:

1) прямое. Direct Attached Storage (DAS) — этот термин используется для описания устройства хранения, которое напрямую подключается к материнской системе. Простейшим примером DAS будет внешний жесткий диск серверной станции, хотя устройства хранения, расположенные во внешнем носителе, также подпадают под эту категорию. DAS до сих пор является наиболее распространенным методом хранения данных в компьютерных системах;

2) сетевое:

— Attached Storage (NAS) — этот механизм хранения данных использует специальные устройства, подсоединяемые непосредственно к сетевой среде. У этих устройств имеется собственный IP адрес, который может быть доступен клиентам через сервер, служащий шлюзом к данным, или может быть использован для немедленного доступа, минуя все препоны;

— сеть хранения данных (Storage Area Network — SAN) — это сеть из устройств для хранения данных, объединенных в общий сервер или кластер из серверов, где каждый из них также действует как отдельное устройство хранения данных SAN. По данным исследовательской компании IDC, на SAN приходится более 70% всего сетевого хранения[1].

Архитектура типа SAS. Это идеальное решение для небольших и средних компаний, а также для индивидуальных пользователей. Традиционный способ подключения системы хранения данных к высокоскоростному интерфейсу в сервере, как правило, к параллельному SCSI интерфейсу. Производительность SAS зависит от операционной системы машины и используемой файловой системы, а также от загрузки сервера, обслуживающего систему хранения. Примером принципа хранения данного типа может служить файловый сервер[2].

Особенности SAS: доступ к данным зависит от ОС и файловой системы; сложность организации систем с высокой готовностью; высокое быстродействие.

Архитектура типа NAS. Этот вариант организации доступа появился сравнительно недавно. Основным его преимуществом является удобство интеграции дополнительной системы хранения данных в существующие сети. NAS — чистый файл-сервер.

Они представляют собой, по сути, выделенный файл-сервер, и являются более простым и достаточно быстрым способом решения задачи отделения процесса доступа к данным от сервера и обеспечения равномерной загрузки ЛВС, а доступ к данным не зависит от ОС и платформы. NAS-сети лучше всего подходят для небольших офисов или отделов предприятий. Системы такого типа достаточно просто администрировать.

Особенности NAS: выделенный файл-сервер; доступ к данным не зависит от ОС и платформы; удобство администрирования; максимальная простота установки; низкая масштабируемость.

---

[1] *SAN*, SAS, NAS: шаг к сетям хранения данных. URL: https://www.ixbt.com/storage/san.shtml.

[2] *Системы* хранения данных — SAS, NAS, SAN. URL: https://www.iptc.ru/content/view/40/62.

Основным ее преимуществом является интеграции дополнительной системы хранения данных в существующие сети.

Архитектура сети типа SAN. Высокоскоростная сеть передачи данных Storage area network (SAN) предназначена для подключения серверов к устройствам хранения данных. SAN-решение представляет собой дополнительную выделенную сеть, связывающую один или несколько серверов с одной или несколькими системами хранения данных. SAN- решение позволяет любому серверу получить доступ к любому накопителю, при этом не загружая ни серверы, ни корпоративную локальную сеть. Помимо этого, становится возможным обмен данными между системами хранения данных без участия серверов. Основой SAN является отдельная от LAN/WAN сеть, занимающихся их прямой обработкой, которая служит для организации доступа к данным серверов и рабочих станций[1].

Статья[2] говорит нам о том, что сеть SAN и сетевая система хранения данных (NAS) — это два разных типа сетевых решений для хранения данных с общим доступом.

Сеть SAN — это локальная сеть, созданная на базе нескольких устройств, а NAS-система — это одно устройство хранения данных, подключаемое к локальной вычислительной сети[3].

Автор статьи[4] выделяет единственный недостаток SAN- высокая цена компонент, при этом общая стоимость владения для корпоративных систем, построенных с использованием технологии сетей хранения данных, является довольно низкой.

На основе статьи «Сети хранения SAN»[5] можно выделить следующие задачи SAN:

— повысить скорость и надежность передачи данных;

— обеспечить доступ к устройствам хранения, находящимся на большом расстоянии от серверов, с минимальным снижением производительности;

— решить задачу построения отказоустойчивого решения с физически распределенными хостами обработки и хранения данных;

---

[1] *Как* хранить данные: SAN, NAS или DAS. URL: https://www.cnews.ru/articles/kak_hranit_dannye_san_nas_ili_das/2.

[2] *Сеть* SAN и принципы ее работы. URL: https://www.vmware.com/ru/topics/glossary/content/storage-area-network-san.html.

[3] *Сеть* SAN и принципы ее работы. URL: https://www.vmware.com/ru/topics/glossary/content/storage-area-network-san.html; Сетевые хранилища. URL: www.nstor-it-news.blogspot.ru/2010/06/blog-post.html.

[4] *SAN*, SAS, NAS: шаг к сетям хранения данных. URL: https://www.ixbt.com/storage/san.shtml.

[5] *Сеть* SAN и принципы ее работы. URL: https://www.vmware.com/ru/topics/glossary/content/storage-area-network-san.html.

— подключить к системе новые серверы и дисковые RAID-массивы к SAN без прекращения работы ИТ-среды;

— значительно увеличить скорость резервного копирования данных и восстановления информации с созданной резервной копии;

— включать в работу ранее приобретенные устройства вместе с новыми СХД;

— построить централизованное управление ИТ-средой для хранения данных.

Основные преимущества SAN:

— независимость топологии SAN от сторедж-систем и серверов;

— удобное централизованное управление;

— отсутствие конфликта с трафиком LAN/WAN;

— удобное резервирование данных без загрузки локальной сети и серверов;

— высокое быстродействие;

— высокая масштабируемость;

— высокая гибкость;

— высокая готовность и отказоустойчивость.

Е. А. Еременко, М. П. Воронов, В. П. Часовских
Уральский государственный экономический университет, г. Екатеринбург

Современные проблемы сетевого администрирования

Аннотация. На основе анализа литературных источников поднимаются проблемы сетевого администрирования на уровне локальных, городских и глобальных сетей. Определяются основные функции администратора сети.

Ключевые слова: информационные технологии; телекоммуникационные сети; сетевое администрирование; локальные сети; городские сети; глобальные сети.

В настоящее время во многих сферах жизни человека практически невозможно обойтись без информационных технологий. Чтобы быстро передавать информацию с одного компьютера на другой, все компьютеры должны быть соединены сетью. Ни одна сеть не может эффективно функционировать без сетевого администрирования. Именно здесь на помощь приходят сетевые администраторы, основной задачей которых является обеспечение безопасной, непрерывной и продуктивной работы сети.

Компьютерная сеть — это система связи для компьютеров и вычислительного оборудования [2].

С помощью сети различные типы компьютерных систем легко взаимодействуют друг с другом. Все устройства, работающие в одной сети,

должны общаться на одном языке. Стандарты являются ключевым фактором при подключении сетей.

Компьютерные сети можно разделить на три основные классификации: LAN (Local Area Network) — локальные сети; MAN (Metropolitan Area Network) — городские сети; WAN (Wide Area Network) — глобальные сети.

Локальные сети. Длина сети составляет не более одного километра. Высокая скорость обмена данными. Используют методы, не требующие предварительного установленного соединения. Каждый компьютер имеет сетевой адаптер. Подходит для отдельных организаций.

Городские сети. Длина сети в несколько сотен километров. На больших расстояниях теряется скорость. Содержат активные коммутационные устройства. Подходят для населенного пункта.

Глобальные сети. Имеет наибольшую протяженность. Работает на низких скоростях. Ориентированы на соединение перед началом передачи данных между абонентами. Состоят из групп мощных пакетных маршрутизаторов.

Рассмотренные сети могут объединяться в крупных организациях. Коммуникационная система, управляемая одной организацией в соответствии с правилами этой организации, определяет такое понятие как «корпоративная сеть» [1].

Снизить риск возникновения сетевых ошибок помогают сетевые администраторы. Для бесперебойной работы корпоративной сети администратор выполняет следующие задачи:

1) планирование сети. Администратору приходится планировать определенные изменения в структуре сети, например, добавление новых рабочих мест;

2) настройка компьютеров;

3) установка и настройка сетевых узлов;

4) установка и настройка сетевых протоколов;

5) установка и настройка сетевых служб;

6) поиск неисправностей;

7) повышение эффективности работы сети. Анализ функционирования сети и выявление наиболее узких мест, требующих либо замены сетевого оборудования, либо модернизации рабочих мест;

8) мониторинг сетевых узлов и сетевого трафика;

9) технический контроль сети. Системы технического контроля сети поставляются традиционными производителями коммутационного и модемного оборудования. Эти системы обеспечивают доступ к удаленным объектам по выделенным или телефонным линиям, а также по вспомогательному модемному каналу;

10) обеспечение защиты данных. Защита данных включает в себя резервное копирование и восстановление данных, разработку и внедрение политик безопасности учетных записей пользователей, построение защищенных коммуникаций.

Анализ задач сетевого администратора показал, что по мере роста размера и сложности сетей растут и требования к сетевому администрированию и сетевой безопасности.

Библиографический список

1. *Ляш О. И., Королева Н. Ю.* Сетевые технологии: теория и практика администрирования: учеб.-метод. пособие. Мурманск: Мурманск. гос. пед. ун-т, 2010. Ч. 2.

2. *Муратов Д. Ш., Минанхузина Г. И., Марданшин Р. Г.* Цели и задачи сетевого администрирования // Итоги 2016 года: идеи, достижения: сб. материалов III регион. науч.-практ. конф. с всерос. участием (Альметьевск, 25 ноября 2016 г.). М.: Изд-во «Перо», 2016. С. 114–117.

Е. Д. Жирняков
Южно-Уральский государственный гуманитарный педагогический университет, г. Челябинск

Защита конфиденциальной информации в общеобразовательной организации с помощью симметричного шифрования данных

Аннотация. Рассматривается алгоритм шифрования данных, реализованный на языке программирования Python, с использованием симметричного ключа шифрования данных (AES).

Ключевые слова: информация; криптография; шифрование; дешифрование; Python; алгоритм.

Множество общеобразовательных организаций имеют потребность в защите конфиденциальной информации, которая храниться на устройствах долговременной памяти в виде файлов. Существует множество способов защиты информации, один из них — криптография.

Современные программы криптографической защиты информации позволяют зашифровать данные с помощью различных методов шифрования, использующих симметричные ключи (DES, AES, RC4), ассиметричные (SHA-1/2, MD4) и хэш-функции. Программу для шифрования данных можно написать на различных языках программирования, таких как Python, C, C#, Java и др. В данной статье будет рассмотрен алгоритм

шифрования, реализованный на высокоуровневом языке программирования Python.

Программа основана на симметричном ключе шифрования AES, который производит вычисления не в битах, а в байтах, что позволяет рассмотреть 16 битную матрицу, расположенную в прямоугольной области. Данный метод шифрования основан на алгоритме замены и перестановки строк и столбцов, включающий ряд связанных между собой операций, часть которых производят замену входных данных, а другая часть — перестановку битов.

Программа представляет собой небольшое графическое окно, построенное с помощью модуля Tkinter GUI языка программирования Python. Пользователь добавляет в программу файлы, которые необходимо зашифровать, выбирает ключ шифрования (сгенерированный программой или системный) и режим шифрования или дешифрования файлов (рис. 1).

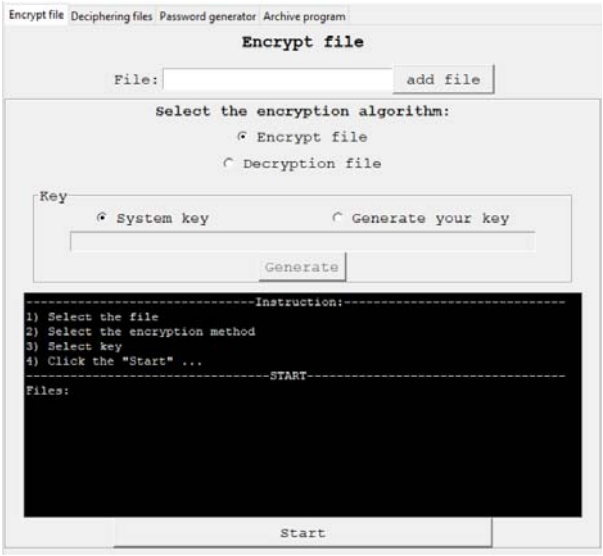


Рис. 1. Графический интерфейс программы шифрования данных

Для шифрования и дешифрования файлов в программе используется пакет «cryptography». Это пакет, который предоставляет разработчикам Python криптографические функции и методы. «Cryptography» — включает в себя функции как высокого уровня, так и низкоуровневые

интерфейсы для общих криптографических алгоритмов, таких как симметричные шифры, дайджесты сообщений и ключевые функции производных.

Шифратор принимает на вход данные и преобразует их в матричный формат с ключом шифрования (рис. 2).

```
def generate_key():
    global YOUR_KEY
    key = Fernet.generate_key()
    entry_keys.insert(0, key)
    YOUR_KEY = bytes(entry_keys.get(), 'utf-8')
```

Рис. 2. Фрагмент кода программы

Для того, чтобы не было возможности расшифровать данные, в матрицу добавляется сгенерированный симметричный ключ. Генерация ключа происходит с помощью метода **generate_key()** библиотеки «cryptography».

Модуль fernet генерирует новый ключ. Если пользователь потеряет данный ключ, то больше сможет расшифровывать данные. При утере ключа и получении к нему доступа злоумышленником, он сможет расшифровать данные, а также подделать произвольные сообщения, которые будут проверены и расшифрованы. Кроме сгенерированного ключа, программа может использовать вшитый в код ключ, который храниться в переменной YOUR_KEY (рис. 3).

```
if answer:
    for filename in open_file:
        if var_key.get() == 'system':
            f = Fernet(KEY)
        elif var_key.get() == 'your key':
            try:
                f = Fernet(YOUR_KEY)
```

Рис. 3. Фрагмент кода программы (YOUR_KEY)

Шифрует преданные данные метод **incrypt**. Результат этого шифрования известен как Fernet, который обеспечивает конфиденциальность и подлинность обрабатываемых данных (рис. 4).

```
encrypted_data = f.encrypt(file_data)
with open(filename, 'wb') as file:
    file.write(encrypted_data)
```

Рис. 4. Фрагмент кода программы (Fernet)

Далее функция **decrypt** расшифровывает ключ Fernet. При успешной расшифровке вы получите исходный простой текст в результате, в противном случае будет поднято исключение. Безопасно использовать эти данные немедленно, так как Fernet проверяет, что данные не были подделаны до их возвращения (рис. 5).

```
decrypted_data = f.decrypt(encrypted_data)
with open(filename, 'wb') as file:
    file.write(decrypted_data)
```

Рис. 5. Фрагмент кода программы (decrypt)

Fernet идеально подходит для шифрования данных, которые легко записываются в память. Это означает, что полное содержимое сообщения должно быть доступно в памяти, что делает Fernet непригодным для очень больших файлов.

В общеобразовательной организации, как правило, конфиденциальная информация хранится в виде множества небольших документационных файлов, в связи с чем, непригодность Fernet к большим файлам не станет помехой для сохранения конфиденциальности данных организации.

А. А. Зыкова
Уральский государственный экономический университет, г. Екатеринбург

Анализ программно-аппаратного комплекса Positive Technologies Industrial Security Incident Manager

Аннотация. Каждый год число уязвимостей на промышленных объектах неуклонно растет. Под угрозой оказывается не только дорогостоящее оборудование. Опыт Positive Technologies в практической безопасности и экспертиза в исследованиях систем управления технологическим процессом позволили создать решение, сводящее к минимуму угрозу ущерба оборудованию в случае атак. В статье анализируется программно-аппаратный комплекс Positive Technologies Industrial Security Incident Manager, позволяющий вывести индустриальную безопасность на новый уровень.

Ключевые слова: АСУ; атака; безопасность; вирусы; защита; уязвимость.

PT ISIM — это программно-аппаратный комплекс, который предназначен для повышения уровня защищенности, проводящий диспансеризацию сети автоматизированной системы управления технологическим процессом (АСУ ТП), а также помогающий на ранней стадии выявить кибератаки, обеспечивая соответствие требованиям Российского законодательства[1].

В отличии от аналогов, PI ISIM разработал первый в мире бесплатный инструмент мониторинга информационной безопасности АСУ ТП — PT ISIM free View Sensor.

Он свободно распространяется, не требует сложной настройки и специальных знаний и не уступает раскрученным аналогичным продуктам.

PT ISIM freeView Sensor производит анализ сетевого трафика и находит инциденты на основе правил корреляции и моделирования. Обработка трафика происходит в несколько этапов.

1. Сбор — захват трафика со SPAN-порта коммутатора и анализ сообщений общесетевых и промышленных протоколов с целью выявления информации о событиях информационной безопасности. Собранная информация передается на нормализацию.

2. Нормализация — извлечение данных из атрибутов записей, которые могут иметь разный формат, и приведение их к единому формату нормализованных сообщений.

3. Фильтрация — удаление сообщений, не представляющих интереса с точки зрения информационной безопасности.

[1] *Positive* Technologies Industrial Security Incident Manager. URL: https://www.ptsecurity.com/ru-ru/products/isim.

4. Корреляция — проверка потока событий на соответствие определенному правилу. Результатом является скоррелированное сообщение.

5. Моделирование — составление актуальной карты вычислительной сети, отражающей ее реальный состав и взаимодействие между узлами.

6. Заведение инцидентов — PT ISIM freeView Sensor принимает решение о том, является ли событие инцидентом. Итогом обработки трафика является заведение записей о событиях и инцидентах в PT ISIM freeView Sensor.

Но, как и любой бесплатный продукт PT ISIM freeView Sensor не предусматривает технической поддержки и постоянного обновления Positive Technologies. В связи с эти, рассмотрим еще два инструмента с расширенным функционалом[1].

PT ISIM netView Sensor — простое решение сложных задач промышленной информационной безопасности. Позволяет инвентаризировать сетевые атаки, обеспечивает постоянный анализ трафика, выявляет неавторизованную активность и своевременно сигнализирует о кибератаках на промышленную сеть предприятия и дает знать о слабых местах в ИБ АСУ ТП.

К преимуществам рассматриваемого инструмента относятся:

1) не требует профессиональных знаний при внедрении и эксплуатации; доступная цена;

2) используя встроенные базы данных промышленных угроз, позволяет обнаружить до 80% угроз сети АСУ ТП;

3) инвентаризация сети АСУ ТП происходит, не прерывая технический процесс; оповещает об опасных ошибках;

4) используется на предприятиях любого размера и вида деятельности;

5) соответствует требованиям по защите объектов КИИ ФЗ-187, приказов ФСТЭК № 31 и 239 и ГосСОПКА[2].

Функции PT ISIM ViewSensor представлены в таблице.

Анализируя стоимость рассматриваемых продуктов, самый дешевый считается PT ISIM free View Sensor. Да, у него урезанный функционал, но для начала, например, для малого бизнеса этого достаточно.

---

[1] *Панов М. А., Зыкова А. А.* Анализ программно-аппаратного комплекса Positive Technologies Indastrial Security Incident Manager // Новые информационные технологии и системы в решении задач инновационного развития: сб. ст. Междунар. науч.-практ. конф. (г. Магнитогорск, 14 апреля 2020 г.). Уфа: OMEGA SCIENCE, 2020. С. 29−41.

[2] *PT* ISIM netView Sensor — Краткое описание продукта. URL: https://www.ptsecurity.com/upload/corporate/ruru/products/isim/PT-ISIM-netView-PB-rus.pdf.

Функции PT ISIM ViewSensor

Функция	freeView Sensor	netView Sensor	proView Sensor
Автоматическое построение карты узлов и их сетевого взаимодействия, контроль подключений к сети в реальном времени	Да	Да	Да
Поддержка промышленных протоколов	Да	Да	Да
Инструменты поиска и фильтрации событий и инцидентов	Да	Да	Да
Визуализация инцидентов на схеме сети	Да	Да	Да
Формирование списков разрешенных соединений и авторизированных узлов	Да	Да	Да
Возможность выгрузки в виде CSV-файла списка событий, инцидентов и узлов	Да	Да	Да
Хранение и возможность выгрузки копии трафика, относящегося к периоду, событию или инциденту	Нет	Да	Да
Ролевая модель пользователей, история действий	Нет	Да	Да
Передача сообщений об инцидентах в syslogсервер	Нет	Да	Да
Контроль технологических параметров	Нет	Нет	Да
Обработка событий с учетом логики техпроцесса	Нет	Нет	Да
Инструмент создания собственных правил заведения инцидентов	Нет	Нет	Да
Инструмент создания мнемосхемы техпроцесса	Нет	Нет	Да
Визуализация инцидентов на мнемосхеме	Нет	Нет	Да

Если рассматривать повышенную защищенность для более крупных компаний, бесплатная версия не подходит, поскольку не предоставляет подробную информации об инциденте. Например, PT ISIM netView Sensor или PT ISIM proView Sensor обладают таким возможностями, как централизованное управление сенсорами PT ISIM — это обновление, диагностика, предоставление информации по зафиксированным инцидентам ИБ.

Также производят анализ трафика и выявляют инциденты в распределенных, слабонагруженных системах АСУ ТП, первичный анализ трафика производится с помощью недорогих, низкопоизводительных сенсоров PT ISIM Sensor, размещенных на удаленных площадках.

М. С. Казаковцев, С. С. Рогачев, Е. С. Кремлев, У. В. Михайлова
Магнитогорский государственный технический университет им. Г.И. Носова,
г. Магнитогорск

Программная реализация алгоритмов обработки изображения отпечатка пальца для создания криптографической последовательности из биометрических данных

Аннотация. Рассматривается процесс создания криптографической последовательности из биометрических данных человека. Представлена программная реализация алгоритмов обработки изображения отпечатка пальца, построения поля направлений, а также поиск уникальных точек с последующим преобразованием их в криптографическую последовательность.

Ключевые слова: биокриптография; отпечаток пальца; последовательность; бинаризация; алгоритм; ключ.

В прошлой работе[1] мы рассматривали совмещение биометрии и криптографии с целью повышения безопасности СКУД. В данной же работе мы приступили к программной реализации описанных алгоритмов.

Практическая реализация была разделена на несколько этапов: считывание изображения, обработка изображения, поиск особых точек, получение биометрической последовательности из особых точек, получение криптографического ключа и его хранение.

Первый этап считывания был реализован с помощью сканера. Подручными средствами был снят отпечаток пальца с помощью карандаша и скотча, после чего он был просканирован на сканере с достаточно высокой плотностью изображения 500 ppi (пикселей на дюйм).

Изображение обрабатывалось фильтром Габора, который основан на направленном гауссианском размытии.

Для получения более детального изображения, необходимо производить фильтрацию по нескольким направлениям в интервале $[0; \pi)$. Нами было выбрано оптимальное число промежутков в данном интервале, равное 18. Результаты фильтрации объединяются в одно с помощью «умножения». Для отсеивания шума отфильтрованное по направлению изображение перед перемножением бинаризируется. Бинаризация представляет собой избавление изображения от пикселей оттенков серого, т. е. остаются пиксели только чистого черного и белого цветов с яркостями 0 и 255, соответственно.

[1] *Использование* особых точек отпечатков пальцев в биокриптографии и кодировании информации. URL: http://www.info-secur.ru/index.php/ojs/article/view/285/265.

Функция фильтра Габора в классическом виде выглядит следующим образом:

$$g\left(x, y, \lambda, \theta, \Psi, \sigma, \gamma\right) = \exp\left(\frac{-x'^2 + \gamma^2 y'^2}{2\sigma^2}\right)\cos\left(2\pi\frac{x'}{\lambda} + \Psi\right),$$

где:

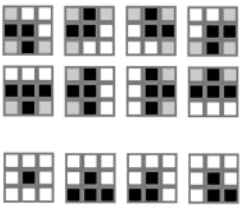
$$x' = x\cos\theta + y\sin\theta$$
$$y' = x\sin\theta + y\cos\theta$$

Стоит отметить, что параметры σ и *f* относятся к маске фильтра, а угол θ — к ориентации маски над изображением. Формула является произведением гауссиана и периодической функции, что подразумевает улучшение монотонных областей повторяющихся частей изображения.

Эмпирическим путем были определены значения параметров: длины волны λ, равной 5, сдвига фазы ψ = 1, стандартного отклонения σ = 2 и коэффициента сжатия γ = 1.

В теоретической части нахождение особых точек осуществлялось с помощью алгоритма Базена, однако ввиду отсутствия достаточного количества теоретической информации в открытом доступе для реализации его, поэтому мы отказались от данного алгоритма в пользу скелетизации.

Мы использовали метод шаблонной скелетизации. Суть которого состоит в преобразовании изображения по некоторым шаблонам-маскам. Шаблоны соответствуют матрице 3×3, где центральный элемент является текущим пикселем в обходе изображения. Примеры шаблонов приведены на рисунке, где белые и черные пиксели должны совпасть, а серые не имеют значения.



Шаблоны обхода изображения

Когда блок пикселей совпадает с шаблоном, центральный пиксель окрашивается в белый цвет (не принадлежит скелету). Обход продолжается, пока остаются возможности удаления.

Далее идет поиск особых точек. Если в окрестности из 8 точек, есть только одна черная, то это конечная точка. Если же их 2, то это просто точка линии. Три — точка ветвления.

Таким образом, мы нашли особые точки, но представлены они в виде координат в плоскости изображения, где отсчет идет от края области, где лежит отпечаток, а не от центра папиллярного узора. Дальнейшее усовершенствование алгоритма будет за счет привязки точки отсчета к центру папиллярного узора.

Следующим этапом разработки будет создание биометрической последовательности, преобразование ее в криптографический ключ блоками fuzzy. Справиться с задачей преобразования входного набора биометрических данных в последовательность битов помогает блок генерации биометрической последовательности. Полученная последовательность потребуется в дальнейшем для того, чтобы сформировать криптографический ключ.

А. В. Кутуева
Уральский государственный экономический университет, г. Екатеринбург

Интеллектуальный анализ вредоносных атак в сети Интернет с применением SAP Analytics Cloud

Аннотация. В эпоху информационных технологий все личные данные находятся под угрозой. В статье рассматриваются способы интеллектуального анализа атак, предпринимаемых с целью получения конфиденциальной информации, и средства защиты от атак.

Ключевые слова: атака; вредоносная активность; информация; уязвимость; информационная система.

В настоящее время жизнь человека сложно представить без информационных технологий. Информационные технологии стремительно развиваются, становятся более сложными, но в тоже время и понятными для пользователей — возникают онлайн утилиты и множество социальных сетей. Из-за этого люди стали больше времени проводить в интернете.

Большим помощником для человека являются Интернет-ресурсы, за доли секунд человек может найти интересующую его информацию, общаться с родственниками и друзьями, знакомится с новыми людьми, которые могут находится за тысячи километров и многое другое. Но стоит отметить и то, что вместе с этим увеличивается количество угроз,

связанных с вредоносными атаками в сети Интернет. Для борьбы с этими угрозами необходимо использовать методы кибербезопасности, которые призваны не только минимизировать угрозы, но и служат для защиты наших данных от злоумышленников.

В связи с ростом объемов данных, находящихся в локальных и глобальных вычислительных сетях и расширением количества задач, которые можно решить с помощью информационных ресурсов, появилась проблема, связанная с увеличением уязвимостей информационной системы.

Уязвимость — это свойство информационной системы, обусловливающее возможность реализации угроз безопасности, обрабатываемой в ней информации.

Атака (вторжение) — это действия злоумышленника, использующего уязвимости в информационной системе, которые приводят к нарушению целостности, доступности и конфиденциальности информации.

Одним из самых популярных методов внедрения вредоносного ПО — это распространение вредоносного кода через веб-страницы.

На веб-страницу помещаются зараженный файл и скриптовая программа, эксплуатирующая браузерную уязвимость. Когда на эту страницу заходит пользователь, скриптовая программа скачивает зараженный файл на компьютер пользователя, используя уязвимость в браузере, и затем запускает этот файл.

Существует множество вредоносных активностей в сети Интернет, которые пытаются классифицировать, но с появлением новых угроз требуется обновление классификаций.

Один из способов получения таких классификаций является интеллектуальный анализ данных.

Продемонстрируем на примере датасета «Cybersecurity_attacks», взятого на сервисе «Kaggle» с данными об атаках на кибербезопасность, в котором проанализируем категории атак. Dataset состоит из: Attack category (категория атаки), Attack subcategory (подкатегория атаки), Protocol, Source IP (IP-адрес отправителя), Source Port (исходный, начальный порт), Destination IP (IP-адрес получателя), Destination Port (порт назначения), Attack Name (имя атаки), Attack Reference (ссылка на атаку), Time (время атаки в микросекундах).

С помощью SAP Analytics Cloud построили диаграмму (рис. 1), на которой видно, как распределены категории атак, т.е. какие атаки встречаются чаще всего.

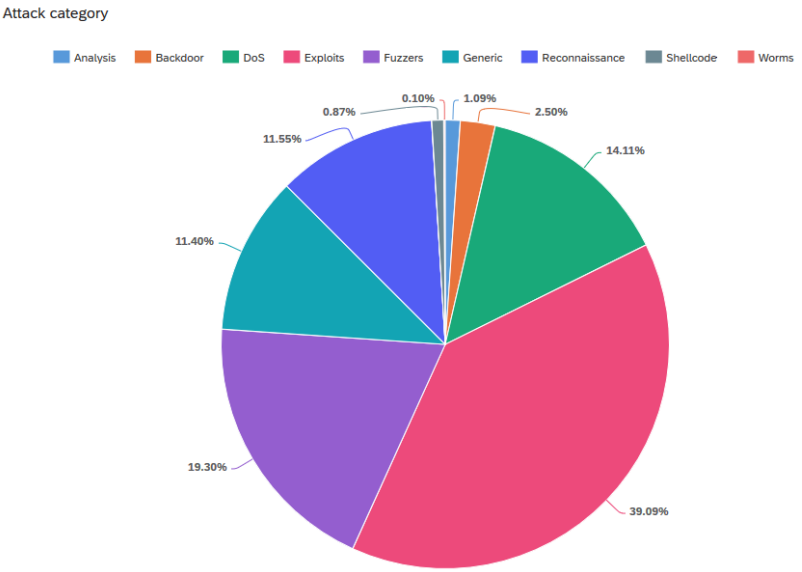


Рис. 1. Диаграмма категорий атак

Из диаграммы видно, что самая распространенная атака — это Exploits (39,09%). Exploits — это подвид вредоносных программ, они содержат данные или исполняемый код, например, у вас есть браузер, и есть уязвимость в нем, которая позволяет исполнить «произвольный код», то есть установить и запустить некую вредоносную программу на вашей системе без вашего ведома.

Следующей часто встречаемой атакой является Fuzzers (19,30 %) — это файловый фаззинг, подразумевающий, что некой программе предлагается открыть некорректно составленный файл, что может повлечь за собой сбой системы.

Третьей по частоте встречаемости идет атака DoS (отказ в обслуживании 14,11 %) — атака на вычислительную систему с целью довести ее до отказа, то есть, создание таких условий, при которых правомерные пользователи системы не могут получить доступ к предоставляемым системой ресурсам.

Следом с небольшой разницей идут атаки Reconnaissance (11,55 %) и Generic (11,40 %). Reconnaissance (разведывательная атака) — в разведывательной атаке путем перечисления учетных записей злоумышленник использует словарь с тысячами имен пользователей или такие сред-

ства, как KrbGuess, чтобы попытаться угадать имена пользователей в вашем домене. Атака Generic в автоматическом режиме может загружать на ваш компьютер различные вирусы. Так же, ваш компьютер может использоваться и для противоправных действий, к примеру, для DDOS атак.

Остальные 4,56 % занимают следующие атаки: Backdoor (2,50 %) — метод обхода надлежащей авторизации, который позволяет получать скрытый удаленный доступ к компьютеру, Analysis (1,09 %) — прослушивание каналов связи, анализ передаваемых данных и связанной с ними служебной информации для изучения архитектуры построения системы, получения конфиденциальной пользовательской информации, Shellcode (0,87 %) — это часть кода, встроенного во вредоносную программу и позволяющего после инфицирования целевой системы жертвы получить код командной оболочки, Worms (0,10 %) — «компьютерный червь», вредоносные программы, которые способны воспроизводить себя на компьютерах или через компьютерные сети.

Из вышеперечисленных атак видно, какие встречаются чаще всего и как они действуют на нашу информационную систему. Интеллектуальный анализ позволил установить ключевые факторы, которые оказывают влияние на категории атак. Сильное влияние оказывают начальный порт и порт назначения (рис. 2).

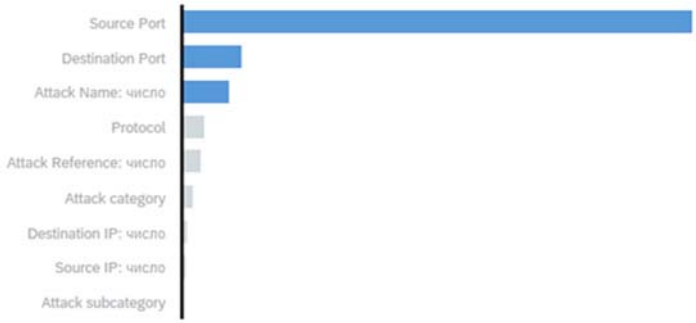


Рис. 2. Ключевые факторы

Для борьбы с такими атаками необходимо использовать антивирус, например, Kaspersky или ESET NOD32, они обнаружат большинство вирусов, заблокируют их распространение и сообщат вам об этом.

Е. А. Патрашкина, А. Е. Баринов
Южно-Уральский государственный университет — НИУ, г. Челябинск

Гибридные и виртуальные стенды для изучения АСУ ТП

Аннотация. Система информационной безопасности на предприятиях с автоматизированным технологическим процессом настолько же распространена, как и проектирование самой АСУ ТП. В работе рассматриваются основные реализации стендов для исследования безопасности АСУ ТП.

Ключевые слова: информационная безопасность; АСУ ТП; стенды АСУ ТП.

В последние несколько десятилетий все популярнее становится автоматизация процессов производства. На многих предприятиях внедряются автоматизированные средства управления (АСУ) операциями производственного цикла, технического процесса (ТП).

С развитием технологий АСУ ТП преобразовались из закрытых управляющих устройств в многоуровневые промышленные сети на базе стандартных сетевых протоколов. Они имеют множество сходных с корпоративными сетями признаков, в том числе и уязвимостей, которые тесно связаны с угрозами кибербезопасности.

Эти сети подвержены заражению компьютерными вирусами, взлому, выводу из строя программного обеспечения (ПО) и другим видам внешнего воздействия.

Одним из методов исследования информационной безопасности АСУ ТП является разработка стендов. Они представляют собой некий макет системы управления и позволяют находить слабые стороны АСУ ТП без вреда для нее самой.

На данный момент существует множество реализаций стендов информационной безопасности АСУ ТП. Все они направлены на тестирование безопасности, проверку новых методов обеспечения безопасности и позволяют:

1) моделировать технологический процесс;
2) моделировать системы передачи данных;
3) апробировать решения по аудиту технических средств АСУ ТП;
4) апробировать угрозы информационной безопасности АСУ ТП;
5) апробировать решения по обеспечению информационной безопасности АСУ ТП;
6) апробировать решения по оптимизации производственных процессов.

Под физическим стендом стоит понимать макет, который полностью или частично повторяет технический процесс. За частую данные

стенды являются выставочными образцами и служат для наглядной реализации угроз информационной безопасности (ИБ) и применения мер по защите.

К этому виду можно отнести стенды компании Infowatch & Инжиниринговый центр НИЯУ МИФИ, такие как:

— «Комплекс телемеханических средств объектов электроэнергетической отрасли»;

— «Модель населенного пункта (промышленный и жилой сектор, транспортная узел)»;

— «Автоматизированный склад».

Также разработкой стендов информационной безопасности АСУ ТП занимается Лаборатория Касперского. Одним из ее продуктов является демонстрационный стенд, который представляет собой модель промышленного объекта, состоящего из конвейера с фрезеровальной головкой, программируемого логического контроллера (ПЛК), компьютера с автоматизированной системой управления технологическим процессом (АСУ ТП) и рабочей станцией инженера [1].

Главный минус данных стендов — они достаточно громоздкие и являются решением только для определенной системы. Для другого производственного процесса придется разрабатывать абсолютно новый стенд, проектирование и создание которого требует силы, время и много денег.

Обратная их сторона — полностью виртуальные стенды для исследований в области ИБ АСУ ТП. Они также описывают систему управления, но при этом не занимают большие площади, так как все его части, включая эмуляцию физических сигналов и распределенный ввод/вывод размещены в полностью виртуальной среде. Следовательно, их проще использовать, нежели физические стенды. Подобные подходы описаны в работах [2; 3].

Подход в работе [3] является примером гибридного стенда; а полностью виртуальный стенд [2], созданный в ЮУрГУ, отличается тем, что все его части, включая эмуляцию физических сигналов и распределенный ввод/вывод размещены в полностью виртуальной среде.

Данный стенд описывает один из процессов сталелитейного цеха. Части системы представляют собой отдельные виртуальные машины (схема информационной среды стенда представлена на рис. 1).

Недостатком таких систем является невозможность полной виртуализации некоторых специфических компонентов АСУ ТП. Например, программируемые логические контроллеры (ПЛК), в зависимости от производителя могут иметь разный синтаксис встроенного ПО. Кроме

того, невозможно быть уверенным, что при одинаковом ПО в «виртуальном» ПЛК и в реальном, они будут работать одинаково, особенно в части компонентов, зависимых от временных параметров (синхронизация и т.д.).

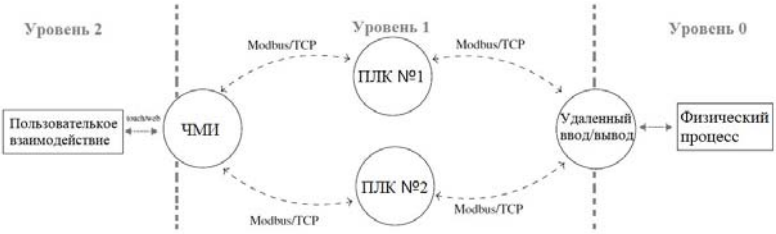


Рис. 1. Схема информационной среды [3]

Гибридные стенды для исследования информационной безопасности автоматизированных систем управления технологическими процессами на данный момент не имеют достаточного распространения, поэтому среди русскоязычных специалистов в области защиты информации они еще не обсуждаются на должном уровне. Такие стенды представляют собой виртуальный стенд, дополненный физическими, реальными компонентами. Для простоты реализовывать физически проще всего контроллеры, или хотя бы один контроллеров, которые есть в системе. Для примера, можно рассмотреть виртуальный стенд [2] и немного видоизменить его.

Для этого достаточно хотя бы один виртуализированный ПЛК заменить на реальный. Допустим, это будет ПЛК № 1. Выделим его на схеме (рис. 2).

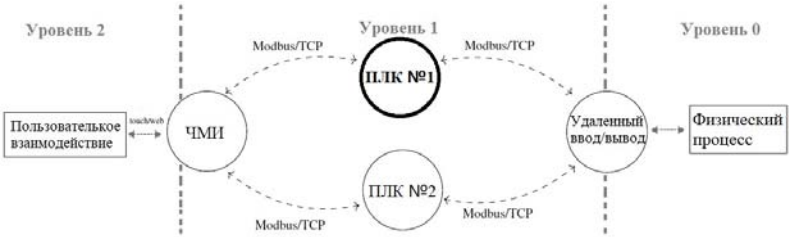


Рис. 2. Информационная схема гибридного стенда

В таком случае, появится больше возможностей в исследовании ИБ АСУ ТП, от реализации угроз до апробирования новых мер защиты.

Таким образом, мы получаем универсальный вариант между физическими и виртуальными стендами в виде гибридных стендов. По сравнению с физическими аналогами гибридные стенды должны иметь относительно маленькие размеры и меньшую стоимость производства. Это даст нам возможность, не привязываясь к определенному техническому процессу, разрабатывать системы, способные давать колоссальные результаты в области информационной безопасности автоматизированных систем управления.

Библиографический список

1. *Шипулин А.* Российские демонстрационные стенды и исследовательские лаборатории по безопасности АСУ ТП. URL: https://bis-expert.ru/blog/8463/50472.

2. *Barinov A., Beschastnov S., Boger A., Kolpakov A., Ufimtcev M.* Virtual Environment for Researching Information Security of a Distributed ICS // 2020 Global Smart Industry Conference (GloSIC). Chelyabinsk, Russia, 2020. P. 348–353.

3. *Sauer F., Niedermaier M., Kießling S., Merli D.* LICSTER — a low-cost ICS security testbed for education and research: a preprint. URL: https://arxiv.org/pdf/1910.00303.pdf.

А. И. Пономарева, М. В. Тарасова
Уральский государственный экономический университет, г. Екатеринбург

Анализ уязвимости сети хранения цифровых данных Storage Area Network

Аннотация. Рассматривается и анализируется сеть хранения данных Storage Area Network (SAN). SAN обеспечивает данным гарантированную полосу пропускания, предотвращает появление единой точки отказа системы, предоставляет доступ к практически неограниченному масштабированию не только со стороны серверов, но и со стороны информационных ресурсов.

Ключевые слова: защита информации; хранение данных; уязвимости системы хранения; высокоскоростная сеть; риск.

SAN — это не что иное, как высокоскоростная сеть, которая устанавливает соединения между устройствами хранения и серверами[1]. Сегодняшние приложения очень ресурсоемкие, из-за количества запросов, которые необходимо обрабатывать одновременно в секунду. Возьмем

[1] *Программно-аппаратные* средства защиты информации. URL: https://otherreferats.allbest.ru/programming/00152155_0.html.

пример веб-сайта электронной коммерции, где тысячи людей размещают заказы в секунду, и все они должны быть правильно сохранены в базе данных для последующего поиска. Технология хранения, используемая для хранения таких баз данных с высоким трафиком, должна быть быстрой в обслуживании и реагировании на запросы (вкратце, это должно быть быстрым на входе и выходе). В таких случаях, мы можем использовать SAN.

Плюсы SAN:

1) высокая надежность доступа к данным, находящимся на внешних системах хранения. Независимость топологии SAN от используемых СХД и серверов;

2) централизованное хранение данных (надежность, безопасность);

3) удобное централизованное управление коммутацией и данными;

4) перенос интенсивного трафика ввода-вывода в отдельную сеть, разгружая LAN;

5) высокое быстродействие и низкая латентность;

6) масштабируемость и гибкость логической структуры SAN;

7) возможность организации резервных, удаленных СХД и удаленной системы бэкапа и восстановления данных.

Минусы SAN:

1) более высокая стоимость;

2) сложность в настройке FC-систем, FC — класс протоколов, использующихся для высокоскоростной (гигабитной) передачи данных;

3) необходимость сертификации специалистов по FC-сетям (iSCSI является более простым протоколом);

4) более жесткие требования к совместимости и качеству компонентов[1].

Уязвимости сети хранения цифровых данных Storage Area Network.

SAN имеет высокий риск несанкционированного доступа по открытым каналам, так как все узлы расположены в одной сети. Взлом одного или нескольких узлов в корпоративной сети хранения данных, в большинстве случаев, приводит к ужасным последствиям для бизнеса. Потенциальные уязвимости определяют составляющие элементы и свойства архитектурных решений сетей хранения, собственно:

— элементы архитектуры;

— аппаратные платформы;

— системное программное обеспечение;

— условия эксплуатации;

[1] *Основные* системы хранения данных и их особенности. URL: https://www.anti-malware.ru/data_storage_technologies_review#_Toc226177806.

— территориальное размещение узлов сети хранения.

Остановимся на наиболее присущих уязвимостях решений SAN. Рассмотрим по уровням предоставления необходимых служб.

Выделим три уровня:

— уровень устройств;

— уровень данных;

— уровень сетевого взаимодействия.

1. Уровень устройств.

Наиболее распространенная угроза несанкционированного доступа к устройству возникает в результате слабой парольной защиты и непродуманной схемы авторизации пользователя. В результате несанкционированный доступ с полными правами дает полный контроль над этим узлом, что создает реальную угрозу нарушения целостности архитектуры и хранимых данных[1].

2. Уровень данных.

В архитектуре SAN несанкционированный доступ с правами администратора дает пользователю полный или частичный контроль над данными, что приводит к риску блокирования доступа, искажения, модификации или уничтожения данных. Существует огромный риск получения контроля доступа к блокам данных на уровне сервера. Несмотря на то, что блочный доступ к хранимым данным присущ архитектуре SAN, сами вычислительные узлы, если активированы соответствующие сервисы, могут обеспечить доступ по протоколам CIFS/ SMB, а также NFS, что в ряде случаев не гарантирует должного уровня защиты.

Не стоит забывать, что на сегодняшний день наиболее актуальной является проблема нарушения доступности и целостности хранимых данных из-за внешних DoS-атак, вирусов и «червей». Основная цель этих атак заключается в ухудшении имиджа компании и ее финансового положения на рынке, а также получении доступа к данным.

3. Уровень сетевого взаимодействия.

Существует риск несанкционированного подключения к каналам с искажением адреса не только в дата-центрах, но и в филиалах. Благодаря открытой архитектуре и взаимной удаленности коммутационного и преобразовательного оборудования, устройства могут стать объектами атаки с последующей потерей контроля над каналами и несанкционированным доступом к передаваемым данным. Неправильно настроенные конечные устройства сети хранения данных также становятся привлекательной мишенью для сетевых атак.

На сегодняшний день в сети хранения данных не уделяется должного внимания решению вопросов информационной безопасности, что

[1] *Безопасность* в системах хранения данных. URL: https://www.osp.ru/lan/2005/07/140778.

может привести к непредвиденным последствиям. Долгое время защита данных была сосредоточена на надежности их хранения. По мере того как архитектура становится все более открытой, ее элементы (серверы, коммутаторы и т. д.) становятся мишенями для различного рода атак из-за возможных уязвимостей, что приводит к потере информации и ее искажению. Мы надеемся, что рассмотрение выявленных уязвимостей в этой сети хранения данных заставит нас по-новому взглянуть на задачи, которые необходимо решить при организации сетей хранения данных.

Д. П. Салалайко, Р. А. Симбирцев, Д. М. Назаров
Уральский государственный экономический университет, г. Екатеринбург

Антивирусное программное обеспечение на основе искусственного интеллекта как средство защиты цифровых данных в информационном пространстве

Аннотация. Защита цифровой информации от вредоносных программ осуществляется с помощью антивирусного программного обеспечения. Рассматриваются популярные интеллектуальные системы обнаружения вредоносного ПО, их преимущества и недостатки.
Ключевые слова: антивирус; защита информационных систем; данные; несанкционированный доступ; искусственный интеллект; кибербезопасность.

Введение. Вопросы кибербезопасности представляют собой ключевую проблему цифровой экономики, основу которой представляют собой данные. Кибербезопасность стала основной потребностью в обеспечении устойчивой защиты пользователей онлайн услугами в цифровом пространстве Учитывая стремительный рост технологических решений, киберугрозы становятся интеллектуальнее и сложнее, поэтому меры кибербезопасности нуждаются в постоянной адаптации с учетом появления новых угроз в информационных системах. Выявление, характеристика и классификация таких угроз и их источников необходимы для функционирования и развития устойчивой киберэкосистемы, поэтому существует много компаний, которые разрабатывают программное обеспечение, позволяющее эффективно противостоять этим угрозам. Одним из классов такого программного обеспечения является антивирусное программное обеспечение[1].

Средство антивирусной защиты — это программное средство, реализующее функции обнаружения компьютерных программ, либо иной

[1] *Zubair S., Ahmed M., Sikos L. F., Najmul Islam A. K. M.* Toward a Sustainable Cybersecurity Ecosystem // Computers. 2020. No. 9 (3). P. 74. DOI: 10.3390/computers9030074.

компьютерной информации, предназначенных для несанкционированного уничтожения, модификации, блокирования, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирования на обнаружение этих программ и информации. Антивирусное программное обеспечение (антивирусное ПО) является важным элементом в системе защиты информации на устройствах пользователей. На данный момент существующее антивирусное ПО и используемые в нем методы защиты не всегда может в должной мере выполнить функции защиты. Од-ним из трендов XXI в. в разработке антивирусного ПО является использование методов искусственного интеллекта[1].

Сравнение традиционного антивирусного ПО и интеллектуального антивирусного ПО. Традиционный антивирус использует сигнатуры файлов и данных, а также анализ шаблонов для сравнения потенциальной вредоносной активности с предыдущими экземплярами. Антивирус знает, как выглядит вредоносный файл, и может быстро изолировать его в так называемую карантинную зону, чтобы остановить заражение системы. Данный тип антивирусного ПО использует три вида сканирования файлов: полное сканирование (жесткие диски, системная память, элементы реестра, резервное копирование системы, файлы автозагрузки), выборочное сканирование, быстрое сканирование (часто заражаемые файлы и папки, системная память, эле-менты реестра, файлы автозагрузки)[2].

В настоящее время наряду с традиционным существует антивирусное программное обеспечение, основанное на технологиях машинного обучения и искусственного интеллекта (ИИ-антивирусы). ИИ-антивирусы используя информацию и данные сетевых сред пытаются на ее основе выявить конкретные угрозы и выполнить защитные действия автоматически (без подсказок и инициатив пользователей).

Для этого ИИ-антивирусы используют сложные алгоритмы машинного обучения и с помощью них определяют базовый уровень безопасности для сетевых информационных систем. Любые отклонения от базового уровня фиксируются и воспринимаются, как потенциальная угроза[3].

Не только антивирусные программы могут иметь искусственный интеллект, но и вредоносное программное обеспечение. Так компания

---

[1] *These* 4 Antivirus Tools Are Using AI to Protect Your System. URL: https://www.makeuseof.com/tag/artificial-intelligence-antivirus-tools.

[2] *The* 3 Types of Antivirus Scans and When to Use Each One. URL: https://www.makeuseof.com/tag/antivirus-scan-types.

[3] *These* 4 Antivirus Tools Are Using AI to Protect Your System. URL: https://www.makeuseof.com/tag/artificial-intelligence-antivirus-tools.

IMB Research разработала вредоносное ПО, управляемое искусственным интеллектом (ИИ) под названием Deeplocker, который является одним из страшнейших примеров вредоносных программ. Deeplocker был ПО для телеконференций, на которых он сканировал лица людей, его использовавших. Его цель заразить компьютер конкретного человека, поэтому он следил за всеми. Когда программа обнаруживала лицо цели, она вводила в систему данного пользователя штамм сетевого червя WannaCry (программа вымогатель денежных средств). После заражения программа шифровала большинство файлов на компьютере, предлагая заплатить денежный выкуп за расшифровку, иначе в течение 7 дней с момента активации возможность расшифровки файлов теряется навсегда[1].

Главное отличие традиционных антивирусных программ и ИИ-антивирусов заключается в том, что традиционное антивирусное ПО не может самостоятельно обучаться, адаптироваться в сетевой среде и принимать решения для предотвращения вредоносных действий. Следовательно, ИИ-антивирусы имеют определенное конкурентное преимущество и постепенно будут завоевывать рынок услуг, связанный с использованием антивирусного ПО (см. таблицу).

Антивирусные программы с использованием искусственного интеллекта

Антивирус	Возможности	Недостатки	ИИ
Cylance Smart Antivirus	Полностью полагается на ИИ, чтобы отличить вредоносное ПО от безопасных файлов. Ждет момента исполнения и немедленно сводит к нулю угрозу вредоносного ПО без вмешательства пользователя 2);3)	Позволяет посещать вредоносные сайты, предположительно, что продукт остановит загрузку вредоносного ПО, но он не защищает от фишинговых атак или подобных угроз	+
Malwarebytes Premium	Главным инструментом Malware Premium можно считать интеллектуальную (несигнатурную) защиту. Она строится на отсутствии баз данных, по которой антивирус сравнивал бы коды файлов. Система интеллектуального сканирования построена с учетом поведения, а не кода вирусов.	Возможны некорректные срабатывания системы, поскольку точность алгоритмов ИИ не равна 100%	+

[1] *Вредоносное* ПО DeepLocker Malware с искусственным интеллектом. URL: https://www.make-info.com/deeplocker-ai-malware/; *How* Artificial Intelligence Will Shape the Future of MalWare. URL: https://www.makeuseof.com/tag/artificial-intelligence-future-malware/; *WannaCry* — Википедия. URL: https://ru.wikipedia.org/wiki/WannaCry.

Окончание таблицы

Антивирус	Возможности	Недостатки	ИИ
	Это позволяет избежать их проникновения в систему. В том числе речь идет о мимикрирующем вирусе (переписывающем свой код при проникновении в файл). Несмотря на отсутствие баз данных, такая интеллектуальная защита эффективна. Причина заключается в том, что даже новые вирусы построены на основе логики старых. По крайней мере, они частично используют их методы, чем выдают себя. За счет этого интеллектуальная система обнаруживает вредоносное ПО еще на начальной стадии заражения 1);2)	Возможны некорректные срабатывания системы, поскольку точность алгоритмов ИИ не равна 100%	+
Deep Instinct D-Client	Использует глубокое обучение, для обнаружения любого файла, прежде чем с ним будут проводиться какие-то операции или он будет доступен, а также использует статический анализ файлов в сочетании с моделью прогнозирования угроз 3)	Точность модели, используемой в этом антивирусе не идеальна. Возможны ложные срабатывания	+

Примечание: + означает присутствие ИИ в антивирусном ПО; − отсутствие ИИ в антивирусном ПО. Источники: *Malwarebytes:* кибербезопасность для систем Windows, Mac, Android и iOS. URL: https://ru.malwarebytes.com; *14 Premium* Antivirus to Security your Computer. URL: https://geekflare.com/premium-computer-antiviru; *These 4* Antivirus Tools Are Using AI to Protect Your System. URL: https://www.makeuseof.com/tag/artificial-intelligence-antivirus-tools.

Вывод. Преимущества антивирусных ПО с использованием «искусственного интеллекта» заключаются в том, что с помощью своего ИИ антивирус способен найти наилучшее решение для защиты операционной системы без предварительных настроек и вмешательства со стороны пользователя. Особенностью антивируса является уменьшение нагрузки на систему за счет того, что сканирование проводится в промежутки, когда ОС пребывает в режиме ожидания и просканированные ранее чистые файлы пропускаются. Обычные антивирусные программы, которые не применяют ИИ оказываются бессильными перед лицом современных угроз, поскольку слишком медленно реагируют на атаки.

М. А. Сидоров, Б. В. Мамин
Уральский государственный экономический университет, г. Екатеринбург

Методы защиты POS-терминалов в торговых точках от потенциальных угроз (атак)

Аннотация. Рассмотрены уязвимости POS-терминалов в торговых точках, а также меры для сохранения конфиденциальной информации.
Ключевые слова: POS-терминал; скриммер; транзакции; угрозы; безопасность.

В современных реалиях существует множество угроз, которым подвержено население, одной из них является махинация в сфере товарно-денежных отношений, которая направлена на компрометацию данных платежных карт потребителя.

За последние года число операций, осуществляемых при использовании POS терминалов, существенно возросло, так как их использование значительно облегчает проведение платежных операций и бизнес-процессов. Параллельно с ростом производимых транзакций интерес злоумышленников возрастал в геометрической прогрессии.

POS-терминал — это аппаратно-программный комплекс, позволяющий осуществлять торговые операции, как это делает обычный кассовый аппарат.

Помимо учета продаж, POS-терминал может накапливать и другие данные для их последующего анализа[1].

Процедура оплаты в обычном магазине представляет из себя следующий алгоритм:

1. Покупатель проводит картой по считывателю терминала для оплаты своих покупок.

2. Данные банковской карты покупателя поступают в терминал далее поступая в POS-систему.

3. POS-система связывается с PSP[2], который в зависимости от типа банковской карты, обращается в банк для прохождения процедуры авторизации транзакции.

4. При успешном прохождении процедуры, код авторизации возвращается из банковской сети в PSP и передается в POS-систему и терминал.

Схема работы представлена на рис. 1.

[1] *Wikipedia*. URL: https://ru.wikipedia.org/wiki/POS-терминал.

[2] *Payment* Service Provider − юридическое лицо или его структурное подразделение, обеспечивающее информационное и технологическое взаимодействие между участниками расчетов (*Артимович Д. А.* Электронные платежи в интернете. М.: Де'Либри, 2018).

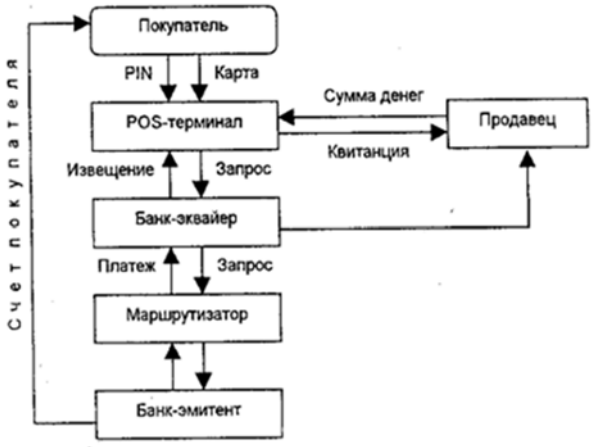


Рис. 1. Схема работы POS-системы при проведении транзакции

Во время запуска POS-терминалы синхронизируют время и получают обновленные параметры с сервера магазина, включая цены на товары, информацию об их наличии и другие служебные данные. После этого кассиры могут залогиниться за своими рабочими местами и начать работу. Каждое действие на кассе записывается в Log-файл[1] (далее логи).

В конце дня менеджеру необходимо повторить процедуру в обратном порядке: сначала закрыть кассы, а после — магазин. После этого действия ни одна транзакция не может быть проведена до открытия магазина. Во время закрытия POS-терминалы отправляют свои логи на сервер. Это и есть те бизнес-процессы, о которых упоминалось выше. Именно их POS-системы позволяют упростить и облегчить.

Однако ни одна система с участием финансов не обходится без внимания субъектов, которые заинтересованы в получении данных и денег участников транзакций. Миру известны инциденты кражи данных банковских карт и заражения POS-терминалов организаций.

Одним из таких случаев является хакерская атака на торговую сеть «Target». В результате инцидента были скомпрометированы более 40 млн банковских карт и данные более 70 млн клиентов компании. За месяц злоумышленникам было добыто более 11 Гб информации составляющей ценность[2].

[1] *Log*-файл — специальный файл, в котором накапливается собранная служебная и статистическая информация о событиях в системе (программе).

[2] *Kaspersky* daily. URL: https://www.kaspersky.ru/blog/ohotniki-za-terminalami/2849.

Данный пример является доказательством того, что POS-терминалы являются одним из множества систем, которые имеют свои уязвимости. В Российском законодательстве данная преступная деятельность попадает под статью УК РФ 159 «Мошенничество». О том какие есть на данный момент уязвимости и как их закрывать поговорим дальше.

Наиболее распространенным и простым физическим методом компрометации данных банковской карты является скиммер. Он из себя представляет миниатюрное устройство, которое может крепиться на банкомат или терминал оплаты (рис. 2). Скиммеры проектируются под конкретные модели банкоматов, кассы самообслуживания и платежные терминалы таким образом, чтобы затруднить обнаружение. В каждом скиммере присутствует компонент для считывания карт, состоящая из небольшой микросхемы, которая запитывается от батареи. Вторым компонентом зачастую является небольшая камера, которая записывает область пин-панели, через которую набирают пин-код от банковской карты.

Рис. 2. Скиммер (справа) на платежный терминал Ingenico

Более продвинутым и опасным методом компрометации данных банковской карты является заражение POS-терминала. При всем этом, заражение может нести как локальный характер, так и массовый. Вредоносные программы для POS-терминалов можно различать по объему решаемых задач и характеру похищаемой информации.

RAM-скрапер записывает содержимое ОЗУ. При транзакции все данные с банковской карты обрабатываются именно в оперативной памяти. RAM-скраперы записывают информацию из памяти и пересылают

ее на сервер злоумышленника для дальнейшего анализа, либо сами способны выделять нужную информацию, что избавляет от необходимости анализировать информацию при получении злоумышленником.

Такие программы помимо анализа оперативной памяти записывают и все нажатия клавиш, фиксируя PIN-коды и другую вводимую информацию. Поскольку все транзакции проводятся через компьютер или мобильное устройство, разработка вредоносного кода часто происходит не с нуля: киберпреступники модифицируют уже созданные троянские программы и вирусы, добавляя в них RAM-скраперы для хищения данных с банковских карт. Соответственно, такие экземпляры могут содержать руткиты для скрытия следов активности или бекдоры для удаленного доступа, похищать другую информацию.

Клиент, воспользовавшись терминалом, изначально доверяет и предполагает нормальную работу системы. Для обычного рядового покупателя похищение и передача данных происходит совершенно незаметно. В результате последствия для бизнеса очевидны, покупатель теряет лояльность и доверие к компании.

На данный момент выявление использования вредоносного кода занимает очень много времени так как с начала сбора информации до фактического начала списания средств может пройти месяца, а то и годы. Для устранения данных инцидентов разработано множество мер необходимые для сохранения конфиденциальной информации, например:

— все управляющие POS терминалами компьютеры оснастить актуальными антивирусными программами;

— своевременно проводить обновление «прошивок» терминалов и ПО компьютера;

— все программы, которые могут быть установлены на управляющий компьютер должны быть строго ограничены;

— доступ к управляющим компьютерам и POS терминалам необходимо контролировать и ограничить;

— необходимо настроить шифрование машин и грамотно составить политику безопасности;

— обязательно обучить персонал правилам информационной безопасности.

Также были разработаны технологии выявления физического открытия терминала (анти-тамперинга[1]), к примеру в некоторых терминалах при попытке вскрытия происходит разрыв электрической цепи, благодаря которому устройство перестает функционировать. Аппаратная

[1] *Anti*-tampering (анг) - предотвращения несанкционированного вмешательства.

же составляющая защищена проверкой файлов, во время закрытия кассового дня терминал производит проверку контрольных сумм файлов со сведеньями на сервере, в случае нахождения расхождений производится блокировка терминала.

В совокупности перечисленных мер мы предлагаем также рассмотреть идею с помощью цифровых интеллектуальных технологий произвести сбор данных с терминалов компаний и в последующем обработать их с помощью нейронных сетей для нахождения потенциальных угроз безопасности (рис. 3). Данная мера позволит заранее выявлять угрозы, которые еще не были классифицированы до начала их эксплуатации, и в том числе ранжировать угрозы по степени опасности.

Рис. 3. Использование нейронной сети для нахождения угроз

В заключение можно сказать, что на сегодняшний день рынок POS-систем активно развивается, внедрение вышеперечисленных мер в комплексе поможет компаниям значительно снизить риски атак на свои POS-терминалы и сети, таким образом обеспечив безопасность данных платежных карт своих покупателей.

М. Н. Синадский
Уральский федеральный университет имени первого Президента России Б. Н. Ельцина,
г. Екатеринбург

Модуль генератора шаблонов перемещений в рамках компьютерного полигона по расследованию инцидентов информационной безопасности

Аннотация. С целью проведения практико-ориентированных занятий по изучению информационно-аналитических систем безопасности предложен модуль генератора массивов биллинговой информации о взаимодействии пользователей, учитывающий поведенческую модель абонентов на основе шаблонов перемещений.

Ключевые слова: информационно-аналитические системы безопасности; генератор; биллинговая информация.

В рамках обеспечения информационной безопасности с целью выявления и расследования, в том числе, фактов мошенничества с использованием средств связи применяются информационно-аналитические системы безопасности (далее — ИАСБ). При проведении на потоках по направлению «Информационная безопасность» практических занятий по расследованию компьютерных инцидентов, в ходе которых изучаются ИАСБ, должны использоваться массивы биллинговой информации. При этом использование настоящих данных невозможно, в том числе в силу ограничений, накладываемых федеральным законом «О связи».

Для совершенствования методики обучения и создания условий для проведения практико-ориентированных занятий по изучению аналитических методик в рамках компьютерного полигона Учебно-научного центра «Информационная безопасность» ИРИТ-РтФ УрФУ развернут «Генератор массивов биллинговой информации» [2]. Одна из задач проекта — разработка модулей программного комплекса генератора массивов биллинговой информации, соответствующих реальным массивам по формату данных, статистической и поведенческой модели абонентов.

В рамках проекта реализована генерация массивов биллинговой информации о взаимодействии пользователей в сетях операторов сотовой связи, которая заключается в создании псевдослучайных действий абонентов на основании статистико-событийной модели [1]. Генерация осуществляется с учетом статистических распределений, сгенерированной совокупности имен, фамилий и отчеств с их частотным распределением, случайных неповторяющихся данных IMSI, IMEI, MSISDN, LAC, CELLID, а также шаблонов перемещений.

Для придания итоговому массиву биллинговой информации наибольшей реалистичности поведенческих характеристик абонентов разработан генератор шаблонов перемещений. В модуле реализован алгоритм поведения вымышленных абонентов, основанный на задании их осмысленных перемещений в рамках населенного пункта по заданной территории между базовыми станциями операторов сетей сотовой связи.

Карта населенного пункта (города) разделена на отдельные квадраты. Для каждой клетки квадрата задаются уникальные параметры LAC (Location Area Code — код локальной зоны) и CellID (уникальный номер, предназначенный для идентификации базовых станций) обслуживающих ее базовых станций, которые могут модифицироваться посредством применения списков базовых станций (см. рисунок).

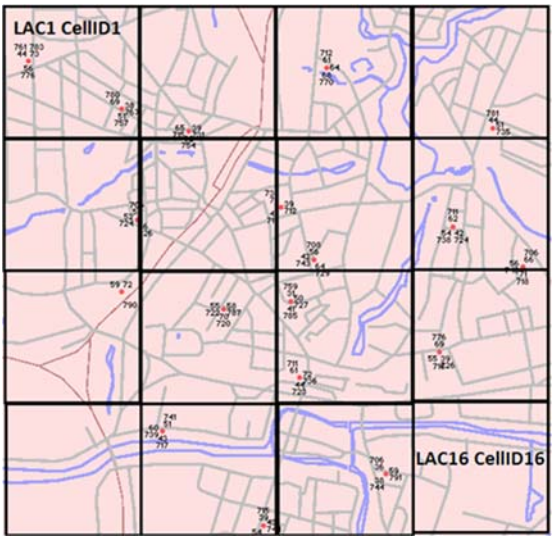


Схема разделения территории на области действия базовых станций

Передвижение абонентов в рамках населенного пункта описывается шаблонами перемещений. Шаблон перемещений представляет собой упорядоченный по времени список LAC и CellID, по которому отслеживается передвижение абонента в течение заданного времени. Так как каждой базовой станции ставятся в соответствие ее прямоугольные координаты, то шаблон перемещений является набором геометок позиций полей карты. Количество меток определяется частотой обновления

геопозиции. Геометка показывает, в каком из участков местности находился абонент в период между обновлениями геопозиции. Коррекция перечня LAC, CellID и их прямоугольных координат на географической карте позволяет формировать биллинг для произвольного населенного пункта.

При генерации биллинга каждому абоненту присваивается один из заранее сгенерированных шаблонов перемещений, что позволяет учитывать различные поведенческие характеристики абонентов. Входными данными для модуля являются: размер квадрата карты, в который вписан город; необходимое количество шаблонов перемещений; частота считывания обновления геопозиции; временные промежутки, в которые абоненты совершают перемещение от объектов «дом» до объектов «работа» и обратно. В зависимости от полученных на вход параметров, определяющих характеристики населенного пункта и поведенческие свойства абонентов, модуль формирует массив шаблонов перемещений, который в дальнейшем используется для учета движения абонентов между базовыми станциями.

Модуль генератора шаблонов перемещений является совокупностью блоков: генерации объектов на карте; инициализации начального состояния; выбора пункта назначения; перемещения между объектами. В начале работы модуля происходит инициализация и считывание входных параметров. Далее осуществляется создание объектов на карте: «домов» (на половине ячеек карты), «работ» (на четверти ячеек карты) и «магазинов» (на четверти ячеек карты). Карта представляет собой упорядоченный список номеров квадратов (ячеек карты), нумерация ведется построчно от 0 и до максимального значения, задаваемого размером города. Следующим шагом создается структура данных абонента: позиции дома, работы, временные метки. Имитация перемещения абонента происходит по временным меткам. При наступлении временного события происходит назначение цели («работа» или «дом») перемещения абонента, вспомогательная функция рассматривает движение абонента по двум осям, и каждый временной промежуток перемещает его на одну геометку ближе к цели. Перемещение между объектами происходит по кратчайшему пути, но если абонент движется от объекта «работа» к объекту «дом», и на пути следования в пределах меры близости оказывается объект «магазин» (при этом признак посещения объекта «магазин» не был определен положительно), то абонент обязательно изменяет траекторию, посещая объект «магазин», а потом продолжает движение к цели — объекту «дом».

Результатом работы является модуль генератора шаблонов перемещений, учитывающий поведенческие характеристики абонентов и характеристики местности — размер поля карты и количество объектов,

размещенных на ней. В формируемом массиве шаблонов перемещений для произвольного количества абонентов задается индивидуальное осмысленное движение по полю карты. Сформированные массивы протестированы с применением ИАСБ «Лампир»[1].

Библиографический список

1. *Семенищев И. А., Синадский А. Н., Синадский Н. И., Сушков П. В.* Синтез массивов биллинговой информации на основе статистико-событийной модели взаимодействия абонентов сетей сотовой связи // Вестник УрФО. Безопасность в информационной сфере. 2018. № 1 (28). С. 47–56.

2. *Semenishchev I., Sinadskiy A., Sinadskiy M., Sinadskiy N., Sushkov P.* Method for Forming the Dynamic Components of Conditionally Real Data Arrays Based on Color Petri Net Algorithms for Organizing a Computer Training Platform for Investigating Information Security Incidents // Proceedings – 2020 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology, USBEREIT 2020. Institute of Electrical and Electronics Engineers Inc., 2020. P. 582−585.

А. Р. Федорова, В. А. Шпак, Г. И. Лукьянов
Магнитогорский государственный технический университет им. Г. И. Носова, г. Магнитогорск

Разработка модуля поиска конфиденциальной информации в аудиофайлах

Аннотация. Проведено сравнение форматов аудиофайлов, рассмотрены их структуры. Определены основные методы стеганографии, применяемые при сокрытии конфиденциальной информации в аудиофайлах, и способы их выявления. Разработана структура ПО и алгоритм функционирования. Рассмотрено реализованное ПО для поиска конфиденциальной информации в аудиофайле и проведена оценка работы.

Ключевые слова: стеганография; сокрытие данных; конфиденциальная информация; теги аудиофайла; спектрограмма аудиофайла; обложка аудиофайла.

Огромное количество медиа информации, а также плохое регулирование авторских прав дают свободу для внедрения стеганографии. Информационная достаточность форматов хранения аудиоданных выделяет места для сокрытия конфиденциальной информации в аудиофайлах. Спрятать информацию может оказаться просто, но найти стегосообщение будет проблематично, поэтому цель данной работы — разработать модуль поиска конфиденциальной информации, который позволит выявлять скрытые данные в аудиофайлах методами стеганографии [2].

[1] *Data* analysis & OSINT tool for everyone. URL: https://lampyre.io.

В данный момент стоит проблема стеганографии в аудиофайлах, а также вдобавок к этому на рынке отсутствуют программы, позволяющие проводить комплексный анализ аудиофайлов на следы скрытой информации.

Поэтому создание такой программы очень актуально для решения современных проблем, связанных с утечками информации и скрытой ее передачи [1; 3].

Рассмотрим сравнение форматов аудиофайлов (см. таблицу).

Сравнение форматов аудиофайлов

	MP3	WAV	OGG
Обложка	+	–	–
Метаданные	ID3v1 ID3v2 ID3v3	RIFF XMP	RDF XML-семейство (включая RDF, CMML и XMP) XML-метаданные MusicBrainz Ogg Skeleton
Содержимое заголовка	Frame sync MPEG version Layer ID CRC Bitrate ID Sampling frequency ID Personal Bit Channel Expansion mode Author rights Original	ChunkId ChunkSize Format Subchunk1Id Subchunk1Size AudioFormat NumChannels SampleRate ByteRate BlockAlign BitsPerSample Subchunk2Id Subchunk2Size Data	Capture pattern Version Header type Granule position Bitstream serial number Page sequence number Checksum Page segments Segment table

Анализируя возможность реализации стеганографии в аудиофайлах разных форматов с помощью программ, распространяемых в свободном доступе, можно выявить следующие места, где может быть спрятано стегосообщение[1].

1. Теги. Они позволяют хранить, а также сохранять какие-либо не стандартные данные, поэтому в них можно спрятать стегосообщение. К примеру, некоторые программы хранят там настройки громкости

[1] *Спрятать* файл в аудиозапись. URL: http://www.spy-soft.net/spryatat-fajl-v-kartinku-muzyku/; Прячем секретные файлы внутри аудиозаписи как Мистер Робот. URL: https://pikabu.ru/story/pryachem_sekretnyie_faylyi_vnutri_audiozapisi_kak_mister_robot_deepsound_5854241.

и нормализации для каждого отдельного файла. Медиа-плееры, как правило, не отображают не известные им параметры.

2. Обложка. В файле обложки аудиозаписи, которая находится в теге, можно дописать после IEND чанка какой-то текст, причем файл так и будет определяться как изображение. Более того, абсолютно никаких искажений не будет замечено. Сравнив HEX представление содержимых аудиофайлов, можно увидеть, что дописанный шестнадцатеричный код после IEND чанка — стегосообщение.

3. Спектрограмма. В нашем случае она является дополнительным объектом аудиофайла. Для того, чтобы скрыть стегосообщение в спектрограмме выполняется следующий алгоритм: создается картинка, на которой написан нужный текст и далее при помощи программы формируется аудиозапись.

Рассмотрев сравнение аудиофайлов, а также определив места сокрытия данных, перед началом реализации ПО была разработана схема его функциональных возможностей (см. рисунок).

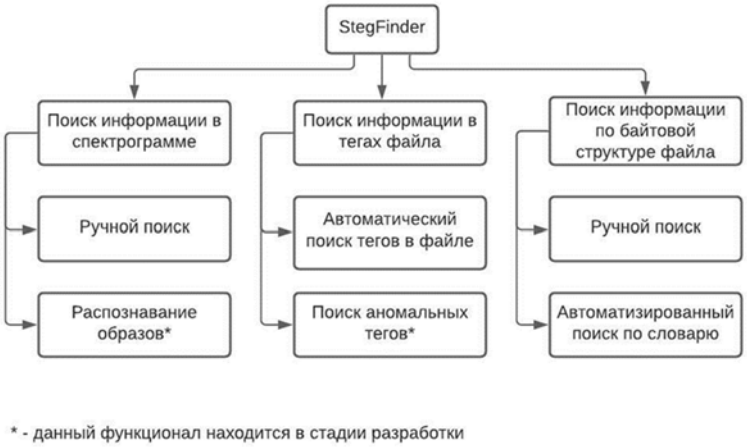


Схема функциональных возможностей ПО

ПО реализовано таким образом, что при загрузке аудиофайла приложение выводит спектрограмму используя библиотеку Bass.Net. Параллельно с этим раскладывает аудиофайл на последовательность байтов, в которой, если знать правила, можно отыскать теги используя библиотеку TagLib. Они помечены особой меткой, состоящей из трех букв «f». Поиском по массиву байтов, преобразованного в 16-ричную систему,

приложение находит начало тегов и по определенным в коде правилам конвертирует следующие за меткой значения в значения тегов, а именно: битрейт аудиофайла, частоту дискретизации и режим канала, а также дату сведения аудиофайла. Так как есть возможность скрывать сообщения в комментариях или иных местах, в приложении мы реализовали поиск по ключевым словам. Был создан текстовый файл с данными, утечку которых допустить нельзя и также добавили эти данные в аудиофайл. ПО проводит поиск по файлу на наличие совпадений с этими словами.

Библиографический список

1. *Баранкова И. И., Михайлова У. В., Лукьянов Г. И.* Формирование компетенций специалиста по информационной безопасности // Актуальные проблемы современной науки, техники и образования: тез. докл. 77-й Междунар. науч.-техн. конф. (Магнитогорск, 22–26 апреля 2019 г.). Магнитогорск: МГТУ, 2019. С. 428

2. *Жиляков Е. Г., Лихолоб П. Г., Кисиленко А. В.* Метод скрытой упаковки сведений в файлы речевых данных // Вопросы радиоэлектроники. 2014. Т. 4, № 2. С. 100−108.

3. *Михайлова У. В., Лукьянов Г. И., Тихомиров С. Э.* Выявление внутреннего нарушителя с применением анализа трафика локальной сети предприятия // Актуальные проблемы современной науки, техники и образования: тез. докл. 77-й Междунар. науч.-техн. конф. (Магнитогорск, 22–26 апреля 2019 г.). Магнитогорск: МГТУ, 2019. С. 399−400.

Информационная безопасность в условиях цифровой экономики Российской Федерации

А. С. Артамонова, О. С. Голубош
Нижегородский институт управления — филиал РАНХиГС, г. Нижний Новгород

Проблема информационной безопасности как вызов цифровой экономики в Российской Федерации

Аннотация. Анализируется состояние информационной безопасности в современной России, выявляются ключевые проблемы обеспечения информационной безопасности. Представлены тенденции защиты от киберугроз как инновационного направления национальной безопасности.

Ключевые слова: цифровизация; киберпреступность; киберугроза; Российская Федерация; киберпреступник; технология.

В современных условиях проблема обеспечения национальной безопасности страны стоит перед многими государствами мира, в том числе и перед Российской Федерацией. В условиях цифровизации и активного внедрения инноваций буквально в каждую сферу жизнедеятельности встает вопрос национальной безопасности в новом контексте — информационном.

В современных условиях активной цифровизации и информатизации многих процессов жизнеобеспечения, сохранение государственного и национального суверенитета на фоне экономически развитых стран мирового сообществ является для России задачей стратегической важности, именно этим обуславливается высокая актуальность данной работы.

В послании Федеральному собранию от 1 декабря 2016 г. Президентом России было предложено «запустить масштабную системную программу развития экономики нового технологического поколения», которая была утверждена распоряжением Правительства РФ от 28 июля 2017 г. № 1632-р «Цифровая экономика Российской Федерации».

Использование передовых технологий изменяет жизнь в лучшую сторону, однако, необходимо заметить, что в условиях развития цифрового пространства Россия столкнулась с новыми угрозами и опасностями в сфере информационной безопасности[1]. Чтобы не усугубить последствия внешних и внутренних угроз, чтобы они не привели к социальным потрясениям, государству необходимо максимально быстро

[1] *Стратегия* развития цифрового пространства ЕАЭС 2025. URL: http://drussia.ru/wpcontent/uploads/2016/10/strategy.pdf.

и заблаговременно ликвидировать опасность, а также предупреждать возможность ее возникновения. В этом смысле информационная безопасность является довольно значимой подсистемой национальной безопасности страны.

Одна из самых опасных угроз на сегодняшний день — это развитие нового вида преступности — киберпреступности, которая в настоящее время развивается ускоренными темпами [2]. В этих условиях перед государством поставлены следующие задачи: защита персональных данные граждан; безопасность коммерческих информационных систем; защита рабочей среды, технологий и ее инструментов. В настоящий момент киберугрозы и ущерб от действий киберпреступников вышли на второе место в мире после техногенных катастроф.

На информационную среду постоянно оказывают воздействие новые вредоносные программы. Это вынуждает службы информационной безопасности развиваться теми же ускоренными темпами и находить «противоядие» от угроз проникновений [2]. Так, происходят многочисленные атаки doc-файлами на HR-отделы предприятий, фирм и организаций.

Стоит также отметить, что киберпреступникам часто содействуют сами сотрудники организаций. Во многих российских компаниях обмен данными организуется ненадлежащим образом, отсутствуют системы допуска, защита удаленных устройств (например, при работе сотрудников из дома или при использовании корпоративных гаджетов в публичных Wi-Fi). Одной из причин слабой защиты от действий киберпреступников считается низкая зарплата ИТ-персонала, а это в свою очередь приводит к отсутствию высококвалифицированных специалистов, которые умеют выстраивать стратегию по информационной безопасности организации [1].

Так, в статье «Информационная безопасность (рынок России)», опубликованной 11 августа 2020 г. на сайте аналитического центра «TAdviser», ведущей компанией в области защиты информации «Кросс Технолоджис» отмечается возросший уровень зрелости организаций и фирм в области информационной безопасности и цифрового сознания — создаются центры мониторинга кибербезопасности и постепенно внедряются «SOAR системы», которые направлены на автоматизацию и оптимизацию сценариев реагирования в рамках экономических процессов и факторов.

Д. Суховей, директор департамента развития технологий компании «Аладдин Р.Д.» отмечает, что в области информационной безопасности произошла переоценка ценностей и приоритетов: многие компании и организации ставят вопросы информационной безопасности на приоритет-

ное место в рамках их развития, а также организации развивают превентивное воздействие в рамках киберугроз. Так, согласно оценкам аналитического центра «TAdviser», объем рынка информационной безопасности в Российской федерации по итогам 2019 г. достиг 90,6 млрд р., что свидетельствует о росте данного показателя по сравнению с аналогичным периодом 2018 г. на 14 %[1].

С целью снижения возможных рисков информационной безопасности государства, российскими властями предприняты конкретные действенные меры. Одной из них выступает постоянный обмен информацией об информационных инцидентах и технологиях защиты между компаниями и конкретными организациями на международном уровне [1], а также международное сотрудничество российских организаций с Европолом и Интерполом по совершенствованию процедур информирования.

Защита государственной целостности от внешних цифровых угроз обеспечивается также в рамках российской системы образования. Так, сегодня наблюдаются активные темпы развития и распространения цифровой «гигиены» со школьной скамьи [3], которая находит свое отражение в образовательных программах. В учебных заведениях проводятся уроки киберграмотности и осведомленности в вопросах информационной безопасности.

В условиях ускоренного развития киберпреступности свои усилия на обеспечение информационной безопасности направляют и финансовые учреждения: банки защищают свои информационные потоки, используя систему «клиент-банк», которая представляет собой программный комплекс на базе автоматизированной системы расчетов, позволяющей клиентам проводить одновременную обработку банковских документов с рабочих мест, находящихся на удалении друг от друга, используя при этом компьютерную или телефонную связь [3]. Данная система гарантирует высокую степень безопасности, поскольку она фиксирует в журнале операций действия любого пользователя, имеющего доступ к данной системе. Передача данных осуществляется в зашифрованном виде, вход в систему требует введения логина и пароля, а каждое платежное поручение, которое оправляется в системе «клиент-банк», необходимо подтвердить электронными подписями первого и второго лица организации.

Таким образом, Российская Федерация в период активного развития цифровых технологий и вектора развития на информатизацию общественных процессов имеет определенные вызовы в области обеспечения

[1] *Аналитический* центр TADVISER — Государство. Бизнес. ИТ. Информационная безопасность (рынок России). URL: https://www.tadviser.ru/index.php.

информационной безопасности. С каждым днем киберугрозы представляют для российского общества все большую опасность, поэтому перед государством поставлены конкретные задачи для преодоления вышеупомянутых трудностей и эффективного и благополучного развития страны.

Библиографический список

1. *Гундерич Г. А.* Состояние киберпреступности // Научный вестник Крыма. 2018. № 4 (15). С. 11.

2. *Никеров Д. М., Хохлова О. М.* Преступления в сфере высоких технологий в современной России // Вестник Восточно-Сибирского института МВД России. 2019. № 2 (89). С. 82–93.

3. *Самурханов М. С.* Понятие и особенности киберпреступности // Международный журнал гуманитарных и естественных наук. 2020. № 4-3. С. 219–221.

М. В. Афанасьева, Н. А. Федосеев

Магнитогорский государственный технический университет им. Г. И. Носова, г. Магнитогорск

Определение целевого профиля зрелости безопасности промышленного интернета вещей

Аннотация. Промышленный интернет вещей (IIoT) в России находится на начальной стадии ввиду множества факторов. Отсутствие единых стандартов, недооцененная важность защиты IoT-систем, трудности нахождения «правильных» решений в интернете вещей ведут к образованию «дыр» в информационной безопасности. Разработка стратегии защиты от киберугроз является важной частью проектирования безопасных промышленных IoT-решений. В статье определяется целевой профиль зрелости безопасности промышленного интернета вещей. Отмечается, что выбор мер и средств обеспечения безопасности должен быть решением задачи оптимизации ресурсов компании, отвечать интересам бизнеса в условиях внешних и внутренних ограничений.

Ключевые слова: информационная безопасность; промышленный интернет вещей; модель зрелости безопасности; целевой профиль зрелости.

Зрелость безопасности — это мера понимания текущего уровня безопасности, ее необходимости, преимущества и стоимости поддержки[1]. Факторы для взвешивания включают конкретные угрозы, нормативные требования и уникальные риски, присутствующие в среде.

[1] *Рудина Е.* Концепция nudge в обеспечении зрелости безопасности интернета вещей // Технологическая перспектива в рамках Евразийского пространства: новые рынки и точки экономического роста: тр. 5-й Междунар. науч. конф. СПб.: Центр научно-производственных технологий «Астерион», 2019. С. 476–480.

Согласно документу «IoT Security Maturity Model: Practitioners Guide» модель зрелости безопасности представляет собой иерархию доменов, суб-доменов и практик (рис. 1).

Для оценки зрелости модели используют такие аспекты как полнота и специфичность реализации практики[1].

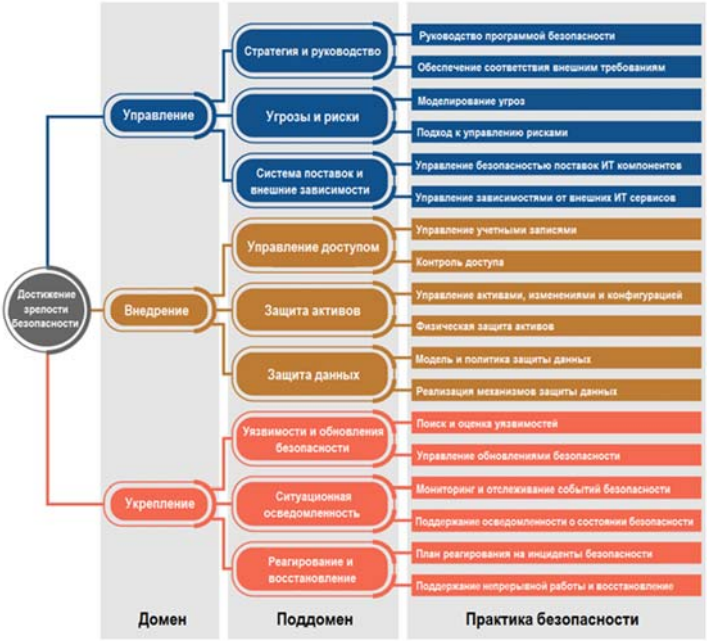


Рис. 1. Иерархия модели зрелости безопасности интернета вещей

Для составления целевого профиля безопасности необходимы четкие характеристики и требования к системе, уточняемые на каждом из уровней полноты:

— минимальный уровень (уровень 1): определяются цели внедрения практики и соответствующие минимальные меры (составление базового представления о безопасности);

— специальный уровень (уровень 2): описываются базовые меры и требования для их поддержки;

[1] *IoT* Security Maturity Model: Description and Intended Use. Version 1.1. 2019-02-15. URL: https://iiconsortium.org/pdf/SMM_Description_and_Intended_Use_FINAL_Updated_V1.1.pdf.

— постоянный уровень (уровень 3): внедрение признанных передовых практик, стандартов, правил и вспомогательных инструментов для обеспечения безопасности системы или организации;

— формализованный уровень (уровень 4): непрерывное улучшение управления программой безопасности, проведение периодического обучения и повышения осведомленности в вопросах безопасности.

Уровень полноты по каждой практики безопасности, к которому необходимо стремится, определяется организацией самостоятельно с учетом потребности бизнеса и особенностями системы.

Но полнота еще не есть зрелость безопасности. Также важно оценивать специфичность реализации практики. Для этого проверяется существуют ли отраслевые требования по каждому домену безопасности, и если да, то присваивается отраслевой уровень. В случае наличия особых требований непосредственно к системе присваивается системный уровень. Отсутствие требований соответствует неспецифичному уровню.

Целевой профиль зрелости безопасности по уровням полноты представлен на рис. 2.

Рис. 2. Целевой профиль зрелости безопасности по уровням полноты системы мониторинга состояния кожуха доменной печи ПАО «ММК»

Рассмотрим определение целевого уровня практики «Обеспечение соответствия внешним требованиям» на примере внедренной системы оценки состояния кожуха 10 доменной печи ПАО «ММК». Эта практика безопасности реализуется при необходимости строгого соответствия развивающимся стандартам безопасности. В силу того, что данный объект относится к критической информационной инфраструктуре (КИИ), необходимо постоянное совершенствование систем безопасности и соответствие нормативным документам по обеспечению безопасности КИИ. Поэтому целесообразно определить целевой уровень полноты данной практики как формализованный.

Установление целевого состояния зрелости с учетом отраслевых и системных требований облегчает создание профилей безопасности. Эти профили фиксируют цель модели зрелости безопасности и могут выступать в качестве шаблона для оценки зрелости безопасности в определенной области использования (общий вариант использования или интересующая система). Сравнение зрелости безопасности целевого состояния и текущего позволяет выявлять пробелы и возможности для улучшения.

В. В. Гамаюнов, М. С. Заверячев
Уральский государственный университет путей сообщения, г. Екатеринбург

Основные векторы атак на производственные процессы, рекомендации по защите от них

Аннотация. Информатизация затронула все аспекты деятельности современных предприятий и производств. Системы управления технологическими и производственными процессами являются важными компонентами в работе производственных предприятий, и их защита требует пристального внимания. Практика показывает, что эти системы уязвимы для атак злоумышленников. В статье выделяются наиболее актуальные векторы атак и предлагаются рекомендации по их предупреждению и нейтрализации.

Ключевые слова: защита информации; защита производственных и технологических процессов.

Стремительное развитие и цифровизация промышленного производства уже является чем-то привычным в современном мире. На протяжении многих лет инженеры и специалисты предприятий оптимизируют производственные и технологические процессы, внедряя в них передовые технологии.

Автоматизированные системы управления технологическими процессами и производством (далее — АСУ ТП) решают задачи синхронизации, координации, финансовой и хозяйственной деятельности, а также

оперативного анализа данных на предприятии. Таким образом, они являются важным компонентом в работе организации и приоритетной целью для злоумышленника. Вопрос защиты подсистем управления производством остается нетривиальным. Так как внедрение новых систем на предприятии, как правило, идет постепенно и может растягиваться на значительные промежутки времени, сложно отследить степень защищенности отдельного компонента структуры. К тому же, в большинстве случаев, используется оборудование зарубежного производства, что затрудняет оценку защищенности системы. Сложившаяся ситуация создает предпосылки на проведение атак злоумышленником на информационные системы предприятия с целью получения выгоды или банального вредительства[1].

Практика показывает, что злоумышленники для реализации атак используют компьютеры операторов и поддержки, системы управления производством, интерфейсы управления «человек-машина», базы данных и внешние подключаемые библиотеки. По данным компании Positive Technologies 85% атак происходит с помощью фишинга. Фишинговые атаки могут проводиться с помощью различных инструментов, таких как: зараженный файл во вложении, web-атаки drive-by compromise, watering hole, strategic web compromise[2].

Следующий вектор атаки может быть направлен на специалистов поддержки. В сложном производстве не обойтись без применения специфичного оборудования. Многие организации прибегают к услугам сторонних организаций технической поддержки таких устройств. Злоумышленник может как провести фишинговую атаку на скомпрометированного поставщика услуг и получить удаленное управление, так и сам представиться им, прибегнув к простым, но действенным методам социальной инженерии. В дополнение к этому хакер может попытаться найти незащищенный канал передачи команд напрямую оборудованию, которые так же не редко встречаются даже у крупных компаний.

В целом векторы атак направлены на:

— компрометацию инженерного АРМ через вредоносную утилиту или уязвимости программного обеспечения для разработки функций автоматизации;

— заражение трояном устройств Industrial Internet of Things (далее — IIoT)[3];

---

[1] *APT*-атаки на промышленные компании в России: обзор тактик и техник // Positive Technologies. URL; ptsecuri-ty.com/ru-ru/research/analytics/apt-attacks-industry-2019/#id3.

[2] *В* 2020 году число атак вымогательского ПО на производства утроилось // Securitylab. URL: Securitylab.ru/news/514061.php.

[3] *Атаки* на производственные системы и IIoT: основные векторы и рекомендации по защите // Securitylab. URL: Securitylab.ru/blog/company/AngaraTech/348380.php.

— уязвимости в программном обеспечении мобильного интерфейса управления «человек-машина»;

— искажение данных на системах управления производством для вызова сбоя в производственном процессе, что приведет к отказу в обслуживании и заблокирует производство;

— использование уязвимой или вредоносной логики автоматизации в сложной производственной машине.

Системы управления производством являются достаточно уязвимыми перед действиями злоумышленников. Большинство APT-группировок, атакующих сегодня российские промышленные предприятия, используют сложные техники, и шансы поймать преступников в момент их проникновения в компанию минимальны. Однако, чтобы обезопасить свое предприятие можно реализовать несколько рекомендаций по защите, которые предлагают эксперты в области информационной безопасности. Для промышленного оборудования и пограничных систем, точек входа в промышленную сеть необходимо:

— провести обзор архитектуры для выявления всех активов, связи и коммуникации между сетями. Определить демилитаризованные зоны для ограничения движения между сегментами;

— построить топологию сети и поведения критических процессов для выявления потенциально слабых мест;

— убедиться, что сети сегментированы в максимально возможной степени. На практике можно реализовать правила брандмауэра для сегментации критических компонентов АСУ ТП из сети, которые можно активировать и деактивировать в зависимости от сохранности и безопасности окружающая среда и любой потенциально вредоносной деятельности;

— услуги и оборудование, которые не требуют подключения в реальном времени или прямой доступ к операциям могут быть виртуализированы. Это способно повысить безопасность при взаимодействии;

— мониторинг исходящих сообщений сети АСУ ТП для обнаружения вредоносных угроз поведения, индикаторов и аномалии;

— проводить фильтрацию сетевого трафика в режиме «белого листа», если возможно — с поддержкой анализа параметров для промышленных протоколов;

— ввести анализ рисков физических и информационных систем, использование доступного мониторинга событий систем средствами SIEM;

— осуществлять контроль целостности среды функционирования как для АРМ, так и для сетевой среды на отсутствие неучтенных сетевых устройств;

— для устройств IIoT осуществлять контроль целостности прошивки и антивирусную проверку используемого программного обеспечения и библиотек;

— использовать цепочку сертификатов в производственных средах;

— использовать «песочницы» и инструменты для обнаружения и распознавания уязвимостей и программных закладок;

— разделить привилегии для программного обеспечения промышленного оборудования.

Для реализации перечисленных рекомендаций потребуются ощутимые силы и средства. Сложности в их внедрении добавляет отсутствие практической базы. Однако на рынке решений информационной безопасности уже существуют продукты, направленные на защиту производственных систем. Многие крупные компании имеют готовые решения, которые можно использовать для защиты промышленной среды. Стоит учитывать, что каждое промышленное производство индивидуально. Многие из них развивались в течении десятков лет, в ходе которого обновлялись и переоснащались. Поэтому система защита должна учитывать все особенности производства и специфику информационных потоков. Внедрение и сопровождение системы защиты информации должны проводить квалифицированные специалисты в области информационной безопасности со стороны разработчика данных системы, а для обеспечения функционирования системы защиты необходимо организовать обучение персонала и регулярное повышение квалификации.

В. А. Довыденко
Брянский государственный университет имени академика И. Г. Петровского,
г. Брянск

Анализ деятельности и выявление перспектив развития ПАО «ВТБ» в условиях цифровизации

Аннотация. Изложены ключевые положения стратегии развития ПАО «ВТБ». Проведен анализ деятельности банка, выявлены приоритетные направления развития.
Ключевые слова: ПАО «ВТБ»; стратегия развития; финтех; прибыль; доходы; расходы; кредитный портфель.

В современных условиях степень развития инфраструктуры банковского рынка оказывает непосредственное воздействие на экономическое положение страны в целом[1].

В этих условиях особую актуальность приобретают вопросы изучения результатов деятельности отдельно взятых банков. Сегодня направления по совершенствованию банковского обслуживания реализуют все крупные банки, в том числе и ПАО «ВТБ». Ключевые направления деятельности закреплены в стратегии развития группы «ВТБ».

Стратегия развития ВТБ на 2019−2022 гг. в качестве основных приоритетов определяет следующее.

Во-первых, усиление бизнес-модели в части постановки клиента и его удовлетворенности. Во-вторых, стратегия предусматривает ускорение цифровизации бизнеса. В-третьих, особое внимание уделено построению передовой операционно-технологической платформы. В-четвертых, банк ставит цель ускорить реагирование на изменение рынка и клиентского спроса.

Уже сегодня банк достиг определенного прогресса в сфере совершенствования банковского обслуживания. В 2018 г. специалистами ВТБ были проведены исследования в области финтеха, в результате были пересмотрены IT-процессы в деятельности банка. Внедрение передовых разработок позволяет гармонизировать IT-ландшафт и повысить надежности информационной системы банка. Искусственный интеллект позволяет наиболее качественно анализировать клиентскую базу и индивидуализировать предлагаемые продукты.

Банк также успешно завершил юридические процедуры по присоединению ВТБ24 и уже с 1 января 2018 г. начал обслуживание клиентов под единым брендом.

[1] *Зверев А. В., Мандрон В. В., Мишина М. Ю.* Механизм санации кредитных организаций: российская практика // Финансы и кредит. 2019. Т. 25, № 8 (788). С. 1727−1741.

После объединения банков клиенты розничного бизнеса группы «ВТБ» продолжат обслуживание в привычных офисах (объединенная розничная сеть возросла до 1350 отделений), но уже под новым брендом.

Процесс объединения двух банков представляет собой ключевой стратегический проект новой трехлетней стратегии ВТБ. Этот шаг повлиял на увеличение управляемости и создал общую высоко конкурентную структуру, которая способна обеспечить результативное взаимодействие бизнес-линий в решении совмещенных задач. Объединение поспособствовало достижению значительной оптимизации расходов и улучшило финансовые показатели ВТБ в целом (рис. 1).

Чистая прибыль группы «ВТБ» по итогу 2017 г. продемонстрировала рост на 68,5 млн р. по сравнению с предыдущим годом и составила 120,1 млрд р. В 2018 г. отмечался прирост в 51,2 %, показатель чистой прибыли достиг значения 181,5 млрд р. Рентабельность собственного капитала в 2018 г. составила 12,3 % (целевой ориентир 10%).

Подобные изменения обусловлены стабильным уровнем доходов от основной деятельности, повышением эффективности затрат и снижением расходов на создание резервов. По итогам 2019 г. на фоне высокого роста комиссионных доходов и улучшения качества активов ВТБ достиг показателя чистой прибыли в размере 201,2 млрд р. В 2019 г. банк привлек свыше миллиона новых клиентов, доведя общее количество клиентов до 13,9 млн.

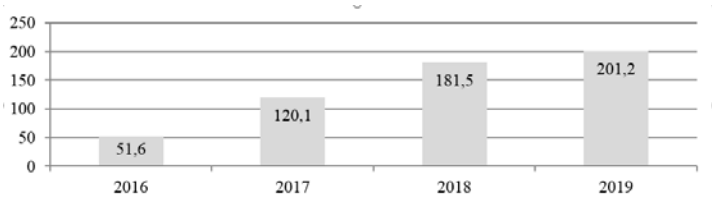


Рис. 1. Динамика чистой прибыли группы «ВТБ» в 2016–2019 гг., млрд р. [1]

Согласно данным рис. 2 более 90% всех доходов группы «ВТБ» приходится на процентные доходы. По результатам 2019 г. этот показатель составил 1039,8 млрд р., что, в свою очередь, свидетельствует о повышении уровня активности банка по сравнению с 2018 г.

Комиссионные и прочие доходы банка в анализируемом периоде составляют менее 10% общей структуры, наибольший прирост отмечен в 2018–2019 гг.

[1] Источник (рис. 1–3): *Официальный* сайт ВТБ. URL: https://www.vtb.ru.

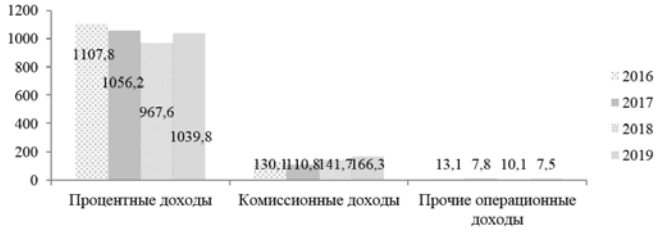


Рис. 2. Динамика доходов группы «ВТБ» в 2016−2019 гг., млрд р.

Подавляющую долю затрат группы «ВТБ» составляют процентные расходы (рис. 3). К ним относят расходы, связанные с уплатой процентов за привлеченные средства (полученные кредиты, остатки на счетах до востребования, срочные депозиты и др.). Комиссионные расходы имеют стабильную тенденцию к увеличению.

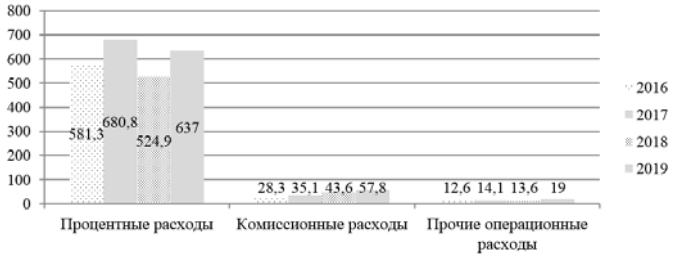


Рис. 3. Динамика расходов группы «ВТБ» в 2016-2019 гг., млрд р.

В рамках действующей стратегии развития ВТБ поставлена цель восстановления динамики кредитования и обеспечения роста кредитного портфеля в общей сложности не менее чем на 10 % в год. При этом стратегия предусматривает опережающий рынок увеличение кредитования физических лиц, а также повышение доли розницы в кредитном портфеле. Доля группы «ВТБ» на рынке клиентских привлечений в корпоративном и розничном сегментах в России по состоянию на 31 декабря 2019 г. составила 20,2 % (снижение на 50 б. п. в 2019 г.) и 15,1 % (рост на 110 б. п. в 2019 г.)[1]. За 9 месяцев 2020 г. группа «ВТБ» показала хорошую динамику операционных показателей. При существенном росте чи-

[1] *Зверев А. В., Мандрон В. В., Мишина М. Ю.* Механизм санации кредитных организаций: российская практика // Финансы и кредит. 2019. Т. 25, № 8 (788). С. 1727−1741.

стых процентных и комиссионных доходов рост расходов был умеренным. На фоне восстановления деловой и потребительской активности после весеннего спада в виду пандемии банк смог достичь значительных темпов роста кредитного портфеля.

Для совершенствования банковского обслуживания как внутри страны, так и в рамках внешнеэкономической деятельности ВТБ стремится регулярно укреплять свою позицию в обслуживании корпоративных и розничных клиентов. В качестве приоритетных задач ВТБ рассматривает усовершенствование различных каналов продаж, например, таких как сеть банкоматов, интернет-банкинг, расширение продуктовой линейки, повышение эффективности продаж, улучшение качества обслуживания клиентов, совершенствование бизнес-процессов и кредитной работы.

Сегодня группе «ВТБ» необходимо совершенствовать свои направления в сфере корпоративного бизнеса. В рамках данного направления следует обеспечить рост кредитования минимум 8 % в год с адаптацией отраслевой структуры портфеля в соответствии с установленными приоритетами совершенствования развития корпоративного бизнеса. Отметим, что целесообразно стремиться к постепенному увеличению доли рынка в средних остатках на текущих счетах и в транзакционном обслуживании корпоративных клиентов с помощью повышения качества сервиса, предложения инновационных продуктов, а также модернизации существующей технологической платформы. Следует уделить внимание диверсификации клиентской базы за счет более конкурентоспособного ценообразования: решению данной задачи будет способствовать формирование улучшенной структуры фондирования, то есть привлечение банком различных ресурсов. Важно развивать реализуемые банковские продукты и расширять географию.

Таким образом, положение ПАО «ВТБ» достаточно устойчивое. Ежегодно банк выполняет ключевые задачи своей стратегии развития. В анализируемом периоде отмечено стабильное увеличение чистой прибыли. В ближайшей перспективе специалисты ВТБ ставят цель улучшить предоставляемые приоритетные инвестиционно-банковские продуктов и услуг и постепенно увеличить долю банка на отечественном рынке.

В. А. Калабин
Уральский филиал Финансового университета при Правительстве РФ,
г. Челябинск

Информационная безопасность в секторе государственного управления в условиях реализации национальной программы «Цифровая экономика»

Аннотация. Определяется роль информационной безопасности в процессе цифровизации сектора государственного управления Российской Федерации. Анализируются основные системные проблемы и уязвимости единиц государственного сектора. На основе международного опыта предлагаются инструменты минимизации ущерба от кибератак.

Ключевые слова: информационная безопасность; сектор государственного управления; цифровизация; информационная система; ретроспективный анализ.

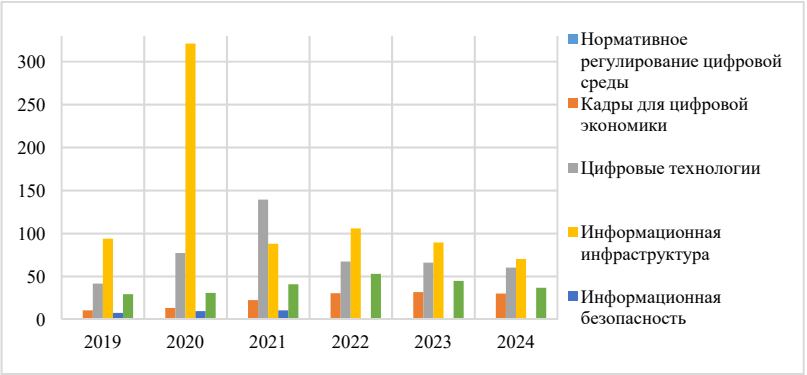
Реализация национальной программы «Цифровая экономика Российской Федерации» заметно ускорила процесс цифровой трансформации сектора государственного управления, который остается крупнейшим ИТ-заказчиком. Среди наиболее распространенных заблуждений можно считать следующую: значительная часть ИТ-расходов идет на создание, развитие и эксплуатацию государственных информационных систем.

В реальности структура затрат органов государственной власти и органов управления государственными внебюджетными фондами состоит из двух частей: инновационной (бюджета развития) и жизнеобеспечивающей (бюджета текущих расходов). При этом, соотношение этих частей в среднем составляет 30/70 %[1]. Такое распределение расходов нередко отражается на информационной безопасности единиц госсектора. Финансовое обеспечение повышения уровня информационной безопасности происходит за счет реализации федерального проекта «Информационная безопасность».

При этом на обеспечение безопасности предусмотрен один из самых низких объемов финансирования (см. рисунок). Это приводит к тому, что в структуре ИТ-расходов у лидеров по затратам на информационные технологии в рамках реализации федерального проекта «Информационная безопасность» занимает незначительные доли: 2,5 % — у Федеральной налоговой службы (общий объем расходов на цифровизацию: 18,1 млрд р.), 1,8 % — у Министерства цифрового развития, связи и массовых коммуникаций (общий объем расходов на цифровизацию:

[1] *ИТ* в федеральных ведомствах России // TAdviser. URL: https://www.tadviser.ru/index.php/Статья:ИТ_в_федеральных_ведомствах_России#

16,8 млрд р.), 7,9% — у ПФР (общий объем расходов на цифровизацию: 14,6 млрд р.)[1].



Финансовое обеспечение национальной программы «Цифровая экономика Российской Федерации», млн р.[2]

На сегодняшний день более двух третей кибератак приходится на сектор государственного управления. В первую очередь, повышению рисков нарушения безопасности информации способствует открытость данных о государственных закупках. Злоумышленники в свободном доступе могут найти информацию об установленном ПО, антивирусных программах, системах мониторинга событий и т.д.

Более того, при исполнении федерального бюджета в 2021−2023 гг. будут применятся следующие коды вида расходов бюджетной классификации: 242 — для закупки товаров, работ, услуг в сфере информационно-коммуникационных технологий (введен в 2011 г. и изначально включал все расходы на ИКТ); (2) 246 — для закупки товаров, работ, услуг в целях создания, развития, эксплуатации и вывода из эксплуатации ГИС[3]. С одной стороны, данная системная мера позволит улучшить систему планирования и учет расходов при управлении ключевыми ИТ-

[1] *Портал* ФГИС КИ. URL: https://portal.eskigov.ru.

[2] *Составлено* на основе паспорта национальной программы «Цифровая экономика Российской Федерации» (распоряжение Правительства РФ от 28 июля 2017 г. № 1632-р «Об утверждении программы „Цифровая экономика Российской Федерации“»).

[3] *О мерах* по обеспечению эффективности мероприятий по использованию информационно-коммуникационных технологий в деятельности федеральных органов исполнительной власти и органов управления государственными внебюджетными фондами: постановление Правительства РФ от 10 октября 2020 г. № 1646.

активами государства. С другой стороны, позволяют API-группировкам более адресно подготовиться к атаке на конкретную систему.

Большую роль в информационной безопасности играет кадровое обеспечение государственных структур. Анализ организационных структур управления цифровой трансформацией государственного сектора позволяет выявить его проблемы. Во-первых, наблюдается дефицит кадров, отсутствие системного обучения сотрудников профессиональным компетенциям в сфере цифровизации и информационной безопасности, недостаточная проработка методов управления имеющимися сотрудниками. По мнению аналитиков, 38% государственных учреждений не уделяют внимания обучению сотрудников основным правилам информационной безопасности, при том, что основным инструментом атаки на госсектор остается фишинг (87%)[1]. Во-вторых, существующие нормативные и финансовые ограничения не позволяют ИТ-специалистам массово входить в постоянный штат государственной структуры. В-третьих, существующий во многих организациях бессистемный подход к цифровизации приводит к переводу в цифровой формат неэффективных и лишних процессов, при этом происходит отсутствие автоматизации в управлении проектами.

Необходимо отметить, что специфика может привести к тому, что государственные структуры будут стремиться выполнять регуляторные и законодательные требования. Это будет означать, что основной объем бюджетных ассигнований будет направляться на разработку и адаптацию документов и внедрение минимально необходимых технических средств защиты. Решением данной проблемы могло бы стать обязательное создание структур по реверс-инжинирингу, что позволит расследовать уже случившиеся инциденты и в будущем обнаружить подобные случаи на ранней стадии.

На более высокую уязвимость госсектора по сравнению с частным сектором влияет медленное обновление цифровых продуктов информационной безопасности, в том числе специализированных средств анализа трафика с возможностью ретроспективного поиска и постанализа. На практике среднее время появления информации о вредоносной атаке в публичном доступе составляет 17 месяцев. По истечению этого срока выходит отчет компании или уведомление от регулятора, содержащие подробное описание техник и тактик, анализ инструментария и индикаторы компрометации. Получив, данные сведения единица сектора государственного управления может запустить ретроспективный анализ, позволяющий выявить проникновения в инфраструктуру, выявить

[1] *ИТ* в федеральных ведомствах России // TAdviser. URL: https://www.tadviser.ru/index.php/Статья:ИТ_в_федеральных_ведомствах_России#

утечки и оперативно принять меры. В большей степени эффективность средств ретроспективного анализа проявляется в том случае, если государственное учреждение является лишь промежуточным звеном в атаке на другую организацию.

Важно отметить, что контролю стоит подвергать не только трафик между корпоративной сетью и интернетом, но и внутриведомственный трафик. В качестве инструментов, обеспечивающих защиту внутренней сети, предлагается применять NTA-решения. Такие системы позволят осуществлять мониторинг обмена файлами, межсерверные взаимодействия, взаимодействия между рабочими станциями пользователей и т.д. Еще одним слабым элементом системы безопасности государственных структур является использование базовых антивирусов. Дело в том, что API-группировки используют такие уязвимости, для которых еще не выпущены обновления безопасности. Детектирование подобных угроз возможно только с применением технологий машинного обучения. Внедрение таких цифровых технологий в ИТ-инфраструктуру государственных структур поможет на основе различных эвристических механизмов, основанных на поведенческом анализе пользователей, выявлять зашифрованные и вредоносные ПО.

Также важно, что большинство современных информационных систем создавались под распространенные продукты Microsoft Office и IE, что делает их уязвимыми для кибератак. Таким образом, необходимо предусмотреть совместимость ГИС с отечественными ПО. Такое взаимодействие позволит безопасно начать взаимодействие государственных информационных систем с экосистемами бизнеса, что позволит, к примеру, интегрировать портал госуслуг с экосистемами крупных игроков бизнеса, а также перенести часть расходов на обсаживание ГИС на корпоративный сектор.

Автор выражает благодарность за помощь в подготовке научного исследования научному руководителю И.В. Балынину, кандидату экономических наук, доценту департамента общественных финансов финансового факультета Финансового университета при Правительстве Российской Федерации.

А. В. Кобяков, С. В. Мухачев
Уральский государственный университет путей сообщения, г. Екатеринбург

Некоторые особенности применения информационных технологий в условиях борьбы с пандемией

Аннотация. Рассматриваются особенности применения информационных технологий в условиях борьбы с пандемией в России. Приведены основные направления использования таких технологий, обсуждается хронология их применения. Отмечены правовые сложности, связанные с вопросами информационной безопасности.
Ключевые слова: информационные технологии; Covid-19; информационная безопасность; цифровой пропуск; правовое регулирование.

Пандемия Covid-19 стала наиболее значимым общемировым явлением последнего года. Она повлияла на все стороны жизни населения земного шара. Информационных технологии стали эффективным инструментом для организации борьбы с пандемией, противодействия распространению инфекции в России. Были задействованы различные информационные системы. Они продемонстрировали возможности оповещения населения, реализации ограничительных мер. Вместе с тем, выявились и определенные сложности, связанные с некоторыми аспектами информационной безопасности, нормативно-правовым регулированием применения информационных технологий в особых условиях пандемии.

Информационные технологии задействованы на всех основных направлениях работы государственных органов.

Для информирования населения наиболее эффективными оказались каналы информирования через СМС-рассылку сообщений и средства массовой информации. И, прежде всего, такая эффективность обусловлена наличием мобильной связи практически у всех граждан.

Следует обратить внимание на некоторые недостатки в организации СМС-рассылки в условиях пандемии Covid-19. Например, отсутствовало широкое и понятное информирование о введении обязательного режима самоизоляции для граждан всех возрастов, когда таковой вводился в регионе; о правилах нахождения на улице; о введении дополнительных требований, таких как обязательное использование лицевых масок; об официальной статистике заражений.

Такое информирование было бы крайне полезно и удалось бы избежать ряда негативных явлений. Другая проблема — распространение недостоверной информации среди населения (а порой и откровенной дезинформации). И в этой ситуации следует дезинформация наиболее опасна.

В борьбу с недостоверной информацией включился Роскомнадзор[1]. Еще одна сложность связана с многократным дублированием информации в рассылках. Хотя понятно, что диктуется это стремлением достичь повышенного внимания, но может приводить к противоположному результату. Повторное отправление сообщений может негативно влиять на восприятие информации, распространяемой по данному каналу, так как психологически это ассоциируется со спамом. Часть получателей блокируют сообщения на своих мобильных устройствах, что сужает масштаб информирования.

Развитие методов информирования населения через средства массовой информации можно рассмотреть на примере Свердловской области. Можно выделить несколько условных периодов. Для начального периода было характерно чрезмерное количество информации об инфекции, распространяемой через СМИ и социальные сети, источники часто недостоверны, интерес граждан к теме максимален. Надежные каналы взаимодействия власти с населением были неустойчивы. Этот период условно длился с 2 марта, когда оперативный штаб сообщил, что у гражданина России, вернувшегося на родину из Италии, подтвердился коронавирус, по 5 апреля 2020 г. Завершение данного периода связано с выступлением Президента России В.В. Путина, в котором разъяснялись меры борьбы с пандемией, текущее состояние, и, в частности, говорилось о том, что нерабочие дни продлены по 30 апреля. Следующий период — промежуточный. Появляются более надежные каналы взаимодействия власти с населением. Интерес населения к тематике, связанной с пандемией, по-прежнему велик. Количество недостоверной информации быстро сокращается. К официальным и надежным источникам информации можно отнести чат Оперативного штаба по Свердловской области, инстаграм-аккаунт губернатора и специальные разделы на интернет-ресурсах средств массовой информации, проходящие модерацию. Этот период длился по 16 апреля. Его окончание можно связать с заявлением губернатора Свердловской области Е.В. Куйвашева о введении режима обязательной самоизоляции.

И, наконец, завершающий, третий период. Количество информации об инфекции в СМИ и социальных сетях постепенно уменьшается. Происходит потеря интереса у населения к тематике, связанной с пандемией, в связи с насыщением информацией. В этот период внимание населения обращается к региональным новостям, что связано с самостоятельностью принятия решений об изменение режима самоизоляции губернатором. Региональные СМИ преимущественно ссылаются на региональные министерства и сообщения губернатора. Устанавливается

[1] *Роскомнадзор* потребовал у СМИ и социальных сетей удалить ложную информацию о коронавирусе. URL: https://rkn.gov.ru/news/rsoc/news72366.htm.

устойчивый канал информирования о пандемии, повышается достоверность информации. Начало этого периода — середина мая, и он продолжается по настоящее время.

Следующее направление — контроль за перемещением здорового населения, т.к. один из главных факторов, снижающих заболеваемость в период пандемии, — максимальное сокращение физических контактов с инфицированными людьми. Были разработаны ограничительные меры, направленные на длительное нахождение граждан дома и получившие название «самоизоляция». Вначале обязательная самоизоляция распространялась только на граждан старше 65 лет, а для иных возрастов она носила лишь рекомендательных характер. Но с 30 марта 2020 г. в Москве ввели обязательную самоизоляцию для всех возрастов. Передвигаться вне жилищ допускалось только по неотложным причинам и к месту работы. На следующий день режим обязательной самоизоляции ввели еще в 26 регионах России. На 2 апреля режим обязательной самоизоляции был введен в 79 регионах, а к 27 апреля во всех регионах был введен режим повышенной готовности. Появилась острая необходимость контроля за перемещением граждан.

Каждый регион решал проблему контроля в соответствии со своими техническими возможностями. В большинстве регионов использовались цифровые пропуска. Однако в нескольких регионах использовались бумажные пропуска, процесс получения и контроля которых стал причиной массовых скоплений людей[1]. Наиболее развитая в техническом и организационном отношении система цифровых пропусков была применена в Москве. Получить пропуск можно было несколькими способами: с помощью интернет-портала mos.ru, звонка по специальному номеру, через СМС-сообщение. О выдаче пропуска заявитель уведомлялся в соответствии со способом оформления заявки. При проведении проверки гражданин был обязан предъявить специальный буквенно-цифровой или QR-код своего пропуска. Разработка и использование цифровых пропусков было сопряжено с некоторыми трудностями. На стадии бета-тестирования приложения «Социальный мониторинг» были отмечены недоработки, связанные с информационной безопасностью: приложение при установке на мобильное устройство запрашивало права доступа ко всей ин-формации, имеющейся в памяти устройства; передавало собранную информацию на серверы без шифрования, использовало зарубежные системы рас-познавания лиц[2]. После официаль-

[1] *Толпы* россиян скопились в очередях за пропусками для автомобилей. URL:https://www.mk.ru/auto/2020/04/03/tolpy-rossiyan-skopilis-v-ocheredyakh-za-propuskami-dlya-avtomobiley.html.

[2] *Приложение* для слежки за москвичами «Социальный мониторинг» убрали из Google Play. URL: https://habr.com/ru/news/t/495088.

ного введения системы цифровых пропусков также обнаружились недостатки. Например, в начале внедрения системы можно было указать любую работающую компанию и получить пропуск, не являясь ее сотрудником. В дальнейшем система цифровых пропусков была подключена к автоматизированным средствам видеофиксации и нарушения регистрировались в автоматическом режиме. Следует отметить, что правовые коллизии, возникшие при реализации системы цифровых пропусков, прежде всего были связаны с обработкой и передачей персональных данных без прямого выражения согласия граждан.

Оповещение граждан о статистике пандемии, режиме ограничения передвижения, особенностях заболевания, мерах профилактики было организовано с применением различных информационных технологий: телерадиовещание, интернет-ресурсы, рассылка СМС-сообщений. Телерадиовещание было задействовано для трансляции обращений главы государства, информационных сводок и разъяснения решений органов власти позволяет охватить большую часть населения. Другой канал информирования — интернет-ресурсы. Перечислим основные. Портал Правительства Российской Федерации Стопкоронавирус.рф содержит официальную информацию о коронавирусе в России. Другой ресурс — «Коронавирус: статистика», созданный Интернет-порталом Яндекс. Он публикует статистическую информацию о динамике пандемии в мире и в России.

Таким образом, информационные технологии нашли широкое применение в условиях борьбы с пандемией. Однако выявились и определенные проблемы, и сложности, связанные с широким применением таких технологий — начиная с психологических особенностей восприятия информации населением и заканчивая проблемами информационной безопасности и нормативно-правового регулирования этой сферы.

А. В. Кулаков
Финансовый университет при Правительстве РФ, г. Москва

Создание безопасной информационной среды Пенсионного фонда Российской Федерации

Аннотация. Рассматривается возрастающая угроза киберпреступлений, оказывающих влияние на деятельность Пенсионного фонда Российской Федерации. Проанализированы меры ПФР для обеспечения безопасности персональных данных, приведены рекомендации по их совершенствованию.

Ключевые слова: киберпреступление; безопасная информационная среда; ПФР; пенсионное обеспечение; цифровизация.

Киберпреступления — новый вид преступной деятельности, появившийся в связи с развитием Интернета (что стимулирует рост прозрачности общественных финансов и активное использование цифровых технологий в процессе управления ими[1]). В Российской Федерации происходит ежегодный рост IT-преступлений — по данным Министерства внутренних дел Российской Федерации, количество таких преступлений в январе — октябре 2020 г. возросло на 75,1 % в сравнении с аналогичным периодом предыдущего года[2]. При этом, около половины киберпреступлений связаны с мошенничеством, в том числе с банковскими картами, а также с попыткой хакеров взломать сервера крупных компаний или государственных органов с целью похищения баз данных о потребителях товаров и услуг, которые затем могут быть проданы или использованы в преступных целях.

К сожалению, основной целью киберпреступников в мире являются и пенсионные фонды, в том числе и государственные. Объемы информации, которые хранятся у пенсионных фондов превосходят многие базы данных за счет большого количество информации, в том числе личной информации, сведения о пенсионных накоплениях и иные. Например, отделения Пенсионного фонда Российской Федерации (далее — ПФР) в Москве, Воронежской и Омской областях и других в 2017 г. был несколько раз «атакован» хакерами с целью похищения баз данных жителей данных регионов, содержащих большое количество конфиденциальной информации. Другой вид мошенничества выявил ПФР и компания «Доктор Веб» — гражданам предлагали ввести данные СНИЛС или

[1] *Балынин И. В.* Повышение пенсионной грамотности населения в контексте обеспечения прозрачности общественных финансов и стимулирования финансовой осведомленности граждан: проблемы и пути решения // Аудит и финансовый анализ. 2019. № 1. С. 161-165.

[2] *Краткая* характеристика состояния преступности в Российской Федерации за январь — октябрь 2020 г. URL: https://мвд.рф/reports/item/21933965.

паспорта для того, чтобы узнать о средствах от частных пенсионных фондов, которые «обязаны делать выплаты всем гражданам России, однако старательно скрывают данный факт». На втором этапе преступники предлагали купить доступ к базам данных частных фондов и моментальный перевод средств от этих фондов[1].

Неизвестно, сколько людей пострадали от подобных обманов, однако можно предположить, что зачастую «целями» мошенников являются именно пожилые люди, которые получают пенсии, или граждане, данные которых находятся в ПФР. В связи с этим перед пенсионными фондами стоит ключевая задача не только в полном обеспечении пожилых граждан заслуженной пенсией, но также и в обеспечении защиты их информации. Подобный тезис высказывал и Ллойд Комори, вице-президент по управлению рисками канадской пенсионной системы муниципальных служащих провинции Онтарио, на Всемирном пенсионном саммите[2]. В своем выступлении Комори остановился на 4 ключевых рисках, которые должны быть учтены при формировании информационной безопасности пенсионных фондов:

1) необходимо чаще оценивать безопасность через проведение внутреннего и внешнего контроля, в том числе со стороны государства;

2) быстрое устранение идентифицированных утечек информации;

3) быть бдительными в отношении привлечения аутсорсинга в части использования облачных хранилищ, так как происходит передача информации, при этом не имеется достаточного представления о безопасности данных, непрерывности или качестве оказываемых услуг партнера по аутсорсингу;

4) сосредоточить внимание на часто отсутствующие формальные процедуры для таких процессов, как разрешение доступа к данным и иные.

Учитывая мировые тенденции, ПФР также стремится обеспечить свою информационную систему, которая бы отвечала необходимым требованиям обеспечения безопасности.

Так, в 2017−2019 гг. компания «Техносерв» создало Центр управления информационной безопасности, который призван решить сразу несколько задач и объединить в себе ключевые источники анализа и сбора основных событий, происходящих в информационных системах фонда (см. рисунок).

---

[1] *ПФР* и ИБ-специалисты предупредили, что мошенники заинтересовались данными СНИЛС. URL: https://xakep.ru/2017/11/23/snils-hunt.

[2] *Pensions* industry underestimating threat of cybercrime, experts warn. URL: https://www.ipe.com/pensions-industry-underestimating-threat-of-cyber-crime-experts-warn/10016222.article.

Основные компоненты и источники событий
для Центра управления информационной безопасности ПФР[1]

Подобная система защиты данных позволяет не только обеспечить их безопасность, но и создавать различные формы отчетности, визуализации и корреляции произошедших событий, что в последующем позволяет предотвратить новые угрозы кибербезопасности.

Однако, несмотря на внедрение комплексной защиты от IT-преступлений, ПФР необходимо непрерывно и комплексно заниматься вопросом обеспечения безопасности.

По мнению автора, этому бы способствовало осуществление следующих «шагов»:

1) создание концепции управления рисками для ПФР, которая будет включать в себя перечень потенциальных угроз информационной безопасности персональных данных граждан;

2) увеличение объема инвестиций в качество управления IT-рисками, которая заключается в поддержке состояния оборудования, повышение квалификации сотрудников и другие мероприятия;

3) мониторинг аутсорсинговых задач с целью снижения стоимости затрат на отдельные инструменты поддержания IT-безопасности, при этом необходимо проводить строгий контроль за сохранностью данных и системой безопасности аутсорсинговой компании;

[1] Источник: *Создание* и развитие Security Operations Center в Пенсионном фонде Российской Федерации. URL: https://globalcio.ru/live/projects/460.

4) внедрение «патч-менеджмента», который предполагает сканирования компьютеров, мобильных устройств или других компьютеров в сети на наличие отсутствующих обновлений программного обеспечения и устранения проблемы путем развертывания этих исправлений, как только они становятся доступными.

В заключение важно отметить, что киберугрозы являются возрастающим вызовом для всех экономических субъектов в связи с развитием технологий, цифровизацией и внедрением электронных баз данных. Однако все перечисленные компоненты необходимо развивать и использовать против IT-преступлений не только в бизнесе, но и в государственных системах, в том числе и Пенсионном фонде России, который обладает большим количеством персональных данных.

По мнению автора, внедрение вышеперечисленных «шагов» в созданный комплекс информационной безопасности позволит обеспечить информационную среду Пенсионного фонда России без киберпреступлений.

Автор выражает благодарность за помощь в подготовке научного исследования научному руководителю И.В. Балынину, кандидату экономических наук, доценту департамента общественных финансов финансового факультета Финансового университета при Правительстве Российской Федерации.

В. А. Ледовская
Финансовый университет при Правительстве РФ, г. Москва

Проблемы информационной безопасности цифровой экономики в Российской Федерации и возможные пути их решения

Аннотация. XX век характеризуется быстрым развитием компьютерных технологий и внедрением их в экономику. Россия стремится занять лидирующие позиции на мировом рынке, разрабатывая программы по обеспечению перехода к цифровой экономике. В статье рассматриваются проблемы, возникающие в информационной безопасности страны, необходимость принятия мер на государственном уровне.

Ключевые слова: цифровая экономика; информационная безопасность; киберпреступность; государство; человек.

В настоящее время мы живем в период расцвета цифровых технологий и реорганизации экономической деятельности многих ведущих стран мира. Вторая половина XX в. характеризуется началом перехода общества на путь постиндустриализма. В течение этого времени проис-

ходит развитие наукоемких производств и информационных технологий, компьютеризация и роботизация производства и становление виртуальной культуры. Все это привело к тому, что теперь у подавляющего большинства людей дома есть компьютер или ноутбук, а постоянными спутниками любой поездки человека являются смартфоны и планшеты. Самым главным изобретением в период постиндустриализма стала международная сеть «Интернет», которая позволяет людям общаться друг с другом через социальные сети вне зависимости от местоположения, совершать покупки, не выходя из дома, и предоставляет большое количество других удобных возможностей.

Очевидно, все нововведения, которые происходят в обществе, определенным образом влияют и на экономику. Появление компьютерных технологий сильно изменило способы производства, распределения, обмена и потребления благ. Организациям стало проще создавать необходимые для жизни человека продукты, так как роботизированное оборудование работает эффективнее и быстрее и не требует больших затрат. Финансовые процессы также начали протекать легко и свободно. Использование электронных счетов и банковских карт увеличило денежный оборот, а удобное предоставление онлайн услуг повысило потребительский спрос на товары. Под воздействием подобных положительных результатов многие страны мира стремятся к обеспечению перехода к цифровой экономике. В России принята специальная Программа «Цифровая экономика Российской Федерации», которая определяет направление развития российской экономики.

Однако любые прогрессивные преобразования имеют различные отрицательные последствия. Главным образом новые технологии угрожают информационной безопасности страны и отдельного человека. Люди становятся более уязвимыми, так как зависят от системы, которую при желании можно взломать. В России за последнее время по данным МВД за первое полугодие 2020 г. почти в 2 раза увеличилось количество преступлений в сфере компьютерных технологий. Причем большее количество неправомерных действий связано с банковскими операциями. Очень часто люди безответственно подходят к переводу денег и пополнению своего счета или доверяют ненадежным источникам. Бывают случаи, когда они непроизвольно разглашают реквизиты своей банковской карточки посторонним людям или случайно переводят деньги на счет неизвестного человека из-за неправильного ввода мобильного телефона, к которому привязана банковская карта. Большинство людей, а именно взрослое поколение и дети с открытым доступом в Интернет, не обладают хорошей информационной культурой и плохо разбираются в компьютерах и программном обеспечении. Они используют вирусные ис-

точники, переходят на небезопасные ссылки и становятся жертвами киберпреступлений. Многие компании также подвергаются взломам данных и хищением сведений о своих клиентах. Например, в феврале 2020 г. в Сбербанке произошла утечка информации, которую впоследствии выставили на продажу на теневом рынке. Конечно, она не может позволить злоумышленникам напрямую списывать средства людей, но, обладая личными данными, они могут воздействовать на человека по телефону.

Компьютерное мошенничество становится все более популярным, а киберпреступность угрожает становлению цифровой экономики. Люди стремятся заполучить как можно больше информации, чтобы потом манипулировать разными субъектами экономической деятельности. Злоумышленники взламывают компьютерный сервер организации, сливают информацию и получают большие деньги за реализацию такой операции. Возможно, причина такого поведения человека лежит в основе его биологической сущности, которая главным образом заключается в инстинктах, или в определенных жизненных установках преступника. Крайней сложностью киберпреступлений является разоблачение преступников. Компьютер дает возможность человеку совершать многие действия инкогнито или под ненастоящим именем. По этой причине многие хакеры не несут ответственности за совершенные преступления и продолжают свою деятельность, расширяясь в ее масштабах и нанося большой ущерб экономике страны.

В связи с такими негативными последствиями государству необходимо принимать меры по защите личных данных своих граждан и корпоративной информации компаний. Можно выделить несколько направлений обеспечения информационной безопасности в Российской Федерации:

1) формирование таких государственных структур, которые могли бы выявлять киберпреступников;

2) создание системы оповещений для предупреждения граждан РФ об актах компьютерного мошенничества;

3) внедрение в школьную программу предмета по информационной безопасности;

4) проведение специальных курсов по развитию информационной культуры для взрослых людей.

Цифровизация экономики является приоритетом инновационного развития для России. Этот процесс очень эффективен для страны, так как увеличивает ее доходность и помогает государству занять лидирующие позиции на мировой арене. Однако с большим акцентом на положительные стороны цифровой экономики не стоит забывать и о проблемах, которые необходимо решить, так как они тормозят прогрессивность преобразований в экономической деятельности Российской Федерации.

З. А. Носиров
Финансовый университет при Правительстве РФ, г. Москва

Применение технологии блокчейн и схем разделения секрета в задачах безопасного хранения ключевой информации

Аннотация. В современных информационных системах организаций хранится и обрабатывается большой объем данных, защита которых предусматривает использование ключевой информации. В роли ключевой информации выступают пароли административного доступа, пин-коды и т.д. В случае их потери доступ к информационным системам может быть утрачен. В статье предлагается метод безопасного хранения ключевой последовательности на основе системы распределенных реестров и пороговой схемы Шамира. Одним из главных преимуществ метода является защита от социальной инженерии.

Ключевые слова: хранение ключевой информации; схема Шамира; блокчейн.

Национальная безопасность РФ существенным образом зависит от обеспечения информационной безопасности (ИБ), и в дальнейшем эта зависимость будет только возрастать[1]. Зачастую вопросы обеспечения безопасного цифрового пространства приводят к сложным задачам хранения ключевой информации (КИ) для доступа к информационным системам (ИС). В большинстве случаев ответственность за хранение КИ возложена на людей, которые осуществляют администрирование ИС. Необходимо отметить, что злоумышленники все чаще используют различные техники социальной инженерии для проникновения в инфраструктуру организации. Согласно результатам анализа, проведенного компанией Positive Technologies, можно отметить, что социальная инженерия — мощный инструмент в руках злоумышленников, и даже самые осведомленные в вопросах ИБ сотрудники могут ошибиться[2]. Поэтому можно утверждать, что вопросы, связанные с обеспечением безопасного хранения КИ, являются актуальными по сей день.

Во многих исследованиях, учеными рассматриваются задачи безопасного хранения КИ, где человек (владелец КИ) изначально знает значение ключевой информации. То есть владелец секрета вводит в некую систему значение КИ и с помощью пороговых схем разделения секрета (СРС) делит на части, затем эти части секрета раздает хранителям. Сей факт значительно понижает уровень ИБ, так как владелец КИ может выступать в качестве инсайдера или же может быть подвержен воздействию со стороны социальной инженерии.

---

[1] *Стратегия* национальной безопасности Российской Федерации. М.: Проспект, 2016.

[2] *Social* engineering: how the human factor puts your company at risk // Positive Technologies. 2018. URL: https://www.ptsecurity.com/ww-en/analytics/social-engineering-2018.

Объектом исследования, являются методы безопасного хранения ключевой информации в ИС. *Предметом исследования*, являются характеристики безопасности хранения ключевой информации на основе пороговых СРС и технологии блокчейн. *Целью исследования*, является повышение эффективности хранения КИ, путем разработки методов безопасного хранения ключевой последовательности, основанных на применении пороговых СРС и блокчейн технологии.

Особенностью предлагаемого метода является то, что она должна быть интегрирована в существующую ИС. Это связано с автоматической генерацией КИ.

На основе результатов анализа, представленных в работе[1], в качестве пороговой СРС целесообразнее использовать схему Шамира, так как она является наиболее эффективной по сравнению с остальными. Далее рассмотрим возможный пример интеграции предлагаемого метода в алгоритм установки пароля для СУБД.

В большинстве случаев код аутентификации КИ хранится в некой таблице БД в виде хеша. Алгоритм проверки правильности ключевой информации весьма прост. Высчитывается хеш от предоставленной информации, затем сверяется с хешем хранящейся в одной из таблиц БД. Если хеши совпадают, то это означает, что предоставлена корректная КИ. Рассмотрим подробнее последовательность действий в предложенном решении.

Шаг 1. Инициатором процедуры разделения секрета производится настройка системы, т.е. вводятся следующие данные: минимальное количество легитимных хранителей, необходимых для восстановления секрета; число долей на которое необходимо разделить секрет; ФИО хранителей; выбор алгоритма шифрования (ГОСТ 28147-89 или AES).

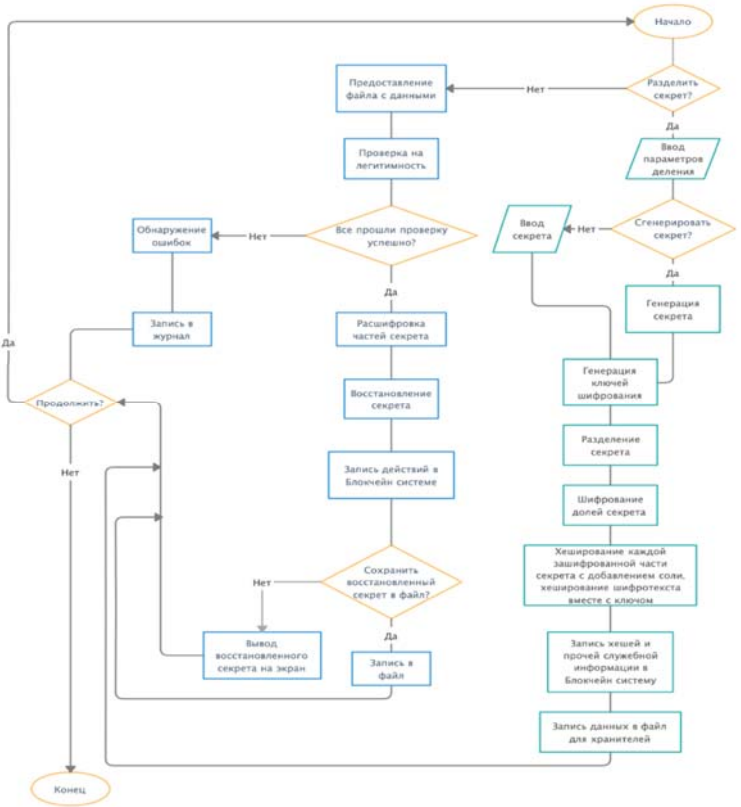
Шаг 2. Системой генерируется КИ с помощью генератора псевдослучайных последовательностей. В соответствующей системной таблице БД записывается хеш сгенерированной КИ.

Шаг 3. Для каждого хранителя генерируются симметричные ключи шифрования. Затем с помощью схемы Шамира сгенерированная КИ делится на заранее выбранное количество хранителей. Каждая часть КИ подвергается шифрованию. Поочередно в блокчейн записываются следующие данные: хеши зашифрованных частей секрета; хеши зашифрованных частей секрета и ключей с помощью которых были зашифрованы; дата и время; ФИО инициатора.

Шаг 4. Для хранителей создаются текстовые файлы с данными: ФИО; зашифрованная часть секрета; симметричный ключ шифрования,

[1] *Носиров З. А., Щербинина О. В.* Анализ криптографических схем разделения секрета для резервного хранения ключевой информации // Прикаспийский журнал: управление и высокие технологии. 2019. № 2 (46). С. 126-134.

использованный для шифрования данной части; хеш блока; хеш сгенерированной КИ. Для восстановления КИ, достаточно лишь определенному количеству хранителей предъявить файл, полученный при делении. Системой осуществляется проверка на легитимность пользователей. Данная проверка осуществляется путем проверок хеш сумм. Сначала проверяется есть ли в блокчейне хеш блока указанный в файле, рассчитывается хеш зашифрованной части КИ и сверяется с хешем хранящимся в блокчейн сети. Затем проверяются значения хешей зашифрованных частей и ключей с помощью которых были зашифрованы. При успешном восстановлении, КИ записывается в файл и создается соответствующая запись в блокчейне. На рисунке представлена блок-схема программной реализации.



Блок-схема программной реализации

Предлагаемое решение может обеспечить защиту от следующих видов атак: нарушитель специально предоставил измененный файл с целью приостановления процесса восстановления КИ; нарушителю удалось сойтись за «своего», и он спровоцировал начало процедуры восстановления секрета с целью узнать доли секрета других хранителей; нарушитель имитирует (k+1)-го участника пороговой схемы (k — минимальное количество хранителей не-обходимое для восстановления секрета); нарушитель использует методы социальной инженерии в отношении хранителей. Осуществление вышеперечисленных атак невозможна, так как нарушитель не сможет пройти проверку на легитимность и быстро может быть вычислен группой хранителей. Использование пороговой СРС усложняет применение техник социальной инженерии, так как для восстановления всего секрета нарушителю необходимо получить доступ, как минимум к k частям секрета.

В рамках данной работы предложен метод безопасного хранения КИ на основе схемы Шамира и блокчейн-технологии. Описанный метод усложняет реализацию атак с применением различных техник социальной инженерии. Основной отличительной особенностью предложенного метода является то, что значение КИ изначально неизвестно никому, даже инициатору протокола разделения. Данное свойство позволяет значительно повысить уровень ИБ протокола хранения ключевой информации.

М. В. Паршина
Волгоградский государственный социально-педагогический университет,
г. Волгоград

Школьное экономическое образование как одно из условий информационной безопасности цифровой экономики России

Аннотация. Рассматриваются основные аспекты цифровой экономики России. Обоснована необходимость школьного экономического образования для обеспечения информационной безопасности цифровой экономики страны. Выявлены причины, влияющие на эффективность обучения экономике в школе.

Ключевые слова: цифровая экономика; информационная безопасность; обучение; экономическое образование; информационная грамотность.

Ориентация российской экономики на интенсивный сценарий развития, а также постепенный переход к цифровой экономике требуют наличия экономически грамотного и активного населения.

Вместе с ростом благосостояния российских граждан должно формироваться и их активное сберегательное поведение, основанное на ис-

пользовании накопительных и страховых инструментов. Для формирования такого поведения требуется наличие достаточно высокого уровня экономической и информационной грамотности, который должен служить основой для взаимодействия граждан с различными финансовыми институтами в условиях цифровой экономики, осознанного использования ими продуктов банковского и страхового сектора, формирования стратегии пенсионного обеспечения.

С ростом населения планеты и мобилизации ресурсов, электронная экономика не ограничивается бизнесом, электронной торговлей и сервисами, а затрагивает каждый аспект жизни, в том числе и образование. Учитывая массовый перенос документов и коммуникаций на цифровые носители, перед обществом стоит сложная задача — целенаправленно формировать у подростков экономические знания и умения применять их в цифровой среде. Формирование данных умений личности необходимо рассматривать как педагогическую технологию, включающую определенную совокупность методов и средств, обеспечивающих достижение заданного результата [2].

В сложившихся экономических условиях, учащиеся должны быть готовы к дальнейшей активной экономической жизни. С формированием цифровой экономики и единого информационного пространства многие жизненные ситуации, связанные с экономическими вопросами, можно решить, не выходя из дома. Для этого необходим только компьютер и выход в сеть Интернет. Ведь цифровая экономика представляет собой деятельность, непосредственно связанную с развитием цифровых компьютерных технологий, в которую входят сервисы по предоставлению онлайн-услуг, электронные платежи, интернет-торговля и многое другое. Обычно главными элементами цифровой экономики являются электронная коммерция, интернет-банкинг, электронные платежи, а также интернет-реклама и онлайн-игры.

Там не менее, внедрение в жизнь «цифры» и электронной коммерции несет для человечества и ряд минусов, среди которых:

— риск киберугроз, связанный с проблемой защиты персональных данных;

— использование данных о миллионах людей для управления их поведением;

— разрыв в цифровом образовании, в условиях доступа к цифровым услугам и продуктам, и, как следствие, разрыв в уровне благосостояния людей, находящихся в одной стране или в разных странах [2].

Таким образом, перед образовательным учреждением стоит большая задача — научить ребят грамотно работать с информационными источниками. В условиях школы это можно сделать с помощью методов обучения на основе информационных ресурсов.

Учащиеся должны уметь получать необходимую информацию из сети Интернет. Так, например, одним из направлений современного экономического образования может стать ознакомление ребят с сайтами Федеральной налоговой службы, Пенсионного фонда РФ, порталом Государственных услуг РФ, сайтами банков и других организаций, а также обучение работе с ними.

Обучение экономике на основе информационных ресурсов предполагает нахождение необходимой в процессе обучения информации и отработку навыков, которые имеют практическое значение и пригодятся учащемуся в будущем.

Таким образом, экономическое образование, основанное на современных цифровых технологиях необходимо всем категориям граждан. Оно дает представление о ценности денег, закладывает фундамент для дальнейшего развития навыков планирования бюджета и сбережений. Грамотный потребитель финансовых услуг лучше защищен от мошеннических действий в области финансов.

Основными причинами низкой результативности, неэффективности деятельности образовательных учреждений в решении данного вопроса является неподготовленность кадров, а также отсутствие мотивационного компонента со стороны педагогических коллективов в значимости знаний и умений работы с электронными ресурсами социально-экономической направленности [1].

Сегодня возникает необходимость специальной подготовки кадров, способных на профессиональной основе проводить занятия по экономике в условиях информационной среды. Решение данной проблемы возможно при использовании профессионального потенциала педагогов учреждений дополнительного образования, владеющих специальными знаниями по финансам в цифровой экономике.

Библиографический список

1. *Камнева В. В., Коняева Е. А.* Цифровая экономика в образовании // Скиф. Вопросы студенческой науки. 2018. № 3 (19). С. 101–105.

2. *Формирование* основ финансовой грамотности у детей и подростков: сб. метод. разработок. Ставрополь: СКИРО ПК и ПРО, 2016.

Е. Г. Петрищева, В. А. Григоров
Курский государственный университет, г. Курск

Рост цифрового мошенничества в период пандемии

Аннотация. Выявлены основные методы выманивания денег у физических и юридических лиц кибермошенниками, проанализировано влияние коронавируса на рост телефонного и интернет-мошенничества.

Ключевые слова: пандемия; кибератаки; мошенничество; Российская Федерация; фишинг.

В период коронавирусной инфекции в Российской Федерации был отмечен колоссальный рост киберпреступности, адаптированный под «новую реальность». Апрель и май стали рекордными по числу успешных кибератак, так как граждане в связи с ограничительными мерами и режимом самоизоляции массово начали в апреле переходить на дистанционную работу, многие потеряли заработный доход и с помощью интернета пытались найти способ заработка онлайн и др.

Рост связан именно со вспышкой COVID-19, вызвавшей создавшей почву для фишинговых атак и социальной инженерии. С 2016 по 2020 г. число мошеннических действий выросло на 29,5 %, согласно данным Генпрокуратуры России[1]. Риск столкнуться с фишингом в несколько раз выше, чем с хакерской атакой. Данные Сбербанка показывают, что уровень развития фишинга поднялся на 3 % с 2017 по 2020 г.[2] Преступники по-прежнему активно используют методы социальной инженерии.

После введения режима повышенной готовности мошенники быстро «переквалифицировались» и стали предлагать гражданам товары и услуги, «актуальные» в условиях распространения COVID-19.

Рассмотрим способы получения мошенниками финансового дохода через современные технологии.

1. Создание онлайн-магазинов. С началом пандемии вырос спрос у граждан на приобретение товаров и услуг через сеть Интернет, особенно популярностью пользовались такие товары, как маски, перчатки, лекарства, санитайзеры. Один банк фиксировал в среднем 400−600 таких мошеннических попыток в месяц, «средний чек» одного перевода – более 7 тыс. руб. Злоумышленники ставили одно из условий для получения товара — предоплата без фактической доставки и в результате заказанный продукт лицо не получало.

[1] *Основные* статистические данные о деятельности органов прокуратуры. URL: genproc.gov.ru.

[2] *Аналитика* и исследования — СберБанк. URL: sberbank.ru.

2. Создание вирусных сайтов. Число DDoS-атак за время карантина выросло на 15 %, атак на сотрудников компаний, в первую очередь через фишинг, — на 10 %; сами вредоносные рассылки стали более таргетированными и потому чаще вызывали доверие у получателей[1]. Часто как физические, так и юридические лица переходили по вирусным ссылкам, которые распространяли вредоносное программное обеспечение для кражи личных данных или данных банковской карты. Кража личных данных также возможна через массовые рассылки, когда пользователя просят перейти по ссылке. Как сообщают данные «Рамблер», около 70% сайтов российского сегмента были созданы преступниками во время пандемии[2].

Создание «идентичных» государственных сайтов. В условиях пандемии происходило резкое увеличение числа цифровых двойников, дублирующих аккаунтов, страниц в Интернете, имитирующих государственные сайты электронных услуг и аккаунты органов власти. На такую уловку может попасться любой гражданин, который, например, захотел узнать информацию или получить услугу на официальном сайте попадает на фейковые порталы реальных организаций, так Всемирной организации здравоохранения или Минздрава России, благотворительных организаций, осуществляющих помощь и поддержку граждан.

3. Сайты, где размещаются способы легкого и быстрого заработка через сеть Интернет. Согласно данным Федеральной службы государственной статистики[3], с февраля по июнь 2020 г. количество безработных граждан выросло на 2,8 млн чел., рост составил 1,6%. Зарплатный фонд в апреле достиг минимума — 23%, спад по сравнению с прошлым месяцем составил 35%. Согласно данным Росстата, средний доход наемных работников средних и крупных организаций в реальном выражении снизился на 4,3% в апреле 2020 г. За период быстрого роста безработицы произошел рост числа сайтов, предлагающих якобы простой и быстрый заработок, например обещание заработка на майнинге криптовалюты.

4. Телефонные звонки. Мошенникам чаще всего удавалось получать доступ к конфиденциальным данным граждан помощью телефонных звонков от «службы безопасности» банка. Мошенники обзванивали граждан в качестве сотрудников банка и предлагали такие услуги, как: оказание финансовой поддержки, оформление кредитных каникул, предоставление рассрочки и др. Для данных операций звонящие просили сообщить им данные банковских карт (реквизиты, срок действия и CVV-

[1] *Число* дел о мошенничестве рекордно выросло на фоне пандемии. URL: https://www.rbc.ru/society/31/08/2020.

[2] *Пандемию* COVID-19 используют для массового обмана. URL: https://news.rambler.ru/other/44072950.

[3] *Федеральная* служба государственной статистики. URL: https://rosstat.gov.ru/.

код) и персональную информацию. Число людей, которых доверяли таким службам, существенно выросло за весну, поэтому для противодействия телефонным мошенникам была создана межведомственная рабочая группа, в которую представители Минкомсвязи, МВД, ФСБ, Роскомнадзора, ЦБ, а также операторов связи и банков. Также фиксировалось телефонное информирование граждан о государственных услугах, о начислениях социальных льгот и пособий, связанных с распространением инфекции, осуществляемое таким образом, чтобы узнать личные данные граждан либо «помочь» с получением данных услуг за деньги.

5. Рассылка СМС. Мошенникам удавалось обманывать не только уязвимые группы населения, но и молодежь, все население в целом, так как во время социальной и экономической нестабильности и неопределенности в сети Интернет тиражировались как официальные данные, так и фейковая информация, произошел информационный бум, который явился следствием недоверия и непонимания людьми какой информации верить, а какой нет. Поэтому многие граждане воспринимали серьезно информацию, получавшую через фейковые СМС-сообщения о том, что им выписан штраф за нарушение карантина или самоизоляции. Часто в таких случаях просили оплатить его немедленно — по номеру телефона или карты, угрожая возбуждением уголовного дела или мотивируя тем, что завтра сумма штрафа удвоится.

6. Оказание услуг. Злоумышленники обещали предоставить вам определенные услуги, например, пройти обследование без очереди на коронавирус в поликлинике, но перед этим, необходимо зарегистрироваться на неизвестном сайте или установить программу на компьютер или телефон, а также предложения по урегулированию взысканий, отсрочке по выплате кредитов или помощи в проведении упрощенной процедуры банкротства за комиссию. Получив предоплату, преступники скрывались.

Таким образом, во время пандемии тема киберугроз, мошенничества, стала особо актуальна, так как миллионы людей перешли на дистанционный формат общения и работы. За время действия ограничений, связанных с эпидемией коронавируса, в России резко выросло число зарегистрированных случаев мошенничества. Онлайн-преступники не упустили шанс использовать такой момент в целях собственного обогащения путем обмана. Они гражданам предлагали дефицитные товары, государственные услуги, выгодные условия для заработка или прохождения онлайн-курсов для повышения квалификации, тренинги; создавали имитирующие порталы государственных органов, вирусные сайты, онлайн-магазины и т.д., т.е. применяли огромный спектр методик выманивания финансовых средств, сведений о своих учетных записях в Интернете, пароли, пин-коды и номера банковских карт, другие персональные и конфиденциальные данные. Согласно данным Сбербанка, за

3 года рост фишинга составил 3%. Около 70% сайтов российского сегмента были созданы преступниками во время пандемии. Органам власти следует вовремя противодействовать новым вызовам кибератак мошенников, которые используют ситуацию шока и тревоги граждан в период пандемии. Роскомнадзор, МВД, иные ведомства должны оперативно обеспечивать защиту населению. Генпрокуратура России своевременно возбуждала уголовные дела, чтобы пресекать попытки манипулирования общественным мнением, распространение паники и призывы в Интернете не подчиняться мерам властей, призванным снизить заражение во время эпидемии. Эти действия осуществлялись в координации с Роскомнадзором.

М. Н. Рябцева
Филиал ТФОМС Свердловской области, г. Екатеринбург

Информационная безопасность цифровой экономики Российской Федерации

Аннотация. Рассмотрены основные задачи федерального проекта «Информационная безопасность». Выявлена их социально-экономическая роль, описаны результаты, полученные с начала реализации проекта.

Ключевые слова: информационная безопасность; цифровая экономика; экономическое развитие.

Цифровая экономика — экономическая деятельность, основанная на цифровых технологиях, связанная с электронным бизнесом и электронной коммерцией, и производимых и сбываемых ими цифровыми товарами и услугами. В связи с этим, были разработаны национальные программы и федеральные проекты, направленные на обучение граждан безопасному использованию сети Интернет, рациональной работе с персональными данными и их защите от злоумышленников и иных возможных угроз. Информационная безопасность является одним из важнейших направлений нацпроекта «Цифровая экономика». Это, прежде всего, связано с появлением новых требований регуляторов и увеличением числа киберугроз. В реализации данной программы выделяют три ключевых направления: импортозамещение, защита критически важной инфраструктуры информационных систем и подготовка кадров.

Одной из основных реализуемых программ в нашей стране, связанной с обеспечением защиты информации, является национальная программа «Цифровая экономика Российской Федерации». Она включает в себя шесть федеральных проектов, одним из которых является проект

«Информационная безопасность». Задачами данного направления является достижение к 2024 г. следующих показателей:

1) 50 % — доля граждан, повысивших грамотность в сфере информационной безопасности, медиапотребления и использования интернет-сервисов;

2) 97 % — доля населения, использовавшего средства защиты информации от общей численности населения, использовавшего сеть "Интернет" в течение последних 12 месяцев;

3) 75 % — доля субъектов, использующих стандарты безопасного информационного взаимодействия государственных и общественных институтов.

С ростом населения планеты и мобилизации ресурсов, электронная экономика не ограничивается бизнесом электронной торговли и сервисов, а затрагивает каждый аспект жизни: здравоохранение, образование, интернет-банкинг и так далее, которые не смогут существовать без информационной безопасности, так как слишком серьезными могут быть последствия потенциальных угроз нарушения их деятельности в результате хакерских и инсайдерских атак.

На сегодняшний день созданы и протестированы информационные системы мониторинга маршрутов трафика в Интернете, мониторинга и управления сетью связи общего пользования и фильтрации интернет-трафика при использовании информационных ресурсов детьми.

Цель национальной программы «Цифровая экономика Российской Федерации» — сделать интернет доступным для всех, покрыть крупнейшие города связью 5G, защитить информацию граждан, бизнеса и государства, повысить эффективность основных отраслей экономики, подготовить кадры для работы в цифровой среде, увеличить долю затрат на развитие цифровой экономики в ВВП страны в 3 раза.

Решение данных вопросов обеспечивает информационная безопасность. Для реализации целей развития цифровой экономики в сфере информационной безопасности являются рост масштабов компьютерной преступности, в том числе международной, отставание Российской Федерации в разработке и использовании отечественного программного обеспечения, недостаточный уровень кадрового обеспечения в области информационной безопасности. В результате реализации направления «Информационная безопасность» будут обеспечены устойчивость и безопасность информационной инфраструктуры, конкурентоспособность отечественных разработок и технологий информационной безопасности и выстроена эффективная система защиты прав и законных интересов личности, бизнеса и государства от угроз информационной безопасности. Конечная цель Программы — обеспечить цифровую независимость

страны и вывести Российскую Федерацию на уровень мировых лидеров в области информационной безопасности.

Вот как направление информационной безопасности обозначено в программе цифровой экономики: «Целью направления, касающегося информационной без-опасности, является достижение состояния защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод чело-века и гражданина, достойные качество и уровень жизни граждан, суверенитет и устойчивое социально-экономическое развитие Российской Федерации в условиях цифровой экономики, что предполагает: обеспечение единства, устойчивости и безопасности информационно-телекоммуникационной инфраструктуры Российской Федерации на всех уровнях информационного пространства; обеспечение организационной и правовой защиты личности, бизнеса и государственных интересов при взаимодействии в условиях цифровой экономики; создание условий для лидирующих позиций России в области экспорта услуг и технологий информационной безопасности, а также учет национальных интересов в международных документах по вопросам информационной безопасности»[1]. По словам заместителя председателя правления ПАО «Сбербанк» С. К. Кузнецова: «Эксперты высказались за создание координационного центра по кибербезопасности, обеспечивающего взаимодействие различных ведомств российского государства, которые профессионально выполняют работу в рамках своих компетенций.

Так, ФСБ с помощью Государственной системы обнаружения предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА) защищает критическую ин-формационную инфраструктуру, федеральная служба по техническому и экспотрному контролю (ФСТЭК) — промышленные системы критически важных объектов, Центральный банк РФ через Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (FinCERT) — банковскую систему, однако координации действий между ведомствами нет, а она необходима для централизованного решения проблем информационной безопасности»[2]. В рамках направления информационной безопасности программы «Цифровой экономики» как раз и предполагается выработать общие подходы и научиться координировать действия различных государственных структур.

---

[1] *Паспорт* национальной программы «Цифровая экономика Российской Федерации». URL: http:// static.government.ru/media/files/urKHm0gTPPnzJlaKw3M5cNLo6gczMkPF.pdf. (стр.85).

[2] *CONNECT*. Мир информационных технологий. URL: https://www.connect-wit.ru/tsifrovaya-informatsionnaya-bezopasnost.html.

В 2021 г. будет разработан и принят комплекс стандартов информационной безопасности, обеспечивающий минимизацию рисков и угроз безопасного функционирования сетей связи общего пользования; разработаны меры регулирования вопросов целостного, устойчивого и безопасного функционирования российского сегмента сети «Интернет»; обеспечен контроль обработки и доступа к персональным, большим пользовательским данным, в том числе в социальных сетях и прочих средствах социальной коммуникации, а также возможность отзыва или уменьшения объема ранее данного согласия на обработку персональных данных; созданы условия для развития образования в области информационной безопасности в интересах реализации за-дач цифровой экономики. В экономической сфере к 2024 г. Правительством РФ будут прорабатываться следующие задачи: создание системы правового регулирования цифровой экономики, основанного на гибком подходе к каждой сфере, а также внедрение гражданского оборота на базе цифровых технологий; со-здание глобальной конкурентоспособной инфраструктуры передачи, обработки и хранения данных преимущественно на основе отечественных разработок; обеспечение информационной безопасности на основе отечественных разработок при передаче, обработке и хранении данных, гарантирующей защиту интересов личности, бизнеса и государства; создание сквозных цифровых технологий преимущественно на основе отечественных разработок; внедрение цифровых технологий и платформенных решений в сферах государственного управления и оказания государственных услуг, в том числе в интересах населения и субъектов малого и среднего предпринимательства, включая индивидуальных предпринимателей; создание единой платформы по принципу «одного окна» с целью обеспечения граждан единой точкой доступа для взаимодействия с государством[1].

На сегодняшний день цифровая экономика не может существовать без информационной безопасности. Поэтому информационную безопасность необходимо укреплять на законодательном уровне. На сегодняшний день принимаются правила защиты цифровых и финансовых отраслей от киберугроз и разрабатываются отечественные программные обеспечения.

[1] *Основные* направления деятельности Правительства РФ на период до 2024 г.

К. М. Саматов, А. А. Заведенская
Уральский государственный экономический университет, г. Екатеринбург

Анализ исходного кода как способ обеспечения безопасности информационной инфраструктуры цифровой экономики

Аннотация. Авторы рассматривают основные виды анализа исходного кода и его применение для обеспечения информационной безопасности субъектов цифровой экономики.

Ключевые слова: анализ исходного кода; безопасность информационной инфраструктуры; цифровая экономика.

Подход к организации деловых процессов в современных компаниях построен на широком использовании программных продуктов на базе веб-технологий: официальные сайты, форумы, корпоративные порталы, интернет-магазины и аукционы, порталы услуг, электронные торговые площадки — все это неотъемлемые элементы информационной инфраструктуры цифровой экономики. Нарушение их штатного функционирования, вследствие реализации угроз информационной безопасности, может привести к существенным финансовым и репутационным потерям. Для того, чтобы этого избежать необходимо применение методов безопасной разработки и анализа безопасности исходного кода в процессе проектирования, создания и эксплуатации программного обеспечения.

Анализ безопасности исходного кода — это анализ программного обеспечения на предмет выявления уязвимостей информационной безопасности, допущенных при его разработке.

Существует три группы методов анализа исходного кода:

1) динамические методы − методы анализа безопасности программного обеспечения, требующие выполнения программ на реальном или виртуальном процессоре, с доступом к исходному коду и среде его функционирования;

2) статические методы — методы анализа безопасности программного обеспечения с доступом к исходному коду (или производным) приложения серверных и клиентских частей, но не требующие выполнения программ;

3) гибридные методы — методы, совмещающие два предыдущих похода.

Статические методы анализа исходного кода могут быть использованы при создании и эксплуатации программного обеспечения, а динамические на этапе ввода в эксплуатацию и в процессе эксплуатации.

На практике анализ исходного кода широко применяется совместно с другим методами анализа защищенности и, нередко, является одной из стадий проекта по анализу защищенности информационных систем. Так, большинство проектов по анализу защищенности, с которыми приходилось сталкиваться авторам, включали в себя следующие стадии.

1. Анализ защищенности методами «черного» и «серого ящика», т.е. динамический анализ безопасности программного обеспечения без доступа к исходному коду:

— метод «черного ящика» направлен на поиск уязвимостей, использование которых позволяет злоумышленнику не имеющему никаких привилегий реализовать следующие виды угроз: получение несанкционированного доступа к информации, полного или частичного контроля над приложением и его использование для организации атак на рабочие места пользователей информационной системы;

— метод «серого ящика» аналогичен предыдущему, с тем лишь исключением, что под злоумышленником подразумевается пользователь, обладающий определенным набором привилегий в информационной системе.

2. Анализ защищенности методом «белого ящика» — динамический и статический анализ безопасности исходного кода.

3. Разработка рекомендаций и итогового отчета.

4. Проверка корректности устранения выявленных уязвимостей.

В качестве конкретного примера подобного проекта, встречавшегося в практике авторов, можно привести анализ защищенности Интернет-магазина, самого распространенного хозяйствующего субъекта цифровой экономики (см. таблицу).

Пример проекта по анализу защищенности интернет-магазина

Стадия/этап	Состав работ (что делается?)
Анализ защищенности интернет-магазина методами «черного» и «серого» ящиков	
Сбор и анализ информации	Сбор общедоступной информации о внешних ресурсах, данных об инфраструктуре (сетевых сервисах, операционных системах и прикладном программном обеспечении), сканирование сетевых портов, анализ сетевого взаимодействия, определение типов и версий сетевых сервисов и приложений по реакции на внешнее воздействие
Анализ защищенности	Выявление уязвимостей Интернет-магазина и его инфраструктурных компонентов с использованием сканеров защищенности и специализированного программного обеспечения, а также ручная проверка доступного функционала

Продолжение таблицы

Стадия/этап	Состав работ (что делается?)
Подтверждение уязвимостей	Моделирование атак на уровне сетевых сервисов и приложений, использование обнаруженных уязвимостей с целью оценки возможности получения несанкционированного доступа к защищаемой информации, попытки получения привилегированных прав и их эксплуатация
Анализ безопасности исходного кода интернет-магазина	
Сбор информации, анализ архитектуры приложений	На данном этапе изучается программное окружение и вся информационная система целиком. В частности, выполняются следующие действия: определяются возможные угрозы; проверяются настройки отдельных элементов системы на соответствие требованиям безопасности; изучается архитектура, выявляются критичные элементы; осуществляется мониторинг уязвимостей в сторонних компонентах
Сбор информации, анализ архитектуры приложений	Основным результатом этого этапа является список критичных элементов системы. К критичным элементам относятся: механизмы валидации и нормализации вводимых данных; механизмы аутентификации и авторизации; механизмы криптозащиты; механизмы защиты хранимых данных на предмет предотвращения несанкционированного доступа к аутентификационной и иной критичной информации; протоколы обмена данными между клиентским и серверным программным обеспечением
Поиск уязвимостей с использованием специализированных автоматических анализаторов	На данном этапе выполняется анализ исходного кода с помощью специализированного программного обеспечения (анализаторы исходного кода), позволяющего находить подозрения на уязвимости, которое осуществляет статический и динамический анализ исходного кода. Для разных языков и платформ могут использоваться различные анализаторы, которые специально подбираются для используемых технологий
Ручная проверка найденных подозрений на уязвимости и критичных элементов, выявление недокументированных возможностей в программном обеспечении	На данном этапе проводится изучение критичных элементов системы и ранее найденных подозрений на уязвимости. В частности, выполняются следующие действия: проверка наличия и работоспособности механизмов безопасности; поиск недостатков и уязвимостей исходного кода, связанных с вызовом опасных функций языка программирования и (или) платформы; проверка реализации механизмов защиты на соответствие рекомендациям безопасности языка программирования или платформы; поиск синтаксических ошибок; проверка наличия и работоспособности механизмов обработки входных данных; поиск логических ошибок и логических «бомб»; проверка реализации механизмов криптозащиты; мониторинг зависимостей от общеизвестных уязвимостей

Окончание таблицы

Стадия/этап	Состав работ (что делается?)
Разработка рекомендаций и подготовка отчета	
Разработка рекомендаций по устранению выявленных уязвимостей	Перечень актуальных уязвимостей строится на основе рекомендаций производителей по безопасной конфигурации программного обеспечения, материалов свободных исследовательских групп по поиску уязвимостей, каталогов уязвимостей, в частности: Computer Emergency Readiness Team (CERT); Common Vulnerabilities and Exposures (CVE); Web Application Security Consortium (WASC); Open Source Vulnerabilities Database (OSVDB). Для каждой уязвимости описываются возможные последствия ее эксплуатации. Вырабатываются предложения по устранению уязвимостей, выявленных в ходе анализа защищенности, или снижения ущерба от их реализации
Подготовка отчета	Как правило отчет содержит следующую информацию: цель анализа защищенности; состав и методика мероприятий по анализу защищенности; перечень выявленных уязвимостей; результаты эксплуатации выявленных уязвимостей; рекомендации по устранению выявленных уязвимостей и повышению уровня защищенности
Проверка корректности устранения уязвимостей	Проводится проверка наличия выявленных уязвимостей и оценка эффективности принятых мер по их нейтрализации. Подготавливается отчет о проверке корректности устранения выявленных уязвимостей

Подведем итоги: для надежной и корректной работы механизмов обеспечения безопасности в программном обеспечении необходимо регулярно проводить анализ исходного кода. При этом, для большего эффекта в части выявления уязвимостей, необходимо использовать гибридные методы анализа безопасности исходного кода: сочетание статических и динамических методов.

Р. А. Святодухов, С. И. Авсянко
Уральский государственный экономический университет, г. Екатеринбург

Кибератаки и меры по защите от них

Аннотация. Рассмотрены актуальные данные о кибератаках за 2020 г. Описаны наиболее распространенные способы внедрения вредоносного ПО и меры предосторожности.

Ключевые слова: кибератаки; вредоносные файлы; обеспечение защиты.

Последние пять лет количество пользователей сетевыми ресурсами резко выросло — это не могло остаться без внимания мошенников. Одна из главных позиций в мошенничестве — это кибератаки. Кибератака — это атака, инициированная компьютером против веб-сайта, компьютерной системы или отдельного компьютера (совместно именуемого компьютером), которая ставит под угрозу конфиденциальность, целостность или доступность компьютера или хранящейся на нем информации.

Классифицировать атаки можно, сгруппировав их по категориям:

— кража паролей — совокупность методов, целью которых является получение пароля к системе;

— социальная инженерия — использование слабостей человеческого фактора, манипуляции;

— ошибки и так называемые задние двери — использование ошибок в программном обеспечении;

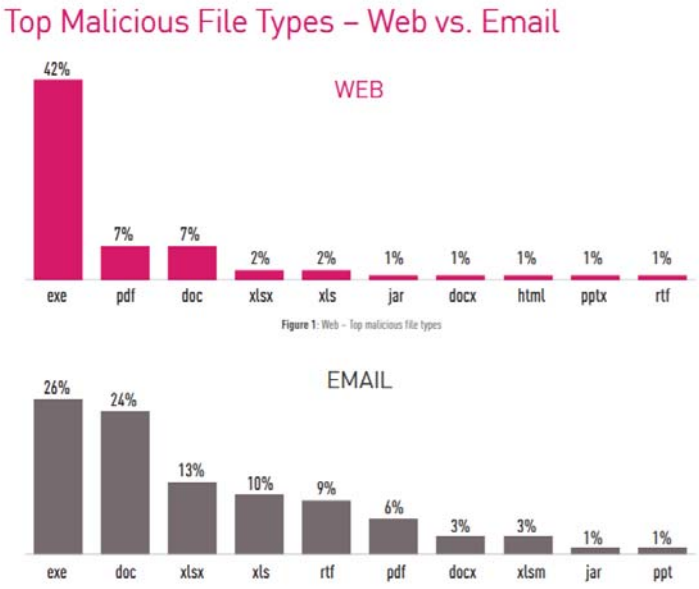
— ошибки в авторизации — использование и нарушение системы авторизации;

— ошибки в протоколах — использование ошибок в протоколах связи — коллекции правил, которые используются программами для общения между собой;

— утечка информации — неправомерное получение доступа к информации, которая необходима для функционирования Сети.

Нарушители размещают вредоносные программы во Всемирной паутине. Маскируют их под полезные, бесплатные программные обеспечения. Также есть скрипты, которые запускаются автоматически, если пользователь открыл веб-сайт. Скрипты могут выполнять различные действия на компьютере пользователя. Похищать личные данные, устанавливать вредоносное программное обеспечение.

Согласно актуальным данным по основным трендах кибератак, предоставленным в отчете Check Point Research за 2020 г., распределение вредоносных файлов различного типа выглядит следующим образом (см. рисунок).



Актуальное распределение вредоносных файлов различных типов
в зависимости от каналов их распространения
(веб-сайты, электронная почта)

По диаграмме видно, что неотъемлемым компонентом многих кибератак служат неисполняемые файлы — офисные документы, доступные для загрузки по веб-ссылкам или электронным письмам. Атаки этого типа пользуются популярностью. Объясню почему. Возьмем, например файлы формата «.exe», в операционных системах Microsoft Windows, отфильтровываются большинством почтовых сервисов, потому что это потенциальная опасность; неисполняемые файлы формата .pdf, .doc и т.п. пропускаются и к тому же большинство пользователей не воспринимают в качестве угрозы. Файлы представлены в формате, который может быть интерпретирован только программой, специально разработанной для этой цели, часто не могут быть исполнены непосредственно. Но неисполняемые файлы не менее опасны для корпоративных информационных систем, поскольку программы, с помощью которых они открываются, могут содержать «дыры», уязвимости, или иметь функциональность по запуску макросов, посредством которых нарушителю удается навредить компьютеру.

Для предотвращения таких атак можно использовать защитные инструменты такие как: брандмауэры для веб-приложений, средства обнаружения и предотвращения вторжений и др.

Не менее опасным являться HTML — стандартный язык разметки, используемый для создания веб-страниц. Этот формат предоставляет широкие возможности для скрытия троянских программ и компьютерных червей.

Меры предосторожности. Для блокирования атак с использованием веб-страниц дополнительно к общим мерам рекомендуется: Включить просмотр HTML-писем в текстовом формате (например, для почтового клиента Microsoft Outlook управление этой функцией производится в разделе «Сервис» → «Параметры» → «Свойства» → «Электронная почта» → «Параметры электронной почты» → «Обработка сообщений»). С осторожностью относиться к письмам, предполагающим незамедлительную реакцию и переход по ссылкам.

При получении веб-ссылки в электронном письме можно навести на нее курсор мыши, чтобы во всплывающей подсказке отобразился URL-адрес: если ссылка и адрес не совпадают, стоит отнестись к сообщению с осторожностью. Использовать средства проверки URL. Это могут быть отдельные сервисы или специальные плагины для браузеров, а также комплексы антивирусной защиты.

Расширение .exe имеет исполняемые файлы, которые становятся активными при открытии, а это значит, что они могут нанести очень большой ущерб. Если такие файлы приходят на электронную почту, их никогда не следует открывать.

Документы офисных приложений с расширением: .doc, .docx, .xls, .xlsx, .xlsb и т.д. При открытии таких файлов первым делом пользователь не заметит ничего подозрительного, но при этом злоумышленник может использовать макросы. Что такое макрос? Макрос — это пользовательский код, который обычно создается и запускается пользователем для автоматизации полезных операций, таких как построение графиков, форматирование текста, вычисления и т.д. Макросы могут использоваться для выполнения внешних операций, таких как запуск файлов, запись в реестр и т.д. Что бы защитить себя на будущее от различных угроз нужно понимать тенденцию кибератак, для этого нужно изучить то, что было.

В 2007 г. троянская программа начала распространяться в социальных сетях. Первыми пострадали пользователи Facebook, получившие письма с фотографиями. При попытке открыть фото пользователь попадал на страницы сайтов, пораженных вирусом ZeuS, вредоносная программа сразу же проникала в систему компьютера, находила личные данные владельца и оперативно снимала средства со счетов человека в европейских банках.

Gauss — банковский троян, крадущий финансовую информацию с пораженных ПК — был создан американскими и израильскими хакерами, работавшими в тандеме. В 2012 г., когда Gauss ударил по банкам Ливии, Израиля и Палестины, его причисляли к кибероружию.

В 2020 г. злоумышленники быстро подхватили тему всеобщего беспокойства по поводу коронавирусной инфекции и стали использовать ее для фишинговых писем. Фишинг — способ кражи конфиденциальной информации (паролей, данных кредитных карт, информации из соцсетей) через массовую рассылку электронных писем (спам), а также именных сообщений от имени финансовых и госучреждений, соцсетей или через фальшивые сайты. По нашим подсчетам, в I и II квартале около 18% атак, в которых киберпреступники задействовали методы социальной инженерии, были связаны с коронавирусом.

Из выше сказанного, можно понять, что будет продолжаться тенденция фишинга путем социально инженерии, так как до сих пор идет эпидемия и люди сидят дома и работают удаленно.

Основной угрозой безопасности является человеческий фактор. Поэтому следует соблюдать некоторые требования безопасности:

1) подключайтесь к интернету через защищенные сети; избегайте открытых сетей;

2) избегайте обмена конфиденциальной корпоративной информацией (например, по электронной почте) через небезопасные соединения;

3) будьте осторожны с любыми электронными письмами, в которых упоминается о коронавирусе, поскольку это могут быть попытки фишинга или мошенничество;

4) данные, находящиеся на локальных носителях, должны быть зашифрованы;

5) не публикуйте URL виртуальной встречи в социальных сетях или других общественных каналах.

А. А. Шумилов, И. В. Смольников
Уральский государственный экономический университет, г. Екатеринбург

Технология блокчейн в информационном обществе: преимущества и недостатки

Аннотация. Технология блокчейн появилась благодаря успешному развитию криптовалюты биткоин. С помощью этой технологии можно создавать общественные базы данных: земельные реестры, голосование через Интернет. Помимо преимуществ блокчейн обладает рядом недостатков с экономической точки зрения, но многие эксперты уверены в большом будущем этой технологии. Авторами рассматриваются основные преимущества и недостатки технологии блокчейн.

Ключевые слова: блокчейн; биткоин; транзакция; криптовалюта; информационная экономика.

В информационной экономике наступил новый этап развития, формирования криптовалюты, биткоин, создание новой системы учета информации, блокчейн. По определению Д. и А. Тэпскоттов, авторов книги «Революция блокчейна», «…блокчейн — это вечный цифровой распределенный журнал экономических трансакций, который может быть запрограммирован для записи не только финансовых операций, но и практически всего, что имеет ценность» [4]. Чтобы было проще понять, о чем идет речь, нужно представить «цепочку блоков», представляющую собой распределенную базу данных, у которой устройство хранения базы данных не подключены к общему серверу. Если произошли изменения в одном блоке, то на других также обновятся данные. Если блок с новыми данными сформирован, то он проверяется другими участниками сети (компьютерами), если все согласны, то изменения будут у всех.

Чем же технология блокчейн так привлекает государственные и бизнес-структуры?

Технология блокчейн, созданная изначально исключительно для криптовалюты биткоин, сегодня на слуху даже у людей, ни разу не использовавших электронные деньги. Данная технология уже несколько лет применяется не только в цифровых финансовых системах, но и в других сферах экономики. Причем и программисты, и финансовые аналитики, и экономисты сходятся во мнении, что с каждым годом распространенность и востребованность блокчейн будет увеличиваться в геометрической прогрессии. Теперь конкретно хотелось бы поговорить о преимуществах данной технологии.

Во-первых, децентрализация. Блокчейн не имеет единого центра управления или места хранения, а поддержанием работоспособности занимаются непосредственно все участники сети, чьи ноды находятся по всему миру. Соответственно, решения касательно работы такой сети принимаются наиболее демократичным путем, а сама сеть является

крайне устойчивой. Блокчейн крайне тяжело взломать, он не подвергается цензуре, а управление единой компанией или государством невозможно.

Во-вторых, сохранность данных. Множественное дублирование данных среди ее участников гарантирует сохранность и неизменность внесенной в блокчейн информации. Более того, из-за специфики устройства блокчейна данную информацию невозможно подменить, отредактировать или удалить. А применение алгоритмов консенсуса говорит о том, что все транзакции, включенные в блокчейн, являются подтвержденными.

В-третьих, прозрачность транзакции. У каждый участник сети есть доступ ко всей истории транзакций, вплоть до самой первой транзакции. Поэтому, для того чтобы проверить, прошла ли та или иная транзакция между двумя адресами, необходимо всего лишь обратиться к их истории, хранящейся в блокчейне.

В-четвертых, высокая скорость транзакции. Поскольку блокчейн-сети являются одноранговыми, то транзакции происходят напрямую между пользователями, вне зависимости от их местонахождения и без участия посредников. Более того, сеть всегда доступна пользователям, она не имеет ограниченных часов работы и не уходит в оффлайн на праздники.

В-пятых, снижение транзакционных расходов. В связи с тем, что блокчейн-сети являются одноранговыми, чтобы провести транзакцию, не нужно прибегать к услугам посредников. Так, благодаря блокчейну пользователи могут упростить проверку транзакций, сократить время на валидацию сделок, увеличить ликвидность и снизить до минимума риски мошенничества. Более того, пользователи блокчейн-сети платят комиссии за подтверждение транзакций, которые, по сравнению с традиционными финансовыми институтами, такими как банки, намного ниже [2].

При всем выдающемся спектре преимуществ стоит отметить, что технология блокчейн далеко несовершенна. Он обладает несколькими весьма существенными минусами. Ввести налогообложение криптовалюты и финансовых операций, связанных с ней, а также создать правовое регулирование его использования, не так сложно, как проделать то же самое с блокчейном [3]. Во многих странах Европы и мира уже приняты соответствующие нормативно-правовые акты, регулирующие операции с криптовалютами. Передовиками в этом плане являются Австралия, Великобритания, Гонконг, Швейцария и Китай. Что касается блокчейна, то здесь ситуация намного сложнее. Эта технология сейчас не регулируется ни одной юрисдикцией мира. Во многом из-за этого с экономической точки зрения технология блокчейн неидеальна.

Во-первых, дорогостоящая технология. Имея высокую энергозависимость самого распространенного блокчейна с алгоритмом консенсуса Proof-of-Work за счет сложности трансакции, делает его очень дорогостоящей технологией, которая не всем по силам. Также стоит отметить, что дорогостоящей технологией блокчейн является еще и потому, что само создание системы и внедрение ее в какую-либо сферу является очень затратным.

Во-вторых, существенным минусом является размер блокчейна. На момент середины июня 2018 г. размер блокчейна Bitcoin составляет 171 ГБ. Это значит, что для поддержания сети каждая полная нода должна иметь достаточно памяти для хранения всех данных блокчейна. Чем больше в сети происходит транзакций, тем больше она весит и тем быстрее она растет. Также стоит иметь в виду, что предварительно каждая полная нода должна скачать всю историю транзакций, на что может уйти значительное количество времени. Как отметил Эдвард Сноуден о блокчейне Bitcoin: «Это просто несовместимо с механизмом, нацеленным на долгосрочную торговлю, потому что невозможно сохранять историю всех покупок, которые человек совершил за свою жизнь, при этом предоставляя другим доступ ко всем проведенным операциям».

В-третьих, отсутствие конфиденциальности. В блокчейне нет имен и фамилий, но это не значит, что сеть полностью анонимна. За каждым пользователем сети закреплен адрес кошелька, и все участники сети видят, какие транзакции с него совершались. Стоит пользователю хоть раз привязать данный адрес к какому-либо сайту или сервису, который сможет указать на его или ее личность, например, к криптобирже, то любой участник сети сможет узнать, сколько средств находится у конкретного человека, на что они тратились и кому отправлялись. В теории это может поставить под угрозу безопасность пользователя с большим количеством криптовалют, не говоря уже о компаниях, для которых данная уязвимость публичных блокчейнов является серьезной проблемой, поскольку может потенциально раскрыть конфиденциальную информацию о клиентах, продажах, контрагентах и прочем.

В-четвертых, хотя блокчейн и трудно взломать, это все же более чем реально. Совершить взлом блокчейна, как мы выяснили, можно несколькими способами.

1. Взлом через пользователя: такая уязвимость ведущая к взлому технологии связана с нарушением анонимности, заключающееся в публикации персональных данных. Они распространяются под анонимные вредоносные программы, которые маскируются под лицензионными программами, а сами являются пиратками.

2. Также воздействовать и взламывать блокчейн можно на уровне сети:

— хакерская атака DDoS (Distributed Denial of Service);

— «атака Сивиллы»;

— Eclipse attack, или «атака информационного затмения».

3. Атаки, которые не зависят от блокчейна и применимы ко всем сетевым технологиям. Одной из таких является: − дефейс — взлом сайтов блокчейн-проектов и подмена адреса для сбора средств на ссылки своих кошельков.

Подводя итог, мы можем сказать, что с технической точки зрения блокчейн-это база данных, представленная в виде распределенного реестра с возможностью открытой проверки у каждого участника. С экономической точки зрения же. Мы можем сказать, что блокчейн технология, которая больше напоминает сеть, связывающую партнеров без каких-либо посредников.

Многие сравнивают открытие блокчейн с открытием интернета, и это конечно связано из-за его выдающихся возможностей, однако он до сих остается полностью не изученным [1]. Впрочем большинство специалистов уверенны в блокчейне и предсказывают ему огромное успешное будущее в развитии нашего общества в экономической, информационной и даже социальной сфере.

Библиографический список

1. *Волошин И. П.* Типы блокчейн и анализ экономических характеристик // Экономическая безопасность и качество. 2018. № 4 (33). С. 65−69.

2. *Волошин И. П.* Управление доступом на основе блокчейн // Информационная безопасность регионов. 2017. № 3-4 (28-29). С. 5−8.

3. *Соколова Т. Н., Петрунин И. А.* Правовое регулирование использования криптовалют // Инновации и инвестиции как драйверы социального и экономического развития: сб. ст. Междунар. науч.-практ. конф. (Челябинск, 8 ноября 2017 г.). Уфа: Омега сайнс, 2017. С. 208−212.

4. *Tapscott D., Tapscott A.* Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World. Portfolio, 2016.

К. А. Тукалов, Т. А. Фарзалиев, Д. М. Назаров
Уральский государственный экономический университет, г. Екатеринбург

Защита персональных данных в информационном пространстве

Аннотация. Анализируется проблема защищенности персональных данных пользователей всемирной сети. Рассмотрены способы несанкционированного доступа к персональным данным пользователя, методы защиты своих конфиденциальных данных, а также цели, преследуемые злоумышленниками.

Ключевые слова: информационная безопасность; персональные данные; мошенники; безопасность данных.

Введение. Основной целью мошенников является получение персональных данных пользователей, а также получение данных банковских карт и электронных систем оплаты, с дальнейшим применением мошеннических схем, ведущих к денежному обогащению преступных лиц. Целью данной статьи является обзор способов кражи персональных данных, а также обзор способов защиты от киберпреступлений.

1. Способы получения персональных данных пользователей.

Благодаря современным технологиям получить персональные данные пользователей сети интернет стало гораздо проще благодаря ряду специализированного программного обеспечения, социальной инженерии и другим способам.

Самым распространенным и действенным методом является фишинговая атака — вид интернет-мошенничества, целью которого является получение конфиденциальных данных пользователя путем массовой рассылки электронных сообщений в различных сервисах или социальных сетях. При этом мошенники для повышения достоверности прибегают к использованию имен известных брендов, государственных органов и др., с целью завоевания доверия пользователей. В большинстве случаев внутри письма содержится прямая ссылка на сайт, внешне не отличимый от оригинала[1]. После того, как пользователь попадает на поддельный сайт, мошенники пытаются побудить пользователя к определенным действиям, которые в итоге приведут к раскрытию персональных данных, чаще всего это выражается в виде предложения ввести свои логин и пароль, которые используются для доступа к личному кабинету реального сайта или сервиса. Фишинг является одним из приемов социальной инженерии — психологической манипуляции людьми с целью определенных действий или разглашения конфиденциальной информации. Еще одним распространенным способом получения персональных

[1] *Steve* Mansfield-Devine. Darknets. Elsevier Science Publishing Company, Inc., 2009. P. 4–6.

данных является покупка баз данных в даркнете[1]. Обычно эти базы данных получаются от сотрудников компаний, желающих получить дополнительных доход.

2. Способы получения и использования данных банковских карт.

Согласно официальной статистике Центрального банка Российской Федерации на 1 января 2020 г. было выпущено 285 832 млн карт, которые используются для оборота денежных средств клиентами банков, но банковские карты являются столь же уязвимыми, как и персональные данные пользователей, и способы их получения в большинстве случаев совпадают с получением личных данных, а именно: социальная инженерия, фишинг, базы данных на черном рынке. Таким образом в ноябре 2019 г. на черный рынок поступили данные о более чем 60 млн кредитных банковских карт, как закрытых, так и действующих[2].

Полученные незаконными путями персональные данные пользователей и данные банковских карт используются мошенниками с целью личного обогащения незаконным путем. На данный момент существует множество способов для использования полученной информации о персональных данных и банковских картах одной из таких «схем» является вывод средств с банковских карт путем маскировки транзакций, использованием электронных платежных систем и крипто валюты, а в частности биткоина, так как принцип его работы обеспечивает достаточный уровень анонимности, что позволяет мошеннику оставаться не найденным[3]. Персональные данные, такие как паспортные данные могут быть использованы для оформления кредитных договоров в банках или микро финансовых организациях, после чего деньги поступают на счета мошенников аналогичными с прошлым методом способами.

Приведем конкретный пример. 12 октября 2020 г. YouTube[4]-блогер Р. Халилов стал жертвой мошенников, которые завладели его персональными данными, а именно: фотографиями паспорта и водительскими правами. Мошенники прибегли к шантажу по средством угроз взять на имя Рафаэля многомиллионные кредиты, а также перевести на его банковский счет деньги, полученные от наркотрафика, если не будет выполнено условие перевода денежной суммы в размере 30 тыс. р. на счет мошенников в течение 72 ч. Так же мошенники взяли на Рафаэля кредит в МТС-банке на сумму 15 тыс. р., чтобы доказать серьезность своих

[1] *Скрытая* сеть, соединения которой устанавливаются только между доверенными пирами, иногда именующимися как «друзья».

[2] *Статистика* национальной платежной системы // Официальный сайт Центробанка России. URL: https://old.cbr.ru/statistics/psrf/sheet013.

[3] *Интернет*-мошенничество — памятка для граждан // Официальный сайт МВД России. URL: https://xn--b1aew.xn--p1ai/document/1910260.

[4] *YouTube* — популярный видеохостинг.

намерений. По истечению нескольких часов мошенники начали массовую рассылку порочащей информации в социальных сетях. После обращения в полицию и придания огласке данной ситуации Рафаэлю удалось избежать всех неприятных последствий, связанных с мошеннической деятельностью[1].

3. Методы защиты персональных данных.

Безопасность персональных данных является одной из приоритетных задач для современного пользователя, который не желает стать жертвой мошенников. Для достижения этой цели существует ряд методов защиты информации:

1) шифрование данных пользователя: современные операционные программы имеют возможность шифрования данных по средством использования специализированного ПО;

2) защита аккаунтов в социальных сетях: при условии наличия нескольких аккаунтов следует использовать разные пароли, которые следует менять их раз в несколько месяцев;

3) установка антивирусной программы на устройства: лучший способ защитить свое устройство от вредоносного программного обеспечения и регулярно проверять свое устройство на наличие вирусного ПО;

4) защита Wi-Fi сети: установка сложного пароля значительно снизит вероятность доступа к сети посторонних лиц.

Заключение. Защита информации в сети является одной из актуальных тем на сегодняшний день. Благодаря невнимательности пользователей, распространением мошеннических схем и вредоносного программного обеспечения совершенно любой человек рискует оказаться жертвой мошенников.

[1] *Блогер* Рафаэль Халилов: «Мошенники оформили на меня кредиты по документам, слитым из каршеринга» // Рамблер. URL: https://news.rambler.ru/internet/45044312/?utm_content=news_media&utm_medium=read_more&utm_source=copylink.

А. В. Йовжий, К. Т. Назаров, Н. С. Удилов, В. Д. Лешуков
Уральский государственный университет путей сообщения, г. Екатеринбург

Сценарии и перспективы использования искусственного интеллекта в информационной безопасности

Аннотация. Представлена теоретическая часть распознавания и идентификации лица человека искусственным интеллектом, исходный код системы. Описаны способы использования искусственного интеллекта в информационной безопасности.

Ключевые слова: информационная безопасность; искусственный интеллект; машинное обучение; угрозы; компьютерное зрение; информация.

Искусственный интеллект (сокращенно — ИИ), **машинное обучение** и **нейронные сети** — термины, используемые для описания мощных технологий, базирующихся на машинном обучении и способных решать задачи реального мира[1].

ИИ строится на знаниях из математики, статистики, теории вероятностей, физики, обработки сигналов, машинного обучения, психологии, лингвистики, науке о мозге и многих других наук.

Актуальность развития ИИ повышается с ростом числа задач, решение которых зависит от большого числа переменных и трудоемких решений, алгоритмизировать которые вручную достаточно затруднительно.

В целом задачи можно разделить на рутинные и нерутинные. К первым относятся те, решение которых базируется на универсальном алгоритме: измерение влажности в комнате или алгебраические преобразования.

ИИ же предназначен для решения именно нерутинных проблем. Например, камеры дорожного движения, регистрирующие нарушения, определяющие госномер транспортного средства и отправляющие штраф нарушителю. Или системы безопасности на вокзалах, умеющие осуществлять поиск человека по фотографии. Все это сегодня принято считать искусственным интеллектом, хотя алгоритмы, лежащие в основе каждой такой технологии, уникальны. И только некоторые из них используют машинное обучение.

Искусственный интеллект — это название не какого-то конкретного алгоритма, а скорее множества методов, используемых для решения различного рода задач. Алгоритмы, базирующиеся на подходах с обучением, являются лишь одной из его подгрупп (рис. 1).

[1] *Искусственный* интеллект. URL: https://www.wikiwand.com/ru/Искусственный_интеллект.

Рис. 1. Уровни ИИ

Машинное обучение — это подход, при котором алгоритм «учится» решать задачу[1]. Например, распознавание котов и собак на фотографиях (рис. 2).

Рис. 2. Распознавание объектов на фотографии

Загрузив изображения с котами и собаками в алгоритм, мы можем заставить его «учиться» различать животных, «ругая» за ошибки в классификации и «поощряя» за правильные ответы. В зависимости от качества и количества предоставленных данных, а также от сложности используемого алгоритма, после некоторого количества итераций с «наказанием» и «поощрением», получается обученный алгоритм, способный с разной степенью успеха отличать котов от собак.

[1] *Как* работают искусственный интеллект, машинное и глубокое обучение. URL: https://trends.rbc.ru/trends/industry/5e845cec9a794747bf03e2c9.

Применяя методы машинного обучения, эти же алгоритмы можно научить выполнять более сложные задачи: поиск людей на кадре, определение пола, возраста, веса человека и прочее.

Термин **«глубокое обучение»** чаще всего используется чтобы описать некоторые нейронные сети и реализованные алгоритмы, которые принимают «сырые» входные данные и пытаются из этих входных данных получить полезную информацию. К таким «сырым» данным применяются определенные алгоритмы. При обработке, данные проходят несколько слоев нейросети для получения нужных выходных данных. Как машинное обучение является подвидом искусственного интеллекта, так и глубокое обучение является подвидом машинного. При «глубоком обучении» на вход алгоритму посылается большой объем входных данных и «наказывают» его за ошибки. Разница в том, что сами алгоритмы глубокого обучения устроены гораздо сложнее и часто используют более серьезные математические модели. Сейчас при использовании алгоритмов глубокого обучения чаще всего подразумевают нейронные сети.

Такое сравнение действительно имеет место быть. Нейронная сеть — это математическая модель, представляющая собой последовательность слоев, а также ее программное или аппаратное воплощение, построенное по принципу организации и функционирования биологических нейронных сетей. Каждый такой слой состоит из нейронов, выполняющих свои роли. Нейроны обучаемы, например, некоторые учатся выделять основные важные элементы на изображениях, такие как материал объекта из его фактуры; некоторые делают выводы, исходя из выделенных элементов — если машина больше определенного размера и есть прицеп, то это грузовой автомобиль. Нейроны объединяются в группы (слои), которые образуют единую искусственную нейронную сеть.

Процесс обучения алгоритма во многом напоминает процесс обучения человека. Человек, совершая ошибки, вероятнее всего получит какое-либо наказание, и, чтобы этого избежать этого в дальнейшем, учится на них; так и алгоритмы в машинном обучении при совершении ошибки получают штраф, после чего пытаются его избежать.

Чтобы понять принцип работы нейросети, рассмотрим процесс ее обучения распознаванию лиц. Залог успеха в обучении нейросети это: массив данных для анализа и санкции, применяемые к нейросети. В нашем примере это 10−20 фотографий лиц для каждого распознаваемого человека, и штраф, если представленный человек не совпадает с человеком на фотографии.

С математической точки зрения нейросеть — это функция с большим количеством параметров. Штрафование этой функции за неверное определение лица — это когда мы, упрощенно говоря, корректируем работу функции таким образом, чтобы в будущем она меньше ошибалась.

В свою очередь, поощрение нейросети — это когда мы ее просто не штрафуем.

Может ли нейросеть думать, как человек? Мыслительный процесс напрямую связан с наличием сознания. Нейронная сеть, как и любой другой алгоритм машинного обучения, по своей сути является лишь математической функцией и умеет решать лишь одну конкретную задачу. Нейросеть, которую обучили различать кошек и собак, не сможет отличить медведя от слона, ведь она даже не знает, что такие животные существуют. Процессы анализа данных, которые происходят в голове у человека, намного сложнее чем те, что происходят в нейросети, так что даже при наличии данных, сопоставимых по размеру с массивом информации, которую за жизнь получает человек, сегодня обучить нейросеть думать, как человек, невозможно.

ИИ проявляет себя в разных формах, поэтому очень важно понимать, чем именно он может быть полезен для той или иной сферы деятельности. ИИ интенсивно используется во многих областях, и круг его применений чрезвычайно быстро расширяется. Рассмотрим наиболее популярные сценарии.

Компьютерное зрение. Разработаны системы, предназначенные для обработки таких визуальных данных, как изображения и видео. Такие системы анализируют содержание изображений и извлекают полезную информацию на о сновании предоставленных типовых образцов. Например, Google использует технологию реверсивного (обратного) поиска изображений для нахождения визуально подобных изображений в интернете.

Обработка естественного языка. Системы этого типа предназначены для распознавания текстов, написанных на естественных языках. Мы можем взаимодействовать с машиной, передавая ей команды в виде текстовых предложений. Поисковые системы интенсивно используют эту технологию для доставки релевантных результатов поиска пользователям.

Распознавание речи. Эти системы способны воспринимать звуковую информацию и понимать произносимые слова. Например, наши смартфоны оборудованы интеллектуальными персональными помощниками, которые понимают голосовые команды и реагируют на них предоставлением соответствующей информации или выполнением запрошенных действий.

Экспертные системы. В этих системах методики ИИ используются для принятия решений или предоставления соответствующих рекомендаций. Как правило, в таких областях, как финансы, медицина, маркетинг и другие. Для этой цели используют базы знаний.

Игры. ИИ широко применяется в индустрии игр. Он используется для проектирования интеллектуальных агентов, способных состязаться в мастерстве игры с человеком. В качестве примера можно привести AlphaGo — компьютерную программу, которая умеет играть в стратегическую игру Go. ИИ также используется для проектирования игр другого типа, в которых от компьютера ожидается интеллектуальное поведение.

Робототехника. Робототехнические системы в действительности объединяют в себе многие концепции ИИ. Эти системы способны выполнять множество самых разнообразных задач. В зависимости от ситуации, роботы могут оборудоваться датчиками и приводными элементами, обеспечивающими выполнение всевозможных действий. Датчики могут распознавать предметы, находящиеся в поле их зрения, измерять их температуру, реагировать на выделяемое ими тепло или совершаемые ими движения и т.п. Встроенные процессоры выполняют расчеты в режиме реального времени. Кроме того, роботы могут адаптировать свое поведение к изменению внешних условий.

Некоторые из самых известных ИИ-систем:

— Deep Blue — победил чемпиона мира по шахматам;

— Watson — перспективная разработка IBM, способная воспринимать человеческую речь и производить вероятностный поиск с применением большого количества алгоритмов;

— MYCIN — одна из ранних экспертных систем, которая могла диагностировать небольшой набор заболеваний, причем часто так же точно, как и доктора.

Банки применяют системы искусственного интеллекта в кредиторской деятельности, при игре на бирже и управлении собственностью. Методы распознавания образов (включая как более сложные и специализированные, так и нейронные сети) широко используют при оптическом и акустическом распознавании (в том числе текста и речи), медицинской диагностике, спам-фильтрах, в системах ПВО (для определения целей), а также для обеспечения ряда других задач национальной безопасности.

Метод обнаружения объектов. Изображения и видеоролики окружают нас повсюду. На файлообменниках, в социальных сетях, на страницах поисковых систем. А камеры даже бюджетных моделей телефонов способны выдавать приемлемое качество фотоснимков. Программирование и разработка алгоритмов для обнаружения объектов по заданным параметрам на изображениях — область компьютерного зрения.

Основной целью мошенников является получение персональных данных пользователей, а также получение данных банковских карт и электронных систем оплаты, с дальнейшим применением мошеннических схем, ведущих к денежному обогащению преступных лиц. Целью

данной статьи является обзор способов кражи персональных данных, а также обзор способов защиты от киберпреступлений.

Исходный код алгоритма, позволяющего реализовать распознавание объектов, представлен ниже.

```
import os # модуль предоставляет функции для работы с операционной системой
import dlib # библиотека машинного обучения
import argparse # модуль для обработки аргументов командной строки
import glob # находит все пути в операционной системе, совпадающие с заданным шаблоном
parser = argparse.ArgumentParser() # объект ArgumentParser() для парсинга аргументов
parser.add_argument('--path_photos', dest = 'path_photos', help = 'Путь к папке с изображениями/фотографиями') # обязательный аргумент, который принимает путь к папке, где лежат изображения, на которых нужно найти объект
parser.add_argument('--path_train', dest = 'path_train', help = 'Путь к базе с данными для тренировки системы') # обязательный аргумент, который принимает путь к файлу для тренировки системы распознавания объектов
args = parser.parse_args() # содержатся все аргументы, которые были переданы скрипту
options = dlib.simple_object_detector_training_options() # функция simple_object_detector_training_options() содержит опции для тренировки системы
options.num_threads = 4 # передаём количество ядер компьютера, которые можно использовать для обучения, чем больше, тем быстрее обучается система
dlib.train_simple_object_detector(args.path_train, "detector.svm", options) # эта функция обучает систему. передаются параметры: путь к файлу для тренировки, имя выходного файла, опции тренировки
detector = dlib.simple_object_detector("detector.svm") # передаём в переменную detector метод simple_object_detector(), обнаруживающий объекты на основе гистограммы направленных градиентов (Histogram of oriented gradients - HOG)
window = dlib.image_window() # объявляем графическое окно для отображения изображений
for file in glob.glob(os.path.join(args.path_photos,'*')): # перебираем каждое изображение
    image = dlib.load_rgb_image(file) # передаём изображение и получаем массив из RGB значений
    dets = detector(image) # в каждом изображении система ищет необходимый объект
    window.set_image(image) # показываем итоговое изображение с найденным объектом
    window.add_overlay(dets) # на каждом изображение обводим прямоугольником найденный объект
    dlib.hit_enter_to_continue() # при нажатии на любую клавишу, показывает итоговые изображения по очереди
```

Ш. И. Ханбеков, О. А. Нестерова
Тюменский государственный университет, г. Тюмень

Особенности защиты информации в распределенных системах хранения на примере файловой системы Hadoop

Аннотация. Использование технологий больших данных российскими компаниями сравнительно новый тренд, развитие этого направления сталкивается с рядом трудностей, среди которых фактор возможности крупных утечек данных в распределенных системах хранения. В статье рассматриваются инструменты и принципы защиты данных в файловой системе с открытым исходным кодом Hadoop.

Ключевые слова: большие данные; распределенные системы хранения; защита данных; Hadoop; Hadoop Distributed File System.

Сегодня развитие российского рынка, охватывающего технологии хранения, обработки и анализа больших объемов данных, затруднено различными факторами: сравнительной новизной сферы и, как следствие, практически полным отсутствием в ней нормативно-правовой базы, а также рядом опасений как потенциальных пользователей таких систем, так и компаний-интеграторов, оказывающих услуги в данном направлении. Одна из наиболее острых проблем — дефицит специалистов[1], в результате чего руководите-лям обычно приходится заниматься переподготовкой имеющихся сотрудников, что затрудняется высокой стоимостью курсов и нехваткой доступных на русском языке материалов. Другим сдерживающим фактором, во многом обусловленным недостаточным правовым обеспечением сферы, является опасение крупных утечек конфиденциальной информации, и это небезосновательно: так, исследование, проведенное основателем поисковика Shodan, выявило свыше 47 тыс. неверно сконфигурированных серверов Apache Hadoop, что позволяло скомпрометировать более 5 тысяч терабайт информации, хранящейся в распределенных файловых системах[2].

В настоящей статье освещаются принципы защиты информации в распределенных системах хранения и рассматриваются инструменты обеспечения безопасности, используемые в файловой системе Apache Hadoop — фреймворка с открытым исходным кодом для обработки больших объемов данных.

Как правило область больших данных охватывает распределенные системы хранения[3]. Рассмотрим особенности защиты в них. Информа-

[1] *Большие* данные (Big Data) в России. URL: https://www.tadviser.ru/a/293060.
[2] *The* HDFS Juggernaut. URL: https://blog.shodan.io/the-hdfs-juggernaut.
[3] *Big* Data и информационная безопасность. URL: https://securenews.ru/big_data.

ция в таких системах содержится на большом кластере машин, где каждый узел участвует в обработке данных, предоставляя свои ресурсы: в первую очередь дисковое пространство, а также оперативную память и вычислительные мощности процессора. При этом, с точки зрения информационной безопасности, неверно утверждать, что машины кластера — это просто набор вычислительных ресурсов, занятых исключительно решением неких задач над данными. Каждый узел в таких системах фактически представляет собой отдельный компьютер, работающий в рамках определенной операционной системы, участвующий в обмене данными по сети, объединяющей все машины кластера.

Отсюда вытекает первая проблема обеспечения защиты распределенных систем хранения — большое число точек потенциальных угроз утечки данных или несанкционированного доступа. Ситуация осложняется еще и тем, что такие системы изначально предполагают, что пользователь не может заведомо знать, на какую из машин кластера данные будут записаны: для него выбор осуществляется прозрачно. Это означает, что для достижения информационной безопасности всей системы, необходимо в должной степени обеспечить защищенность каждого узла кластера, размер которого может составлять сотни и даже тысячи машин. При этом необходимо сохранить нормальное функционирование самой распределенной системы хранения — эффективное использование всех предоставляемых ресурсов для решения поставленных задач. По этой причине распределенные системы имеют некий головной узел, осуществляющий управление и контроль всех остальных машин в кластере. В Apache Hadoop таким узлом является NameNode — он содержит большую часть конфигурации системы, хранит метаданные файловой системы и осуществляет связь между клиентами и узлами DataNodes, занятыми непосредственно обработкой и хранением данных.

Другая задача информационной безопасности — обеспечить защиту узлов в условиях, в которых каждая отдельная машина уникальна: имеет свой набор жестких дисков, определенный объем оперативной памяти и вид процессора, причем сами компоненты могут быть от разных производителей; в крайних случаях узлы кластера вовсе могут работать под разными операционными системами. Таким образом, мы сталкиваемся с целым «зоопарком» устройств кластера — помимо непосредственно компьютеров сюда также включается и сетевое оборудование. Естественно, такая ситуация значительно усложняет подход, при котором все узлы кластера защищались бы по образу и подобию какого-нибудь отдельно взятого устройства системы. С другой стороны, как правило реальные распределенные хранилища проектируются, учитывая данную особенность. Кроме того, принимается и факт того, что «железо», активно используемое узлами кластера, — жесткие диски, ОЗУ

и т. д. — недолговечное и подвержено износу. Это также порождает необходимость обеспечить систему неким механизмом, минимизирующим вероятность полной или частичной потери данных в случае каких-либо ошибок устройств. В Hadoop Distributed File System (HDFS) это называется репликацией — дублированием блоков файла одновременно на несколько узлов кластера.

В российских реалиях защита информации систем хранения и обработки больших объемов данных усложняется также низким уровнем правового обеспечения сферы. Положительным моментом является то, что наработки в этом направлении ведутся: так, готовится к выпуску первый национальный стандарт, посвященный большим данным. Кроме того, разрабатываются за-конопроекты и предлагаются поправки существующего в области информа-ционных технологий и защиты информации законодательства[1].

В итоге специалисту по информационной безопасности необходимо тщательно изучить используемую распределенную систему хранения, ее архитектуру и принципы работы, чтобы обеспечить адекватную защищенность инфраструктуры больших данных.

Теперь подробнее рассмотрим один из основных элементов Apache Hadoop — его файловую систему, HDFS. Главная ее особенность заключается в том, что устанавливается HDFS поверх существующей файловой системы, т. е. каждый отдельный блок данных физически расположен в определенном для него каталоге на некотором узле кластера в рамках установленной системы хранения. Рассмотрим механизмы администрирования HDFS, выполняющие в том числе и функции обеспечения информационной безопасности.

Первый полезный инструмент — это квоты[2]. Существует два типа квот — ограничение на число файлов в директории и на общий размер директории. С помощью такого механизма достигается доступность файловой системы и в некотором роде поддерживается целостность — при неконтролируемом росте директорий неизбежны различные ошибки и торможения, вплоть до полного выхода устройства из строя.

К тому же большое число файлов затрудняет работу NameNode, что также влияет на время отклика при выполнении задач.

Помимо квот, файловая система Hadoop поддерживает ACL — списки контроля доступа[3]. Такой инструмент позволяет разграничить права пользователей на файлы и директории в зависимости от их роли

[1] *Большие* данные (Big Data) в России. URL: https://www.tadviser.ru/a/293060.

[2] *HDFS* Quotas Guide. URL: https://hadoop.apache.org/docs/current/hadoop-project-dist/hadoop-hdfs/HdfsQuotaAdminGuide.html.

[3] *HDFS* Permission Guide. URL: https://hadoop.apache.org/docs/current/hadoop-project-dist/hadoop-hdfs/HdfsPermissionsGuide.html.

и членства в каких-либо группах. Разрешения бывают трех типов — на чтение, на запись и на исполнение. Порядок определения доступа через ACL следующий: сначала проверяется совпадение с именем владельца файла, затем со всеми записями user, после этого то же самое происходит с группами и в конце проверяется поле other.

Важно отметить, что проверка происходит ровно до тех пор, пока одна из записей не удовлетворит выполнению операции — иными словами, если действие было отклонено, то все записи ACL запретили совершать это действие.

Очевидно, ACL в HDFS в точности идентично ACL в файловых системах UNIX. Конечно, такого разграничения не всегда бывает достаточно, но это тоже создает определенный эшелон защиты от несанкционированного доступа к конфиденциальным данным.

И квоты, и списки контроля доступа, являясь метаданными, хранятся на NameNode в файле fsimage. Для специалиста по информационной безопасности это означает две вещи: во-первых, сам файл fsimage должен быть защищен от пользовательской модификации, во-вторых, каталогам DataNode, в которых содержатся блоки данных, также необходима защита от доступа в обход службам Hadoop.

Последний инструмент, который мы рассматриваем, это прозрачное шифрование HDFS[1]. Шифрование осуществляется демоном Key Management Server — специально выделенным сервером, отвечающем за управление ключами. Обычно это отдельное устройство, но в случае небольшого кластера KMS можно разместить на NameNode.

Механизм шифрования заключается в создании зон шифрования (en-cryption zones) — директорий HDFS, зашифрованных на определенном ключе, который необходимо предварительно сгенерировать. После успешного создания такой зоны работа пользователя с самим каталогом и файлами внутри него осуществляется абсолютно прозрачно, т. е. в точности в таком же виде, как если бы шифрование полностью отсутствовало. Стандартная сборка Apache Hadoop поддерживает сравнительно скудный набор алгоритмов шифрования, но при необходимости можно внести изменения в исходный код, чтобы использовать иной криптографический подход.

Функцией шифрования не стоит злоупотреблять — это неизбежно приводит к падению производительности системы и нарушению свойства доступности информации. Шифровать следует те данные, которые являются конфиденциальными либо обращение к которым происходит относительно редко.

[1] *Transparent* Encryption in HDFS. URL: https://hadoop.apache.org/docs/current/hadoop-project-dist/hadoop-hdfs/TransparentEncryption.html.

Учитывая, что сбои в кластере Hadoop при выполнении тяжелых задач далеко не редкое явление[1], вопрос обеспечения доступности в данной системе стоит особенно остро — такие ошибки необходимо сводить к достижимому минимуму.

Итак, мы рассмотрели особенности обеспечения информационной безопасности в распределенных хранилищах, а также ознакомились с различными инструментами администрирования и защиты, применяемые в распределенной файловой системе Hadoop. Был описан их функционал и принцип работы. Очевидно, что неправильно полагаться исключительно на встроенные механизмы защиты, поскольку важно обеспечить безопасность не только самого кластера, но и всех составляющих его элементов — серверов с операционными системами, сетевого и вычислительного оборудования. Однако и пренебрегать этим инструментарием не стоит: каждый слой защиты вносит определенный вклад в поддержание общего уровня информационной безопасности системы.

[1] *Марц Н., Уоррен Д.* Большие данные: перспективы и практика построения масштабируемых систем обработки данных в реальном времени: пер. с англ. СПб.: ООО «Диалектика», 2018.

Содержание

Научные и прикладные исследования в области технической защиты информации

Математические методы информационной безопасности

Организационное и правовое обеспечение информационной безопасности

Программно-аппаратные средства защиты информации, компьютерная безопасность

Информационная безопасность в условиях цифровой экономики Российской Федерации

Безопасность информационного пространства

Сборник трудов
XIX Всероссийской научно-практической конференции
студентов, аспирантов и молодых ученых

(Екатеринбург, 8—11 декабря 2020 г.)

Печатается в авторской редакции и без издательской корректуры.

Компьютерная верстка *К. А. Терехиной*

Поз. 57. Подписано в печать 20.09.2021.
Формат 60 × 84 $^{1}/_{16}$. Гарнитура Таймс. Бумага офсетная. Печать плоская.
Уч.-изд. л. 14,0. Усл. печ. л. 15,6. Печ. л. 16,8. Заказ 437. Тираж 27 экз.
Издательство Уральского государственного экономического университета
620144, г. Екатеринбург, ул. 8 Марта/Народной Воли, 62/45

Отпечатано с готового оригинал-макета в подразделении оперативной полиграфии
Уральского государственного экономического университета