Цифровая трансформация общества и информационная безопасность

Материалы Всероссийской научно-практической конференции

(Екатеринбург, 18 мая 2022 г.)

Министерство науки и высшего образования Российской Федерации
Уральский государственный экономический университет

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ ОБЩЕСТВА И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

М а т е р и а л ы
Всероссийской научно-практической конференции

(Екатеринбург, 18 мая 2022 г.)

Екатеринбург
2022

УДК 004.056(082)
ББК 32.811я44
Ц75

Ответственные за выпуск:

кандидат экономических наук, доцент
А. Ю. Коковихин

доктор экономических наук, доцент
Д. М. Назаров

Ответственный редактор

С. В. Бегичева

Ц75 **Цифровая трансформация общества и информационная безопасность**: материалы Всероссийской научно-практической конференции (Екатеринбург, 18 мая 2022 г.) / ответственные за выпуск: А. Ю. Коковихин, Д. М. Назаров, ответственный редактор С. В. Бегичева; Министерство науки и высшего образования Российской Федерации, Уральский государственный экономический университет. – Екатеринбург: УрГЭУ, 2022. – 94 с.

Обсуждаются вопросы эффективного управления бизнес-процессами и информационной безопасностью современной организации и властных структур с применением корпоративных информационных систем и аналитических подсистем Big Data Analytics, развитие математических, статистических и инструментальных методов экономики, проблемы цифрового общества.

Для научных работников, магистрантов и аспирантов, студентов, участвующих в научно-исследовательской работе, представителей бизнес-сообщества и государственных структур.

УДК 004.056(082)
ББК 32.811я44

Информационная безопасность и компьютерные технологии

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

Методы защиты от DDoS-атак в интеллектуальных сетях

Аннотация. Обсуждаются уязвимые стороны интеллектуальных сетей, предлагающих потенциальные преимущества как для изготовителя товара и (или) услуг, так и для потребителей. Автором рассмотрены особенности организации защиты интеллектуальной сети от распределенных атак типа DDoS.

Ключевые слова: интеллектуальная сеть; промышленная система управления; DDoS; умная сеть электроснабжения.

Все чаще важные инфраструктурные системы, например, как энергоснабжение, подключаются к другим корпоративным интеллектуальным системам. Они варьируются от желания собирать статистику в режиме реального времени, тем самым оптимизируя операции и повышая эффективность, до необходимости удаленного обновления и обслуживания систем, чтобы свести к минимуму необходимые усилия и время, а также количество труднодоступных мест [2].

Частота кибератак на интеллектуальную сеть увеличилась в последние годы, и эти атаки в некоторых случаях приводили к сбоям в работе и краже личной информации [1].

На данный момент, практически все интеллектуальные сети работают автономно. Это означает, что они были изолированы от сети и, следовательно, больше не подвергались риску кибератак. Однако при внедрении в интеллектуальную сеть устройств Интернета, уязвимости, технические недоработки ПО в этих устройствах могут нарушить нормальную работу сети.

В настоящий момент, самой распространенной атакой на интеллектуальные сети является Рефлексивная DDoS-атака. Злоумышленник не атакует IP-адрес целевой службы напрямую, а использует некоторые специальные службы Интернета для открытия сервера.

SCADA (Supervisory Control And Data Acquisition – диспетчерское управление и сбор данных) – программный пакет, предназначенный для разработки или обеспечения работы в реальном времени систем сбора, обработки, отображения и архивирования информации об объекте мони-

торинга или управления. SCADA может являться частью системы экологического мониторинга, научного эксперимента, автоматизации здания. SCADA-системы используются во всех отраслях хозяйства, где требуется обеспечивать операторский контроль за технологическими процессами в реальном времени. Данное программное обеспечение устанавливается на компьютеры для связи с объектом, использует драйверы ввода-вывода или OPC/DDE серверы. Программный код может быть написан на одном из языков программирования, так и сгенерирован в среде проектирования. Практически все существующие интеллектуальные сети, работают по принципу SCADA.

Любое устройство, подключенное к SCADA, имеет IP-адрес, например, человеко-машинный интерфейс (HMI), что позволяет осуществлять его мониторинг и управление центральной инфраструктурой DNS. В атаке с усилением на DNS протокол, мы рассматриваем сценарий, когда хакер компрометирует главный DNS-сервер для организации такой атаки. Злоумышленник может отправлять пакеты UDP с поддельными IP-адресами на преобразователь DNS. Поддельный адрес в пакетах является фактическим IP-адресом HMI. Каждый из пакетов UDP запрашивает преобразователь DNS, часто передавая такой аргумент, как «ЛЮБОЙ», чтобы получить максимально возможный ответ. После получения запросов преобразователь DNS отправляет большой ответ на HMI. Целевая система получает ответ, и сеть становится перегруженной из-за переполнения трафика, что приводит к отключению сигналов тревоги и уведомлений, предназначенных для оповещения операторов о состоянии энергосистемы.

Уровень усилий, необходимых для организации DDoS атак, естественно, зависит от знания топологии коммуникационной сети. Злоумышленник может осуществлять такие атаки, получая несанкционированный удаленный доступ к устройствам интеллектуальной сети. Любое неисправное устройство в сети может быть использовано для продолжения внутренней DDoS-атаки, которая перекрывает работу нескольких узлов одновременно.

Исследование и внедрение новых решений непосредственно в сложную инфраструктуру интеллектуальной сети занимает много времени [3]. Доступ к данным об операциях интеллектуальной сети также затруднен из соображений безопасности и конфиденциальности [4].

Первое, на что нужно обратить внимание при работе с интеллектуальными сетями – это полная автономия этой сети. При подключении новых компонентов, нужно убедиться, что ПО и устройство, сможет стабильно работать автономно [4].

Второе – это качество настройки устройств, их стабильность и защищенность с физической точки зрения. Если к одному из устройств интеллектуальной сети будет иметься свободный доступ всех желающих, то о качестве защиты, не может быть и речи.

И последнее, все оборудование, подключенное в интеллектуальную сеть, должно быть качественно настроено, а также обслужено для стабильной работы сети.

Библиографический список

1. *Бегичева С. В.* Обзор методов обнаружения сетевых аномалий // Инновации в науке: пути развития: материалы XII Всероссийской научно-практической конференции (Чебоксары, 28 сентября 2020 г.). Чебоксары: Экспертно-методический центр, 2020. С. 6–10.

2. *Гольдштейн Б. С., Ехриель И. М., Рерле Р. Д.* Интеллектуальные сети. М.: Радио и связь, 2000. 500 с.

3. *Лихтциндер Б. Я., Кузякин М. А., Росляков А. В., Фомичев С. М.* Интеллектуальные сети связи. М.: Эко-Трендз, 2000. 205 с.

4. *Новичков А. Н.* Интеллектуальные сети для тех, кто еще не в курсе // Сети и системы связи. 1999. №10. С. 86–91.

Г. Д. Голубев
Уральский государственный экономический университет, г. Екатеринбург

Обзор безопасности маломощных глобальных сетей: угрозы, проблемы и потенциальные решения

Аннотация. Статья призвана обобщить недавние исследования ключевых проблем безопасности глобальной сети с низким энергопотреблением LPWAN, являющейся одной из самых быстрорастущих сетей в технологиях Интернета вещей (IoT).

Ключевые слова: глобальная сеть; кибербезопасность; атака; протокол; Интернет вещей.

Эволюционные тенденции в коммуникационных технологиях, которые привели к изобретениям, включая Интернет вещей (IoT) и Интернет всего (IoE), в значительной степени создали новые и лучшие стандарты жизни для людей и их среды [3]. Обеспечивая эффективную связь между различными устройствами, технологии IoT играют решающую роль в повышении качества жизни людей в широком спектре областей, которые не ограничиваются повседневными интеллектуальными приложениями (умные дома, умный транспорт, умное образование, умные города), экономичные приложения (повышение производительности на производственных предприятиях, горнодобывающих и нефтегазовых

месторождениях), приложения для здравоохранения и приложения для обеспечения безопасности [2; 4; 5]. Популярные стандарты ближнего действия, такие как IEEE 802.15.1 и IEEE 802.15.4, широко используются, но их малая дальность связи широко известна как серьезное ограничение, особенно потому, что различные ключевые домены IoT требуют большой дальности связи. В качестве альтернативы сотовые сети, обеспечивающие широкий диапазон подключений, были широко развернуты с различной пропускной способностью. Тем не менее, вопрос стоимости и сложности является основным ограничением. Глобальные сети с низким энергопотреблением (LPWAN) представляют собой жизнеспособную альтернативу различным недостаткам существующих стандартов подключения IoT. LPWAN, одно из самых выдающихся изобретений в области подключения к Интернету вещей за последние годы, представляет собой технологию беспроводной связи с завидными характерными характеристиками, включая дальнее покрытие, низкую скорость передачи данных, низкое энергопотребление и недорогие конечные устройства. Кроме того, они имеют возможность размещения множества конечных устройств, длительное время автономной работы и адаптацию к лицензированному и нелицензированному спектру, и в большинстве стандартов используется упрощенная звездообразная топология сети [1]. Однако, несмотря на желательные функции, которыми обладают технологии LPWAN, проблемы безопасности и конфиденциальности были серьезной проблемой при их широкомасштабном развертывании. Из-за неоднородности, повсеместного распространения и легкого доступа к устройствам в сети уязвимость LPWAN к угрозам и вторжениям продолжает расти в геометрической прогрессии [2].

Целью статьи является обобщение последних методологий исследования основных проблем безопасности LPWAN и разновидностей угроз, последствий атак и, что наиболее важно, различных подходов, предложенных в литературе для смягчения последствий атак.

1. Обзор LPWAN

LPWAN – это беспроводная технология, которая в последнее время продолжает привлекать огромное внимание. Технология специально разработана для связи на большие расстояния (до 50 км в зависимости от устройства LPWAN). Технологии LPWAN отличаются от других технологий подключения, поскольку они обладают выдающимися характеристиками, включая низкое энергопотребление, низкую стоимость, скорость передачи данных, емкость и мобильность. Кроме того, они обеспечивают возможность эффективного использования батареи, рассчитанную на более чем 10 жизнь батареи, универсальное подклю-

чение к глобальной сети, что позволяет использовать множество приложений M2M и IoT, в отличие от популярных сетевых устройств ближнего действия, таких как Bluetooth, Wi-Fi и ZigBee. Что касается сетевых топологий, большинство технологий LPWAN обычно развертывают сети с одним переходом на основе звездообразной топологии, поскольку это способствует сохранению заряда батареи, безопасной стоимости, а также компенсирует дальность связи. В зависимости от региона и стандартов LPWAN могут работать в нелицензируемых промышленных, научных и медицинских (ISM) диапазонах частот 2,4 ГГц, 868/915 МГц (Европа/Северная Америка), 433 МГц (Азия) и т.д. Некоторые LPWAN могут работать на лицензированных частотах. Некоторые общие атрибуты и характеристики LPWAN, которые делают их пригодными для подключения к Интернету вещей, обсуждаются ниже.

Низкое энергопотребление

Низкое энергопотребление считается одной из важных особенностей, приписываемых LPWAN. Сетевые устройства LPWA обычно питаются от батареи и обычно эффективны и надежны в течение очень длительного времени без вмешательства человека. LPWAN могут уменьшить количество потребляемой энергии за счет использования спящего режима [1]. В таких режимах приемопередающие устройства реагируют только тогда, когда данные должны быть переданы или получены.

Широкий или расширенный охват

Широкая зона покрытия также является одним из основных преимуществ для массового развертывания LPWAN. Расширенный диапазон покрытия позволяет конечным устройствам оставаться на связи с базовыми станциями, которые, возможно, находятся на расстоянии километров. Таким образом, развертывание сетевой инфраструктуры подходит для различных приложений, требующих подключения на большие расстояния, таких как умные города, управление электросетями и интеллектуальное сельское хозяйство, а также таких приложений, как подземные трубопроводы, где существующие традиционные коммуникационные технологии с трудом доходят.

Масштабируемость

Масштабируемость – одна из основных особенностей LPWAN. Хорошо известно, что технология LPWAN поддерживает масштабируемое подключение нескольких устройств без ущерба для качества услуг. Поскольку предполагается, что к 2025 г. количество подключенных устройств в среде IoT достигнет миллиардов и даже превзойдет рост сотовых технологий, ожидается, что технологии LPWAN будут играть ключевую роль в будущей схеме вещей.

Безопасность и конфиденциальность

Поскольку многочисленные кибератаки и угрозы вторжения продолжают препятствовать развертыванию беспроводных устройств, проблемы уязвимости безопасности и конфиденциальности были определены как серьезная проблема в приложениях IoT. Чтобы избежать вторжения, меры безопасности и функции, такие как аутентификация, шифрование (AES, RSA и т. д.) и аппаратная безопасность (например, защита от несанкционированного доступа), являются характеристиками, приписываемыми устройствам, подключенным к сети LPWA.

2. Проблемы безопасности LPWAN и потенциальные решения

Несмотря на многообещающие преимущества и прогнозируемое блестящее будущее LPWAN, в текущих работах по обеспечению безопасности, в разработке и развертывании существующего стандарта и т.д. все еще существуют серьезные проблемы безопасности, которые требуют дальнейших исследований. Большинство существующих в настоящее время мер безопасности и исследований в основном сосредоточены на криптографических алгоритмах и проблемах управления ключами. Несмотря на достигнутые успехи, ежедневно возникает ряд проблем безопасности, поскольку сети по-прежнему подвержены техническим проблемам, таким как вторжения. Таким образом, очень важно обеспечить эффективные меры безопасности, которые могут быстро идентифицировать, обнаруживать и изолировать скомпрометированные устройства. В этом разделе рассмотрены некоторые серьезные проблемы, которые представляют собой серьезные угрозы для текущего развертывания LPWAN.

2.1. Управление ключами и хранение

Управление ключами и их хранение всегда были серьезной проблемой в LPWAN. В LPWAN секретные ключи обычно хранятся в электрически стираемом программируемом ПЗУ (EEPROM) узлов. EEPROM очень уязвимы для различных атак, таких как атаки по сторонним каналам. Обращаясь к проблеме хранения ключей, если сервер приложений, на котором хранится весь секретный ключ, скомпрометирован, связь между всеми узлами в сети может быть скомпрометирована. Для обеспечения безопасного обмена данными в сетях необходимо рассмотреть адекватные меры безопасности, такие как надлежащее и быстрое шифрование, меры аутентификации, защита от несанкционированного доступа и элементы безопасности (SE).

2.2. Факторы шифрования

Одним из ключевых факторов, препятствующих полной реализации LPWAN, является проблема неэффективных мер шифрования. Шифрование в большинстве существующих стандартов LPWAN обеспечивает слабый уровень конфиденциальности и целостности данных.

Использование симметричного шифрования не защищено, поскольку для выполнения процесса шифрования используется один ключ. Хотя некоторые стандарты LPWAN используют асимметричное шифрование, такое как RSA, и надежные методы шифрования, такие как AES, лучшие и более быстрые методы шифрования для LPWAN должны быть в центре внимания.

2.3. Проблема с начальной загрузкой и аутентификацией

Эффективный и действенный контроль входа узлов LPWAN также является одной из основных тем безопасности LPWAN. Эффективное развертывание LPWAN требует надлежащей идентификации и проверки законных устройств, особенно устройств конечных узлов. Как правило, IoT использует серверы аутентификации в основном через протоколы доступа к сети, такие как протокол переноса аутентификации для доступа к сети (PANA) для присоединения узла к сети. В типичной настройке LPWAN с неадекватными мерами аутентификации злоумышленник может изменить зашифрованную полезную нагрузку, и сервер приложений не сможет заметить это изменение.

2.4. Глушение сигнала

Как и в любой другой киберсфере, глушение сигнала является серьезной проблемой для LPWAN. Близость злоумышленников к устройствам конечных узлов приводит к огромной вероятности глушения атак в LPWAN. Таким образом, эффективные и инновационные методы, такие как IDS, должны быть в центре внимания, чтобы уменьшить помехи в LPWAN.

2.5. Скомпрометированное устройство IoT и открытая среда

Поскольку LPWAN поддерживают огромное количество устройств IoT, развертывание этих устройств, работающих в открытой среде, делает их уязвимыми для различных угроз безопасности. Следовательно, для повышения надежности связи и улучшения качества обслуживания следует рассмотреть эффективные схемы безопасности для обнаружения, изоляции и классификации вредоносных узлов, такие как системы обнаружения вторжений. Кроме того, обеспечение решения проблем безопасности на физическом уровне, таких как развертывание эффективных средств защиты от несанкционированного доступа.

2.6. Ненадежные шлюзы

Шлюзы – это прозрачные мосты между конечными узлами и сетевым сервером. Они создают связь между конечными узлами и сервером. В большинстве сценариев реализации развернуто несколько номеров. Развертывание шлюзов в открытой среде делает их ненадежными устройствами. Поскольку шлюз взаимодействует напрямую с сетью, если злоумышленник получает доступ к шлюзу, данные, проходящие

через него, могут быть легко записаны и даже манипулированы. Манипуляции с этими шлюзами могут привести к повышенному энергопотреблению конечных устройств, что может вывести их из строя. Кроме того, связь между конечными устройствами и остальной частью сети может быть нарушена. Для обеспечения безопасной передачи данных необходим механизм аутентификации шлюзов, чтобы предотвратить атаки на сеть.

Выводы

LPWAN – одна из наиболее распространенных технологий и, возможно, самый быстрорастущий стандарт подключения в приложениях IoT. Однако технологии LPWAN имеют серьезную проблему в виде уязвимостей безопасности и конфиденциальности. Используя различные средства и лазейки на различных уровнях и инфраструктурах внутри сетей, злоумышленники могут атаковать и создавать нежелательные события, которые могут поставить под угрозу всю сеть. Чтобы решить эти проблемы, в данной статье представлен список основных угроз безопасности и конфиденциальности LPWAN.

Библиографический список

1. *Al-Garadi M. A., Mohamed A., Al-Ali A. K., Du X., Ali I., Guizani M.* A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security // IEEE Communications Surveys & Tutorials. 2018. Vol. 22, no. 3. P. 1646–1685. DOI: 10.1109/COMST.2020.2988293.
2. *Chaudhari B., Zennaro M.* LPWAN Technologies for IoT and M2M Applications. Academic Press, 2020. 456 p.
3. *Grammatikis R. P., Sarigiannidis P., Moscholios I.* Securing the Internet of Things: Challenges, Threats and Solutions // Internet of Things. 2019. Vol. 5. P. 41–70. DOI: 10.1016/j.iot.2018.11.003.
4. *Jose D. V., Vijyalakshmi A.* An Overview of Security in Internet of Things // Procedia Computer Science. 2018. Vol. 143. P. 744–748.
5. *Zeadallya S., Das A. K., Sklavosc N.* Cryptographic technologies and protocol standards for Internet of Things // Internet of Things. 2021. Vol. 14. DOI: https://doi.org/10.1016/j.iot.2019.100075.

Д. Д. Горбунов
Уральский государственный экономический университет, г. Екатеринбург

Криптовалюта и блокчейн: перспективы развития с точки зрения информационной безопасности

Аннотация. Статья посвящена технологии блокчейн и криптовалютам, их перспективе, анализу значимости для мира и рядовых пользователей. Рассмотрено влияние указанных технологий на развитие финансового рынка. Описаны проблемы блокчейна и криптовалют, а также возможные методы их решения.
Ключевые слова: цифровые технологии; криптовалюта; финансовая система; блокчейн; информационная безопасность.

Цифровые технологии – неотъемлемая часть современной жизни: они помогают нам во всех направлениях: политических, общественных, культурных, духовных и т.д. Массовое использование цифровых технологий требует постоянного внедрения чего-то нового и отличного от имеющегося, ведь развитие происходит во всех направлениях. Инновации в цифровых технологиях становятся источником новых идей, способных изменить привычное понимание бытия. Нельзя оставаться в стороне от цифровых технологий, потому что наш мир функционирует с помощью цифровых технологий, это новая интеллектуальная валюта.

Криптовалюта является перспективной цифровой технологией, к концу второго десятилетия XXI в. она стала невероятно популярной. Первые попытки создания криптовалют были предприняты Дэвидом Чомом в 1990 г. в системе электронных денег DigiCash, но пользователи не оценили инновацию, и компания обанкротилась. После этого было еще множество безуспешных попыток создания криптовалюты. Но даже сейчас, когда она находится в обороте не первый год, не все понимают, что это и как этим оперировать. Как следствие, люди относятся к данной системе с недоверием [3].

С момента появления первой системы электронных денег делаются постоянные попытки создания новых абсолютно разнонаправленных криптовалют, идентичных по структуре и совершенно непохожих на остальные. Таким образом, появилась революционная на момент ее возникновения валюта под названием «Биткоин», благодаря которой возросла популярность криптовалют. Биткоин функционирует с помощью технологии «Блокчейн». Блокчейн – это универсальный инструмент для построения различных баз данных, который обладает следующими преимуществами:

— децентрализация, что означает отсутствие головного сервера, вся информация находится в личном пользовании;

— полная прозрачность всех транзакции, проходящих в системе;

— конфиденциальность: все данные хранятся в зашифрованном виде. Пользователь может отследить все транзакции, но не может идентифицировать получателя или отправителя информации, если он не знает номера кошелька. Для проведения операций требуется уникальный ключ доступа;

— надежность: любая попытка внесения несанкционированных изменений будет отклонена из-за несоответствия предыдущим копиям. Для легального изменения данных требуется специальный уникальный код, выданный и подтвержденный системой;

— компромисс: данные, которые добавляются в систему, проверяются другими участниками.

Блокчейн является основой современного рынка криптовалют и рынка в целом. Технологию блокчейн можно внедрить в систему государственного голосования, в систему продаж между юридическими и физическими лицами, в создание договоров и т.д. Самые амбициозные и смелые проекты могут быть реализованы благодаря блокчейну, так как имеют защиту информации и уверенность в том, что ты неподконтролен конкретным лицам, а вся твоя деятельность ограничивается государственным законом.

Можно сказать, что положено начало эры криптовалют, новой финансовой системы [1]. Появляются деньги, созданные людьми и для людей, а управляют этими деньгами законы математики. Соответственно на фоне успеха биткойна появляется множество других криптовалют, например, ethereum (эфир), ripple (рипл), litecoin (лайткоин) и др. Всего насчитывается более 1000 криптовалют.

Казалось бы, что данная система не имеет изъянов, но это не так. К сожалению курсы криптовалют весьма неустойчивы, так, например, если в начале оборота Биткойн стоил 800 долл./шт., то через полгода он стоит 4000, еще через год 14000, а еще через года он обвалится и люди, которые приобрели его на пике понесут убытки, а те, кто успели продать его на пике хорошо заработали, но дальнейший прогноз поведения криптовалюты неизвестен [2].

Так же в связи с активным распространением криптовалюты на рынке появилось огромное множество мошенников, использующих ее в целях противоправного обогащения за счет обычных граждан, так как криптовалютные кошельки имеют весьма высокий уровень защиты и почти невозможно выявить владельца кошелька, на который был произведен перевод. В связи с тем, что на территории Российской Федерации оборот криптовалюты долгое время не контролировался законом,

мошенники оставались безнаказанны и чисты. Решение данной проблемы лежит в жесткой регламентации оборота и применения криптовалюты, как пример создании специальных исполнительных органов власти, занимающимся такими вопросами как: отслеживание нарушителей, принятие мер в отношении нарушителей, передача дел полиции, создание новых, более совершенных, способов защиты от мошенников.

Что касается информационной безопасности, то на территории Российской Федерации блокчейн активно используют в различных проектах. Например, машиночитаемые доверенности ФНС основаны на базе блокчейна, что говорит о необходимости постоянного мониторинга технологии и ее развитии на отечественном рынке.

Блокчейн децентрализован, по этой причине нельзя уничтожить или изменить исходные данные, это цепочка и если попытаться взломать одно из звеньев, то на остальные это не повлияет. Для информационной безопасности – это поле для новых решений, которое позволит вывести оборот данных и безопасность пользователя на новый уровень.

Когда международное признание криптовалют состоится, каждое государство должно позаботиться об обеспечении правового регулирования новшества, чтобы обезопасить граждан. Регулирование виртуальных валют будет относиться к гражданскому, валютному, финансовому законодательству и рынку ценных бумаг. Когда это произойдет. криптовалюта станет неотъемлемой частью жизни общества и основой виртуального финансового рынка.

Выводы

При должном надзоре за оборотом криптовалюты и регламентировании ее использования, она может стать основой финансового рынка, инновацией, изменившей экономику и право во всем мире, стать площадкой, свободной к новшествам и готовой к развитию. Если это произойдет, то рынок криптовалюты станет площадкой, на которой пользователи смогут совершать финансовые операции, не боясь мошенничества и обмана. Криптовалюта – это деньги, которые неподконтрольны и не зависят от государства, в эру нестабильности и риска полного обесценивания собственных средств она является отдушиной, которая вселяет некую уверенность в завтрашнем дне.

Наша страна постепенно движется к легализации криптовалюты. Появится новая площадка для инвесторов и бизнесменов, будут созданы новые организации. Развитие крипто индустрии позволит выйти с отечественным продуктом, возможно, на уровень мировой конкуренции.

Библиографический список

1. *Бурмистрова И. В*. Анализ рынка криптовалют на примере криптовалют биткоин и Риппл как вариант альтернативного инвестирования // Актуальные проблемы финансирования и налогообложения АПК в условиях глобализации экономики: сб. ст. V Всерос. науч.-практ. конф. (Пенза, 15–16 марта 2018 г.). Пенза: Пензенский ГАУ, 2018. С. 37–41.

2. *Цветкова Л. А.* Перспективы развития технологии блокчейн в России: конкурентные преимущества и барьеры // Экономика науки. 2017. Т. 3, № 4. С. 275–296.

3. *Шайдуллина В. К*. Правовое регулирование оборота криптовалюты: зарубежный опыт // Общество: политика, экономика, право. 2018. № 4. С. 49–54.

К. А. Долганов
Уральский государственный экономический университет, г. Екатеринбург

Технология блокчейн с точки зрения информационной безопасности

Аннотация. Рассматривается технология блокчейн в аспекте информационной безопасности. Приводится сравнительный анализ технологий публичного и приватного блокчейна.

Ключевые слова: информационная безопасность; кибербезопасность; публичный блокчейн; приватный блокчейн.

Блокчейн – это один из видов более широкого класса технологий хранения и синхронизации данных - распределенного реестра. Ключевой характеристикой всего класса технологий распределенной регистрации является отсутствие централизованного управления [2]. Каждый узел распределенной системы делает записи в своей версии реестра независимо от других узлов и синхронизируется с ними в рамках одноранговой сети. Особенностью блокчейна как типа распределенного реестра является то, что записи соединяются в инкрементальную цепочку блоков с использованием криптографических алгоритмов, отсюда и его название (англ. blockchain, цепочка блоков). Таким образом, блокчейн – это децентрализованная база данных, в которой все записи собираются в блоки и связываются между собой с помощью криптографии.

Объединяя свойства распределенного реестра с блочной структурой данных, основанной на криптографической связности, блокчейн может эффективно реализовать два из трех ключевых аспектов информационной безопасности – целостность и доступность информации [4]. Однако традиционная модель децентрализованной публичной блокчейн-сети, в силу своей архитектуры и идеологии не обеспечивает третий аспект ИБ – конфиденциальность данных. По этой причине, а также из-за проблем масштабируемости, появилась модель приватного блокчейна.

Приватный блокчейн обеспечивает конфиденциальность записей, поскольку доступ теперь предоставляется в соответствии с политиками безопасности.

Далее в статье будут рассмотрены, более подробно, публичный и частный блокчейн с точки зрения информационной безопасности.

Публичный блокчейн

История публичного блокчейна неразрывно связана с криптовалютами. Являясь базовым сценарием, который сформировал технологию в ее нынешнем виде, криптовалюты и связанные с ними финансовые инструменты продолжают активно развивать технологию и решать архитектурные ограничения первых реализаций. С другой стороны, капитал всегда привлекает значительное внимание злоумышленников, и публичные блокчейн-сети, генерирующие и обслуживающие цифровые ресурсы, постоянно подвергаются различным атакам [1].

Наиболее распространенные атаки напрямую не воздействуют на блокчейн-сети. Они нацелены на кражу активов, доступ к которым осуществляется с помощью приватного ключа.

Приватный ключ генерируется пользователем, и обеспечивает доступ к адресу в блокчейне, на котором может хранится цифровой актив. Зная значение приватного ключа, пользователь фактически владеет и может распоряжаться цифровым активом, закрепленным за ним. Публичный ключ используется в качестве адрес блока или кошелька, а также в качестве аутентификации подписи информации в других блоках другими участниками сети. С некоторым допущением можно сказать, что пара публичного и приватного ключа и являются блокчейн-кошельком.

Принимая во внимание эти особенности надежное хранение приватного ключа является основой безопасных операций с криптовалютой и другими активами [3].

Вектор атаки, направленный на получение доступа к приватному ключу напрямую не связан с блокчейн-сетью. Тем не менее, степень этого риска пытаются понизить в том числе с помощью архитектуры блокчейн-сети. В частности, набирают популярность децентрализованные сервисы, принципиально отличные от традиционных криптобирж. Они не хранят приватные ключи и персональные данные на своих серверах и выступают в качестве посредников для сопоставления заявок на покупку и продажу активов. Пользователь отправляет подписанные торговые команды (ордера), биржа сравнивает подходящие ордера на покупку и продажу актива, а непосредственно обмен происходит напрямую между участниками торгов.

Приватный блокчейн

Публичные блокчейн-сети, в целом, неплохо зарекомендовали себя в качестве инфраструктуры для электронных платежных систем. Сейчас

продолжаются попытки адаптировать публичный блокчейн под корпоративные нужды, но для многих бизнес-заказчиков и государственных заказчиков, публичный блокчейн с его независимостью и открытостью данных по-прежнему является неподходящей концепцией. Именно поэтому появились приватные блокчейн-сетей с контролем доступа и множества корпоративных блокчейн-проектов на их основе. Рассмотрим основные аспекты безопасности приватных блокчейн-сетей.

Очевидно, что частный блокчейн обеспечивает лучший контроль над инфраструктурой организации или группы компаний. Модель угроз для решений, работающих на частном блокчейне, больше не включает в себя ряд атак, относящихся к публичному блокчейну.

Контроль доступа является основной функцией частной блокчейн-сети, без разрешения оператора сети в ней не появится новый участник. Это обеспечивает доступность информации в классическом смысле информационной безопасности – только авторизованные участники имеют доступ к информации.

Ситуация с конфиденциальностью данных принципиально иная в приватных блокчейнах – это свойство реализовано с контролем прав на чтение записей в реестре [1].

Таким образом, подводя итог, можно сказать, что несмотря на действительно уникальный подход к защищенному хранению и обмену информацией, блокчейн-сети и решения на их основе могут быть уязвимы как для специфичных, так и для традиционных атак.

Блокчейн, может быть сам использован как решение информационной безопасности. В последнее время появляется все больше проектов по кибербезопасности, основанных на этой технологии.

Библиографический список

1. *Винья П., Кейси М.* Эпоха криптовалют. Как биткоин и блокчейн меняют мировой экономический порядок. М.: Манн, Иванов и Фербер, 2018. 432 с.

2. *Могайар У.* Блокчейн для бизнеса / предисл. В. Бутерина; пер. с англ. Д. Шалаевой. М.: Эксмо, 2018. 224 с.

3. *Nakamoto S.* Bitcoin: A Peer-to-Peer Electronic Cash System (2008).

4. *Tapscott D.* Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World. Portfolio, 2016. 324 p.

А. А. Иванов
Уральский государственный экономический университет, г. Екатеринбург

Ключевые понятия системного подхода к адаптивному мониторингу информационной безопасности киберфизических систем

Аннотация. Целью статьи является освещение темы адаптивного мониторинга информационной безопасности в киберфизических системах и рассмотрение ключевых понятий. В статье рассматривается проблема выбора наиболее подходящих методов для решения задач безопасности конкретной киберфизической системы.
Ключевые слова: киберфизическая система; адаптивный мониторинг; мониторинг информационной безопасности.

Развитие информационных технологий привело к появлению нового класса систем, которые известны как киберфизические системы (КФС). Эти системы объединят в себе цифровое и физическое управление определенным процессом. Более того, повсеместное внедрение информационных технологий привело к росту количества кибератак на самые разные сферы: от промышленного сектора до здравоохранения и так далее. На сегодняшний день существует большое количество нарушений безопасности, связанных с КФС. Многие ученые разрабатывают новые подходы к обеспечению безопасности киберфизических систем, включая методы аутентификации, шифрования и другие. Однако количество атак показывает, что преодоление систем защиты остается возможным [3]. Целью данной статьи является освещение темы адаптивного мониторинга информационной безопасности в киберфизических системах и рассмотрение ключевых понятий.

С активным внедрением информатизации в общественную жизнь, люди начали интегрировать информационные технологии в какие-либо физические процессы, что привело к появлению киберфизических систем. Это сложная физическая система, которая рассматривается со стороны интеграции цифровых вычислительных ресурсов и различных физических сущностей [1]. К таким системам можно отнести «умный дом», беспилотный транспорт, интернет вещи, автоматизированное производство и многое другое.

Основными характеристиками КФС являются:

— система является гибридной, поскольку в ее рамках происходит интеграция физических и цифровых процессов;

— КФС объединяет как вычислительные, так и коммуникационные возможности с мониторингом, а также контролем объектов;

— система разделяется на физические составляющие (датчики) и информационные системы.

Большое разнообразие КФС, их неоднородность как с конструктивной стороны, так и с технологической, особенности эксплуатации различных систем – все это усложняет задачу создания эффективных систем защиты. В связи с непрерывным изменением нормативно-правовой базы, расширение целей безопасности применительно к КФС требует непрерывных изменений в системах, обеспечивающих их безопасность.

В настоящее время методы защиты КФС активно развиваются и дополняются. Исследователи адаптируют решения для компьютерных сетей, разрабатывают узконаправленные подходы. Поэтому при наличии большого количества проблем выбрать наиболее подходящий конкретный метод довольно сложно. Стоит также отметить, что киберфизические системы изменяются не сами и не полностью, меняются их структурные элементы, связи между ними, а вместе с этим и настройки, конфигурации и требования к безопасности. В данном случае следует не создавать каждый раз новые системы защиты, а подстраивать уже существующие под условия. Для эффективного управления безопасности КФС необходимо создание новых адаптивных систем мониторинга информационной безопасности, которые способны обеспечить осведомление системы управления информационной безопасности с точки зрения эволюционного развития объекта защиты.

Правильный выбор эффективного набора методов, подготовка данных для их применения вовремя, а также корректировка набора методов и данных в случае изменения объекта или внешней среды требуют системного подхода к адаптивному управлению. Он основывается на системном анализе и построении взаимных отображений между проблемами безопасности и методами их решения и уже имеющимися наборами данных.

Подход к рассмотрению исследуемого объекта в системном анализе общей теории систем, который применяется для решения задач интеллектуального адаптивного мониторинга, позволяет сформулировать общие принципы адаптивного мониторинга информационной безопасности КФС, такие как: принцип целостности, принцип эволюционной приспособляемости, принцип иерархической связности.

Принцип целостности. Данный принцип заключается в комплексном рассмотрении объекта исследования, который может быть применен ко всем задачам безопасности. Оценивается как внутренняя, так и внешняя среды функционирования. Любая система рассматривается и как совокупность компонентов или систем меньшего размера, и как часть системы более высокого порядка. Принцип целостности устанавливает способность системы мониторинга учитывать все виды задач безопасности, включая оценку безопасности, анализ операционной среды, изменение целей защиты и так далее. Для реализации этого принципа объект

защиты представляется в виде постоянно обновляющегося набора всех наблюдаемых внешних и внутренних параметров его функционирования за счет технологий управления данными.

Принцип конвергенции предполагает изменение системы мониторинга информационной безопасности в результате эволюционного развития объекта защиты и среды его функционирования. Требуется не только сохранение выполнения текущего списка задач безопасности, но и изменение его в процессе эволюции защищаемой системы и среды. Также необходима автоматизированная или автоматическая перестройка процесса мониторинга при изменении условий работы. Это важно для того, чтобы набор измеряемых параметров объекта мониторинга в текущем режиме работы определялся внешними факторами и являлся динамическим в процессе функционирования.

Принцип иерархической связности подчеркивает иерархическую организацию систем и компонентов при рассмотрении объекта защиты с точки зрения системного анализа. Он позволяет рассмотреть объект в виде совокупности иерархически связанных представлений, которые соответствуют разной степени детализации компонентов объекта мониторинга и уровней мониторинга с точки зрения теории и методов обеспечения информации безопасности.

Каждый метод решения какой-либо проблемы безопасности требует определенного набора входных данных. Базовая модель безопасности, которая управляется данными, генерирует эти наборы. Таким образом каждый набор можно назвать порождающей моделью (согласно теории сложных систем [4]).

Адаптация подходов мониторинга к постоянно меняющимся условиям заключается в изменении методов обработки данных [2]. Однако это необходимо лишь в тех случаях, когда старые методы больше не соответствуют требованиям (например, в скорости обнаружения определенного количества атак). Также при условии, что изменились доступные наборы данных, а следовательно, старые методы больше не применимы, по причине отсутствия данных. Для обеспечения правильной производительности и соответствия ограничениям при мониторинге адаптации, может использоваться подход теории оптимального выбора.

Выводы

Реализация адаптивного мониторинга информационной безопасности КФС в современных реалиях является сложной задачей по причине многообразия задач безопасности и динамических характеристик объекта защиты. Использование системного подхода и теории систем позволяет сформулировать принципы мониторинга: целостность, конвергенция и иерархическая связность, которые обобщают систематический подход к адаптивному мониторингу.

В рамках подхода в соответствии с принципом целостности объект защиты (КФС) рассматривается с различных сторон, от отдельных компонентов до объекта в целом, а также характеристики внешней окружающей среды. При управлении адаптивными характеристиками мониторинга для обеспечения соответствия системы мониторинга к охраняемому объекту и дальнейшей реализации принципов, построение процесса взаимного отображения между задачами безопасности, методами их решения, используются доступные данные. На основе этого процесса можно определить оптимальную схему мониторинга, включающую наборы различных задач, методов, данных и сопоставить между ними, соответствующие граничные условия.

Библиографический список

1. *Кутейников Д. Л., Ижаев О. А., Зенин С. С., Лебедев В. А.* Киберфизические, кибербиологические и искусственные когнитивные системы: сущность и юридические свойства // Российское право: образование, практика, наука. 2019. № 3. С. 75–81.

2. *Лаврова Д. С., Зегжда Д. П., Зайцева Е. А.* Моделирование сетевой инфраструктуры сложных объектов для решения задачи противодействия кибератакам // Вопросы кибербезопасности. 2019. № 2(30). С. 13–20.

3. *Coletta A., Armando A.* Security Monitoring for Industrial Control Systems // Bécue A., Cuppens-Boulahia N., Cuppens F., Katsikas S., Lambrinoudakis C. (eds.). Security of Industrial Control Systems and Cyber Physical Systems. CyberICS WOS-CPS 2015. Lecture Notes in Computer Science. Vol. 9588. Springer, Cham, 2015. https://doi.org/10.1007/978-3-319-40385-4_4.

4. *Wang H., Li S.* General Systems Theory and Systems Engineering. Springer, Singapore, 2018.

Д. О. Килишевский, Д. Б. Ковтун
Уральский государственный экономический университет, г. Екатеринбург

Интеллектуальные методы обнаружения сетевых атак: обзор и направления исследований

Аннотация. Приведена классификация сетевых атак. Содержится описание систем обнаружения сетевых атак с использованием различных интеллектуальных методов, включая модели машинного обучения (ML – Machine learning) и глубокого обучения (DL – Deep learning).

Ключевые слова: сетевая безопасность; сетевая атака; обнаружение атак; машинное обучение; глубокое обучение.

Стремительное развитие технологий сделало Интернет легкодоступным, и в настоящее время он активно используется большинством

людей для выполнения множества профессиональных и личных задач. Интернет помогает поддерживать связь и общение, но целостность и конфиденциальность этих соединений и обмена информацией могут быть нарушены и скомпрометированы злоумышленниками, которые стремятся повредить и нарушить сетевые соединения и их безопасность.

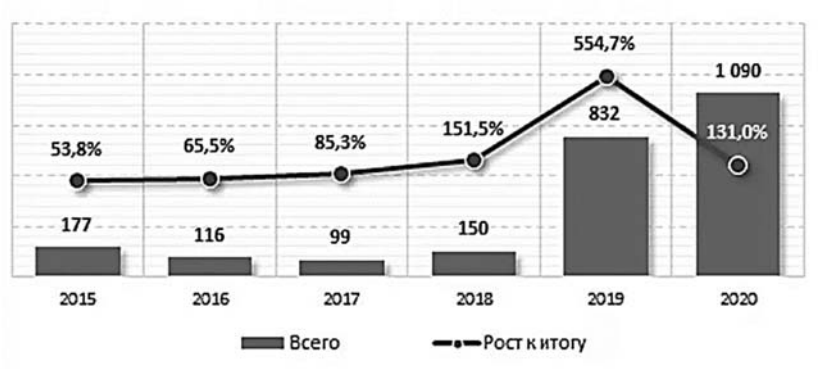
Количество атак, нацеленных на сети, растет с течением времени, что приводит к необходимости их анализа и понимания, а также разработки более надежных средств защиты безопасности. В России примером может послужить банк угроз информационной безопасности. Так для того, чтобы процесс обнаружения факторов риска был максимально быстрым и эффективным, в марте 2015 г. ФСТЭК сформировала Банк данных угроз, который постоянно дополняется.

В начале XXI в. широкое распространение получили концепции интеллектуальных методов, а именно машинного обучения (ML) и глубокого обучения (DL). Исследователи по всему миру признали, что эти методы могут значительно увеличить потенциал вычислений, поскольку они сосредоточены на использовании статистических методов и данных, чтобы заставить компьютеры думать так, как думают люди. Следовательно, эти интеллектуальные методы начали использоваться учеными, исследующими сетевую безопасность, поскольку они могли исключить ограничения неинтеллектуальных методов. В области сетевой безопасности алгоритмы ML или DL могут быть обучены работе с сетевыми данными для распознавания типа трафика как нормального, так и вредоносного, таким образом защищая сети от злоумышленников. Кроме того, алгоритмы могут быть обучены определять тип атаки, если сетевой трафик является вредоносным, станет возможным инициировать соответствующие действия для предотвращения атаки. Анализируя прошлые кибератаки, модель можно научить подготавливать индивидуальные защитные реакции [2].

Приведем классификация сетевых атак и обозначим интеллектуальные методы их предотвращения.

Сетевая атака – это подход к повреждению, выявлению, изменению, уничтожению, краже или получению незаконного доступа к сетевому системному ресурсу [1]. Потребность в более эффективных и стабильных системах сетевой безопасности для защиты данных бизнеса и клиентов растет, поскольку не существует сети, невосприимчивой к сетевым атакам.

Одним из ярких примеров может послужить Фишинг – один из наиболее популярных видов мошенничества в интернете. Его цель – получить личные данные пользователя, включая и банковские счета (см. рисунок).



Динамика количества фишинговых атак, ед.

Атака может происходить изнутри (внутренняя атака) или извне (внешняя атака). Чтобы защитить организации и отдельных лиц от кибератак, сетевой трафик сначала должен быть проанализирован и классифицирован, чтобы можно было обнаружить аномалии и вредоносные атаки. Поскольку роль классификации вредоносного трафика очень важна, многие исследователи стремились улучшить методы классификации.

Начнем с понимания того, что DL – это подмножество ML, которое является подмножеством искусственного интеллекта (ИИ). В некоторых исследованиях для построения моделей обнаружения использовался ряд методов DL, в первую очередь искусственная нейронная сеть ANN. Сложность использования правильного набора данных и функций или правильных алгоритмов ML и DL для идентификации различных типов атак оказалась одной из самых трудных задач для классификации и предотвращению сетевых атак разных типов. В данной статья рассматриваются три наиболее популярных видов сетевых атак: инсайдерская угроза, DDoS-атаки и фишинговые атаки.

Инсайдерская угроза – это нарушение безопасности, исходящее изнутри организации, например, через сотрудников, обладающих внутренней информацией о методах обеспечения безопасности, данных и компьютерных системах. Проблемой послужило то, что меры кибербезопасности, как правило, сосредоточены на угрозах вне организации, а не на угрозах внутри, которые могут вызвать проблемы с информационной безопасностью организации. В связи с этим условием, в первую очередь были рассмотрены именно эти угрозы. В качестве набора данных использовались записи, которые были взяты из строк журнала событий сети компьютера моделируемой организации [4]. Исследование

было сосредоточено на двух подходах к прогнозированию: «следующий шаг времени» и «тот же шаг времени». Результаты экспериментов показали, что подход «с тем же временным шагом» приводит к более высокой производительности. После этого исследователи преобразовали векторы признаков в матрицы фиксированного размера. Наконец, с помощью нейронной сети ANN была классифицирована матрица признаков на аномалии или нормальные, точность данной матрицы достигла 94,49 % [4]. Далее ученые использовали методы DL для построения модели аутентификации пользователя, основанной на характеристиках поведения мыши, которые можно было бы использовать для мониторинга и обнаружения внутренних аутентификаций. Они использовали набор данных с открытым исходным кодом, называемый Balabit Mouse Dynamics Challenge dataset и алгоритм ANN, который продемонстрировала высокую производительность при аутентификации пользователей на основе функций мыши с коэффициентом ложного принятия (FAR) 2,94 % и коэффициентом ложного отклонения (FRR) 2,28 %. Благодаря этому они научили машину различать вредоносные инсайдерские атаки.

Одной из наиболее опасных угроз сетевой безопасности являются распределенные атаки типа «отказ в обслуживании» (DDoS), которые пытаются нарушить доступность сервисов. Поскольку DDoS легко запустить, но нелегко обнаружить, так как в большинстве случаев трафик атаки очень похожи на допустимый системой безопасности, некоторые исследователи сосредоточились исключительно на их обнаружении с использованием различных подходов ML.

Для решения этой проблемы предлагается использование DeepDefense, который представляет собой подход обнаружения DDoS-атак на основе DL. Отличительной чертой DeepDefense является изучение шаблонов последовательности сетевого трафика и отслеживание действия сетевых атак. Был использован набор данных под названием UNB ISCX intrusion detection evaluation 2012 (ISCX2012), и алгоритм RNN для построения модели. Были извлечены 20 полей сетевого трафика для создания трехмерной карты объектов. Data14 и Data15 были извлечены из ISCX2012, которые содержали 9.6 M пакетов и 34.9 M пакетов соответственно. Общее количество обучающих выборок в data14 и data15 составило 15 176 и 233 450 соответственно [3]. Результаты эксперимента показали, что модели DL уменьшили частоту ошибок на 39,69 % по сравнению с методами ML в небольшом наборе данных. Для больших наборов данных снижение частоты ошибок составило от 7,517 до 2,103 %. Для дальнейшего улучшения алгоритмов было предложено увеличение разнообразия векторов DDoS и системных настроек, чтобы протестировать модель DeepDefense, а также сравнить DeepDefense с другими алгоритмами ML.

Исследование, предлагающее модель анализа и обнаружения DDoS-атак на уровне сети и уровне обслуживания экосистемы биткойнов, было проведено позднее. Набор данных состоял из реальных DDoS-атак и содержали следующие значения: затронутую услугу, дату атаки, категорию услуги, количество сообщений и т.д. Из данных биткойн-блока исследователи извлекли статистические данные, такие как максимум, минимум, суммирование и стандартное отклонение. Результаты показали, что точность обнаружения DDoS-атак составила около 50 %, а точность классификации обычных блочных данных – около 70 %.

Некоторые исследования были сосредоточены на обучении моделей и тестировании их для обнаружения фишинговых атак. Например, одной из целей была защита от фишинговых атак путем разработки модели обнаружения атак с использованием алгоритмов RF(RandonForest) и DT(DataTree), которые являются алгоритмами ML. Для обработки ML использовался традиционный набор данных фишинговых атак от Kaggle, содержащий 32 параметра [5]. Для анализа характеристик набора данных в предполагаемой модели использовался PCA – тип алгоритма выбора признаков. Достигнут уровень точности 97 % по RF. Дальнейшие исследования включали прогнозирование фишинговых атак по зарегистрированным атакам в наборе данных путем применения ANN и реализации IDS (Системы обнаружения и предотвращения вторжения). Целью разработанной модели было получить способность к обобщению, что означает, что точность классификации при обучении и тестировании должна быть максимально схожей. Набор данных включал 600 легальных и 800 фишинговых веб-сайтов с 17 характеристиками, полученными с помощью их собственного инструмента. Точность обучающих и тестовых наборов составила 94,07 и 92,18 % для 1000 наборов соответственно [5]. Принцип модели заключался в использовании адаптивной схемы с четырьмя процессами, включая структурную простоту, адаптацию скорости обучения, адаптацию структурного дизайна и подход к ранней остановке, основанный на ошибках проверки.

Выводы

Сетевая безопасность является серьезной проблемой для частных лиц, коммерческих и некоммерческих организаций, а также правительственных организаций. На самом деле, с информационным подъемом, который мы наблюдаем в нынешнюю эпоху, обеспечение сетевой безопасности является насущной необходимостью. Для того, чтобы внедрять в повседневную жизнь общества тысячи новых услуг, которые в основном опираются на основу цифровой жизни, нам необходимо усовершенствовать безопасность сети. Поэтому информационная безопасность оказывается насущным требованием, а не роскошью. Хотя многие

методы защиты были введены, все еще есть некоторые уязвимости, которые используются хакерами, оставляя администраторов сетевой безопасности в непрерывной гонке против сетевых злоумышленников. Методы, основанные на использовании интеллектуальных методов, а именно машинного обучения (ML) и глубокого обучения (DL), доказали свои достоинства в нескольких областях, включая системы здравоохранения, финансовый анализ, высшее образование, энергетику и т.д. Это действительно побудило людей, ответственных за сетевую безопасность, продолжить изучение возможностей этих методов в обеспечении требуемого уровня сетевой безопасности.

Библиографический список

1. *Бегичева С. В.* Обзор методов обнаружения сетевых аномалий // Инновации в науке: пути развития: материалы XII Всерос. науч.-практ. конф. (Чебоксары, 28 сентября 2020 г.). Чебоксары: Экспертно-методический центр, 2020. С. 6–10.
2. *Васильев В. И., Шарабыров И. В*. Обнаружение атак в локальных беспроводных сетях на основе интеллектуального анализа данных // Известия ЮФУ. Технические науки. 2014. № 2 (151). С. 57–67.
3. *Гетьман А. И., Маркин Ю. В., Евстропов Е. Ф., Обыденков Д. О.* Обзор задач и методов их решения в области классификации сетевого трафика // Труды ИСП РАН. 2017. Т. 29. № 3. С. 117–150.
4. *Колпаков А. Л.* Применение алгоритмов интеллектуального анализа данных в системах обнаружения вторжений // Безопасность информационного пространства – 2017: сб. тр. XVI Всерос. науч.-практ. конф. студентов, аспирантов, молодых ученых (Екатеринбург, 12 декабря 2017 г.). Екатеринбург: Изд-во Урал. ун-та, 2018. С. 29–31.
5. *Татарникова Т. М., Богданов П. Ю.* Обнаружение атак в сетях интернета вещей методами машинного обучения // Информационно-управляющие системы. 2021. № 6 (115). С. 42–52.

И. Е. Черепанов
Уральский государственный экономический университет, г. Екатеринбург

Безопасный метод связи, основанный на хэш-цепочке сообщений

Аннотация. Обсуждаются особенности метода цепной связи – метода безопасной связи, основанного на цепочке хэш-сообщений Обосновываются преимущества указанного метода по сравнению с традиционными методами сетевой связи.
Ключевые слова: хэш-цепочка сообщений; метод цепной связи; цепная подпись; эндогенная безопасность.

В настоящее время приложения сетевой связи повсеместно распространены, вызывая различные проблемы безопасности. Получатель данных хочет получить все содержимое данных, отправленное адресантом, и хочет, чтобы данные были полными, аутентичными. В начале проектирования существующих методов сетевой связи основное внимание уделяется только связности передачи данных, в то время как безопасность передачи данных игнорируется. Эта модель принципиально не имеет эндогенных механизмов безопасности, а также является основной причиной проблем безопасности, таких как подмена личности, подделка адреса, и отказ в обслуживании в киберпространстве. Кроме того, слабая связь между каждым сообщением в потоке данных приводит к низкой надежности процесса передачи данных.

Для предотвращения таких случаев используются такие протоколы и пакеты безопасности как:

— IPSec (IP Security) − пакет безопасности сетевого уровня в основном используется для проверки целостности, шифрования данных и аутентификации источника данных. Минус такого пакета в том, что он предназначен для локальных задач и внедрение данной технологии очень трудозатратный процесс;

— AH – протокол аутентификации, обеспечивает целостность передаваемых сообщений, аутентификацию источника данных и защиту от повторного воспроизведения;

— ESP – протокол инкапсулирующей нагрузки безопасности.

Все эти схемы используют хэш-цепочку для шифрования данных или ключей для достижения более высокой безопасности содержимого данных, предотвращая при этом взлом и подделку зашифрованного содержимого, и ни одно из решений не направлено на повышение эффективности безопасной передачи данных.

Стремясь к недостаткам вышеуказанных традиционных методов сетевой связи, предлагается новый метод безопасной связи, основанный

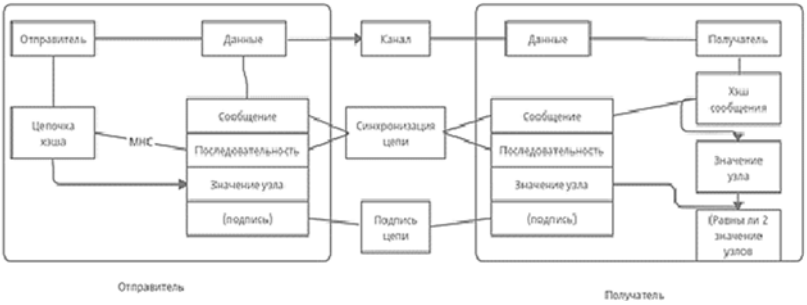
на цепочке хеширования сообщений, называемый методом цепочки хеширования сообщений (MHC) [2]. Основные вклады предлагаемого метода MHC суммируются следующим образом:

— метод MHC использует новый метод передачи по цепочке для обеспечения отсутствия подделки, отказа и более высоких требований к надежности нескольких сообщений. Основная идея состоит в том, чтобы итеративно хэшировать дайджест переданного сообщения, чтобы сформировать цепочку хэшей о последовательности сообщений. Две сообщающиеся стороны могут обеспечить целостность, неизменность и синхронизацию последовательности сообщений через хэш-цепочку, тем самым эффективно гарантируя безопасность передачи сообщений;

— при выполнении подписи данных и аутентификации обе стороны должны выполнять аутентификацию подписи только для сообщений через определенные промежутки времени и не должны завершать ее для каждого сообщения. Таким образом, может быть обеспечена подлинность и не отрицательность всех ранее переданных сообщений, снижены накладные расходы на аутентификацию подписи и значительно повышена эффективность безопасной передачи сообщений [1];

— использование порядкового номера и значения узла цепочки хэш-сообщений метода MHC может обеспечить анти-защиту от повторов и обеспечить надежность.

Метод MHC применяется не только для определенного уровня в модели сети TCP / IP, но и для каждого сообщения в потоке данных, которое может быть применено к любому логическому уровню. Структурная схема модели цепной связи. Метод MHC добавляет порядковый номер сообщения (Sequence) и значение узла полей message hash chain. Последовательность используется для обеспечения надежности процесса передачи, а значение узла цепочки хэша сообщения используется для проверки сообщения (см. рисунок).



Модель цепной связи

В методе MHC необходимо задать порядковый номер, поскольку при построении цепочки значения узлов хэш-цепочки сообщений должны вычисляться в строгом порядке [3]. Разница между порядковым номером, содержащимся в цепочке хеширования сообщений, и тем, что содержится в IPSec, заключается в том, что поле порядкового номера является необязательным полем в IPSec, которое в основном используется для предоставления услуг защиты от воспроизведения, в то время как поле порядкового номера метода MHC является необходимым полем, а каждый узел хэша должен быть построен в соответствии с порядковым номером.

Протокол IP без механизма безопасности обладает самой высокой эффективностью передачи, но не обладает никакими свойствами безопасности, что легко вызывает сетевые атаки. После того как IP-протокол подписан и аутентифицирован пакет за пакетом, хотя безопасность его передачи повышается, это также резко снижает эффективность передачи. Как протокол AH, так и протокол ESP IPSec могут обеспечить целостность, невмешательство и определенную надежность сообщений, а протокол ESP также может обеспечить конфиденциальность сообщений. Однако эти два протокола не могут гарантировать отклонения сообщений в процессе передачи и уязвимы для атак отказа с обеих сторон.

Выводы

Метод MHC улучшает традиционный протокол IP. Использование улучшенного метода MHC для замены традиционного протокола IP может гарантировать, что передача сетевого уровня имеет механизм безопасности и надежности и отслеживаемость сообщения. Хэш-цепочка сообщений может обеспечить целостность, неизменность и синхронизацию передаваемых данных. В то же время использование технологии цепной подписи и аутентификации позволяет значительно снизить накладные расходы на аутентификацию подписи и повысить эффективность безопасной передачи последовательностей сообщений. Метод MHC предъявляет более высокие требования к надежности процесса передачи.

Библиографический список

1. *Блэк У.* Интернет: протоколы безопасности: учеб. курс. СПб.: Питер, 2001. 288 с.

2. *Зубов А. Ю., Алферов А. П., Кузьмин А. С.* Основы криптографии: учеб. пособие. 2-е изд., испр. и доп. М.: Гелиос АРВ, 2002. 480 с.

3. *Таненбаум Э., Уэзеролл Д. Т.* Компьютерные сети. 5-е изд. СПб.: Питер, 2012. 960 с.

Н. С. Жильцов, Е. В. Кислицын
Уральский государственный экономический университет, г. Екатеринбург

Исследование секторов мирового рынка полупроводниковых приборов

Аннотация. Рассматриваются секторы мирового рынка полупроводников, сравниваются ассортимент и доходы крупнейших компаний данного сектора.
Ключевые слова: полупроводник; полупроводниковый прибор; рынок полупроводников; процессор; микрочип; запоминающее устройство; диод; материнская плата.

В последние время, можно увидеть активно развитие рынка полупроводниковых устройств. Полупроводниковым прибор является электронное устройство, принцип работы которого основан на свойствах полупроводников. Полупроводник – вещество, проводимость которого, зависит от температуры, к ним можно отнести большое количество химических элементов и их соединений, но наиболее часто применяются: кремний (Si), арсенид галлия (GaAs) и германий (Ge) (рис. 1).

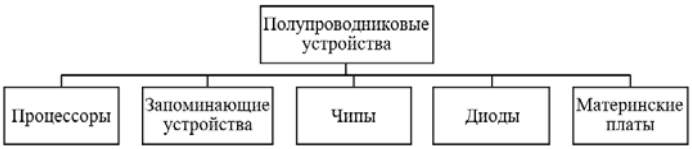


Рис. 1. Основные сегменты рынка полупроводниковых устройств[1]

Разберем развитие каждого сегмента по очереди, и начнем с процессоров. Процессор (Центральный процессор, ЦП) – электронный блок или интегральная схема, выполняющая вычисления и обработку данных (за исключением некоторых математических операций, осуществляемых в компьютерах, имеющих сопроцессор). Процессоры делятся на следующие категории:

— для настольных ПК. Данный тип процессоров используется в стационарных компьютерах, и их производство массово. В мире можно выделить два абсолютных лидера по их производству – это Intel и AMD;

[1] *Ситников А. В., Ситников И. А.* Прикладная электроника: учебник. М.: КУРС; ИНФРА-М, 2022. 272 с.

— для мобильных ПК. Данная категория процессоров используется в ноутбуках, нетбуках и так далее. Отличительной особенностью данной категории можно назвать наличие большого количества процессоров, с заниженным энергопотреблением. Здесь ситуация по производителям аналогична настольным ПК;

— процессоры для мобильных устройств. Они используются в смартфонах с теми же целями, что и в ПК. Лидерами по их производству являются такие компании, как Qualcomm и MediaTek;

— серверные. Процессоры данной категории используются в серверах. Как правило, они обычно работают с более низкой средней тактовой частотой на ядро, в отличие от настольных процессоров. Лидерами по их производству также являются Intel и AMD, но у них есть и отечественные конкуренты в лице МЦСТ Эльбрус и Байкал электроникс;

— графические. Процессоры, которые находятся в видеокартах и выполняют графический рендеринг. В мире выделяется 2 лидера по их производству: Nvidia и ATI.

Следующий сегмент – это запоминающие устройства (далее – ЗУ). Можно выделить две категории ЗУ:

— оперативная память (ОЗУ) − полупроводниковая память, предназначенная для временного хранения программ и данных;

— HDD и SSD – твердотельные накопители, предназначенные для долгосрочного хранения данных.

Безусловным лидером по производству ЗУ является Kingston. По данным на 2020 г., данной компании принадлежало 78 % рынка ОЗУ, и 27 % твердотельных накопителей (табл. 1, 2).

Таблица 1

Доля производителей ОЗУ на рынке за 2020 г.

Место	Название компании	Доля, %
1	Kingston Technology	78,02
2	ADATA Technology	3,19
3	Ramaxel	3,11
4	Kimtigo	2,91
5	POWEV	2,40
6	Другие	10,38

Таблица 2

Доля производителей твердотельных накопителей на рынке за 2020 г.

Место	Название компании	Доля, %
1	Kingston Technology	27
2	ADATA Technology	8
3	Kimtigo	7
4	Netac	6
5	Lexar	6
6	Другие	46

Еще одним из крупнейших сегментов рынка полупроводников являются чипы. Интегральная микросхема (чип) – это электронная схема произвольной сложности (кристалл), изготовленная на полупроводниковой подложке (пластине или пленке) и помещенная в неразборный корпус или без такового в случае вхождения в состав микросборки.

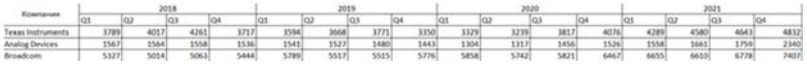
Чипы подразделяются на следующие подвиды:

— аналоговые. В их основе лежат простейшие усилительные каскады. С помощью множества каскадов создаются различные усилители, стабилизаторы напряжения тока, преобразователи частоты, фазы, длительности, генераторы синусоидальных, прямоугольных и других сигналов и т.д. Они используются в телевизорах, устройствах звукоусиления и звуковоспроизведения, измерительных приборах, технике связи и пр.;

— цифровые. В их основе лежат транзисторные ключи, которые могут находится в двух состояниях: открытом или закрытом. Их использование дает возможность создавать логические триггерные и прочие интегральные микросхемы. Они применяются в устройствах дискретной обработки информации ЭВМ, системах автоматики и т.д.;

— аналого-цифровые преобразователи (АЦП) – это электронные устройства, преобразующие входные аналоговые сигналы электрических величин (в большинстве случаев – напряжения), в выходные цифровые сигналы в виде, пригодном для последующей их обработки в микропроцессорных и других цифровых устройствах. Используется в тех случаях, когда надо преобразовать аналоговый сигнал в цифровой (дискретный).

В производстве аналоговых интегральных схем лидируют такие компании как, Texas Instruments, Analog Devices. Выручка компаний (в миллионах USD) за 2018, 2019, 2020 и 2021 гг., производящих аналоговые и цифровые интегральные схемы. Перевод в USD в данной таблице, и ниже, сделан по курсу валюты на 15 марта 2022 г. (рис. 2).



Компания	2018				2019				2020				2021			
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Texas Instruments	3789	4017	4261	3717	3594	3668	3771	3350	3329	3239	3817	4076	4289	4580	4643	4832
Analog Devices	1567	1564	1558	1536	1541	1527	1480	1443	1304	1317	1456	1526	1558	1661	1759	2340
Broadcom	5327	5014	5063	5444	5789	5517	5515	5776	5858	5742	5821	6467	6655	6610	6778	7407

Рис. 2. Доходы лидирующих компаний по производству чипов[1]

Другой немаловажный сегмент – это диоды. Светодиоды – это полупроводниковый прибор с электронно-дырочным переходом, создающий оптическое излучение при пропускании через него электрического тока в прямом направлении.

Можно выделить несколько крупнейших компаний по производству светодиодов. К таким компаниям относятся: Acuity Brands, Cree, Eaton и Osram. Годовая выручка этих компаний в миллионах USD, данные взяты с сайтов компаний (рис. 3).

Компания	Год			
	2018	2019	2020	2021
Acuity Brands	3680	3673	3326	3461
Cree	924,9	1080	903,9	525,6
Eaton	21609	21390	17858	19517
Osram	???	???	2185	847

Рис. 3. Доходы компаний по производству диодов[2]

Последним основным сегментом являются материнские платы. Материнская плата – это печатная плата, являющаяся основой построения модульного устройства. По состоянию рынка материнских плат, можно выделить четыре крупнейших компании по их производству: Asus, Gigabyte, MSI и ASRock. В табл. 3 представлена годовая выручка данных компаний.

Таким образом, данная статья дала ряд важных результатов. Во-первых, были рассмотрены сегменты рынка полупроводниковых приборов, такие как процессоры, ЗУ, чипы, диоды и материнские платы, а также, были даны определения данных понятий. Во-вторых, были рассмотрены доходы лидирующих компаний в данных сегментах рынка полупроводников.

[1] *Analog Devices*: сайт. URL: https://www.analog.com/en/index.html; Texas Instrument: сайт. URL: https://www.ti.com; Broadcom: сайт. URL: https://www.broadcom.com.

[2] *Acuity Brands* (AYI): годовые финансовые отчеты US GAAP// Acuity Brands. URL: https://smart-lab.ru/q/AYI/f/y; SMART-LAB. URL: https://smart-lab.ru; *Eaton* (ETN) выручка US GAAP (годовые значения) // SMART-LAB. URL: https://smart-lab.ru/q/ETN/f/y/GAAP/revenue/; *Osram* LichtAG (OSRn) // Investing.com. URL: https://ru.investing.com/equities/osram-licht-income-statement.

Таблица 3

Годовая выручка Asus, Gigabyte, MSI и ASRock компаний, млн долл. США[1]

Компания	2018	2019	2020	2021
Asus	12 593,14	12 491,56	14 676,41	13 629,46
Gigabyte	2 166,14	2 196,63	3 008,05	3 251,46
MSI	4 214,24	4 284,07	5 208,91	5 210,01
ASRock	12 593,14	12 491,56	14 676,41	13 629,46

Д. Т. Имранова, Е. В. Кислицын
Уральский государственный экономический университет, г. Екатеринбург

Развитие мирового рынка полупроводников

Аннотация. В исследовании представлена динамика развития мирового рынка полупроводников и его секторов с 2017 по 2021 г.
Ключевые слова: полупроводники; рынок полупроводников; сектор рынка; продажи; дефицит.

В исследовании приводится динамика развития мирового рынка полупроводников. Исследование основано на статистических данных за 2017–2021 гг. Гипотеза состояла в предположении, что к 2022 г. рынок активно восстанавливается от мирового кризиса полупроводников.

Целью работы являлось изучение динамики рынка полупроводников с 2017 по 2021 г. В исследовании были использованы такие методы, как анализ источников по теме и сопоставление точек зрения экспертов.

Крупнейшими компаниями на рынке являются Intel, Samsung и TSMC. Intel и Samsung сами занимаются разработкой и производством собственных чипов, в то время как TSMC имеет своих продуктов, специализируясь на производстве. TSMC является тайваньской компанией, Intel американской, а Samsung корейской. Согласно данным Boston Consulting Group и Semiconductor Industry Association[2] основная доля производства полупроводников в мире сейчас принадлежит азиатским странам: Тайваню, Южной Корее, и Китаю. По данным TrendForce, доля Тайваня в общемировом производстве составляет

[1] *Материнские платы* (мировой рынок) // Tadviser. URL: https://www.tadviser.ru/index.php/Статья:Материнские_платы_(мировой рынок); *Investing.com.* URL: https://ru.investing.com.

[2] *Рынок* полупроводников: дефицит чипов и кому он выгоден // Conomy. URL: https://conomy.ru/analysis/articles/333.

63 %, Южной Кореи – 18 %, Китая – 6 %, на долю остальных стран приходится 13 % (рис. 1).

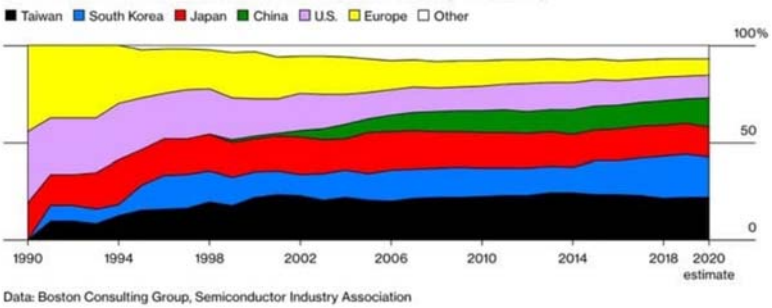


Рис. 1. Доли мирового производства полупроводников по странам[1], %

Почти во всех категориях продаж полупроводников для конечного использования в 2020 г. произошли значительные изменения. Некоторые категории, такие как компьютеры, значительно выросли, другие, к примеру, автомобильный, в течение года имели значительные колебания в продажах, но в итоге потеряли часть своей доли рынка (см. таблицу).

Мировой спрос на полупроводники по конечному потребителю (2020 г.)

Сфера конечного потребления	Доля продаж, %
Компьютеры	32,3
Средства коммуникации	31,2
Потребительская техника	12,0
Промышленность	12,0
Автомобилестроение	11,4
Правительство	1,0

Сост.: *2021 SIA* State of the Industry Report // Semiconductor Industry Association (SIA). URL: https://www.semiconductors.org/state-of-the-u-s-semiconductor-industry.

Согласно данным Semiconductor Industry Association за 2020–2021 гг. ежемесячный рост продаж чипов в совокупности всех потребительских секторах быстро увеличился (рис. 2). Мировой рынок в 2020 году вырос на 6,8 % в сравнении с 2019 годом (рис. 3).

[1] *Рынок* полупроводников: дефицит чипов и кому он выгоден // Conomy. URL: https://conomy.ru/analysis/articles/333.

Рис. 2. Рост продаж в основных потребительских секторах[1]

Рис. 3. Мировые продажи полупроводников, млрд долл.[2]

Если смотреть на динамику продаж полупроводников за 2018–2020 гг. становится видно, что не смотря на увеличение спроса в связи с пандемией COVID-19, в 2019 г. продажи упали.

Не в последнюю очередь это связано с кризисом полупроводников, произошедшим в том числе из-за сложностей, связанных с логистикой, а также из-за дефицита базовых деталей: интегральных схем, микроконтроллеров, сенсоров (рис. 4).

Касаемо прогнозов, мнения экспертов разнятся. По мнению генерального директора, Intel Патрика Пола Гелсингера, дефицит чипов продлится как минимум до 2024 г. При этом исследовательская компания

[1] *2021 SIA* State of the Industry Report // Semiconductor Industry Association (SIA). URL: https://www.semiconductors.org/state-of-the-u-s-semiconductor-industry.

[2] Там же.

IDC представила прогноз, согласно которому к середине 2022 года в отрасли произойдет нормализация спроса и предложения, а в 2023 г. возможна ситуация возникновения переизбытка выпускаемой продукции.[1]

Рис. 4. Продажи полупроводников с 2015 по 2020 г., млрд долл.

Лилиан Ли, вице-президент и старший кредитный специалист Moody's, также считает, что наращивание производства полупроводниковых устройств может привести к переизбытку в виду производства большего количества микросхем, чем необходимо на рынке[2].

Выводы

В виду постоянно меняющихся обстоятельств, на данный момент спрогнозировать дальнейшее развитее мирового рынка невозможно. Сейчас на отрасль влияют не только очевидные причины спада – сложности с логистикой, добычей и обработкой полупроводников, но и санкционные обстоятельства.

[1] *Глава Intel* считает, что нехватка полупроводников сохранится минимум до 2024 года // ТАСС. URL: https://tass.ru/ekonomika/14512587?utm_source=yandex.ru&utm_medium=organic&utm_campaign=yandex.ru&utm_referrer=yandex.ruhttps://www.idc.com/getdoc.jsp?containerId=prAP48247621.

[2] *Now there's* worry the chip shortage will turn into a chip glut // Fortune. URL: https://fortune.com/2021/08/03/chip-global-shortage-glut-semiconductor-supply.

Д. Р. Киприянов, Л. В. Кортенко
Уральский государственный экономический университет, г. Екатеринбург

Проектирование общей схемы CRM-системы для автоматизации бизнес-процесса сопровождения продаж

Аннотация. Авторами представлено разработанное под задачи бизнеса специальное программное обеспечение по управлению взаимоотношениями с клиентами, или CRM-система (Customer Realtionship Management System) для оптимизации маркетинга, систематизации работы с клиентами и анализа внутренних бизнес-процессов компании.

Ключевые слова: CRM; Customer Realtionship Management System; web-приложение; интернет; продажи; клиент.

Предметом настоящего исследования стало обеспечение поддержки бизнес-процессов, сопровождающих продажи компании, через разработку программного продукта, соответствующего требованиям компаний [1].

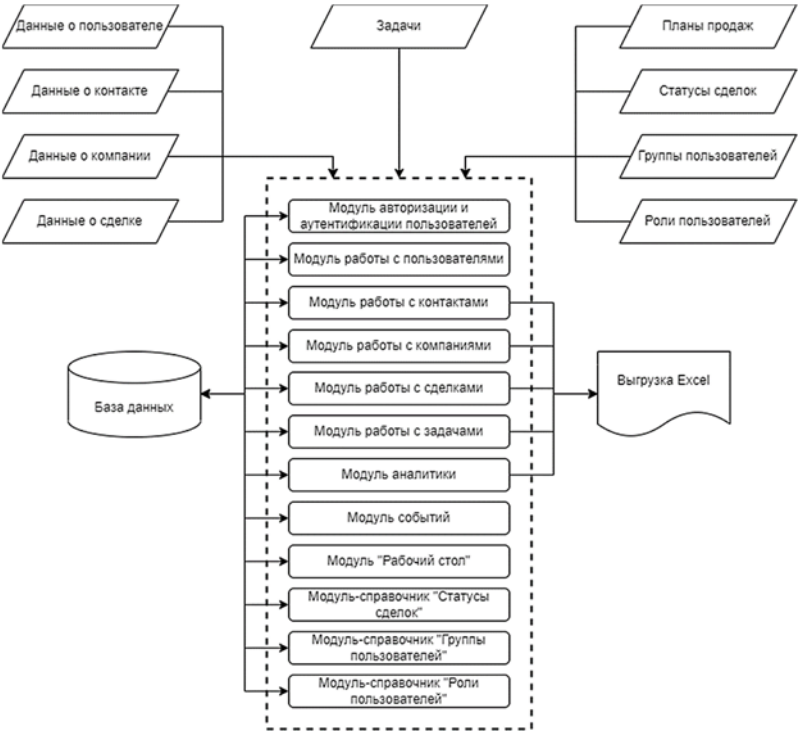
Реализуемой в разрабатываемом программном обеспечении гипотезой стало предположение о том, что за счет упрощения ведения реестра контрагентов увеличится производительность труда менеджеров, которые в освободившееся время смогут искать новых потенциальных клиентов [3].

Пошаговая детализация проектов в CRM с включением в систему самих исполнителей позволит произвести анализ затраченного времени, что увеличит количество проектов, которые одновременно могут разрабатываться и исполняться в организации.

При проектировании общей схемы разрабатываемой CRM-системы, исходя из установленных к ней требований авторами было определено, что программный продукт должен включать в себя модули: авторизации и аутентификации пользователей, «Пользователи», «Контакты», «Компании», «Сделки», «Задачи», «Аналитика», «События», «Рабочий стол», «Статусы сделок», «Группы пользователей», «Роли пользователей».

В процессе работы системы в нее заносятся данные о пользователях, контактах, компаниях, сделках, планах продаж, задачах и справочная информация. Данные, введенные в одном из модулей, должны быть доступны и в остальных модулях системы, а также модули работы с контактами, компаниями, сделками, задачами и аналитикой должны иметь возможность выгрузки данных в Excel.

На рисунке представлена общая схема разрабатываемой системы.



Общая схема разработанной CRM-системы

База данных в составе CRM-системы выполняет следующие функции:

— хранение информации, собранной в процессе работы системы;

— обеспечение эффективного доступа к хранимой информации;

— обеспечение целостности данных при работе системы.

Основной функционал CRM-системы распределен между ее составляющими модулями следующим образом.

Функции модуля авторизации и аутентификации пользователя:

— проверка подлинности учетной записи пользователя по введенным логину и паролю;

— предоставление пользователю установленных прав на выполнение определенных действий.

Функции, выполняемые модулем работы с пользователями:

— просмотр списка пользователей;

— создание, редактирование и удаление пользователей;

— установка прав и группы.

Функции, выполняемые модулем работы с контактами:

— просмотр списка контактов;

— поиск по списку контактов и фильтрация по атрибутам;

— создание, редактирование и удаление контактов;

— возможность просмотреть связанную с контактом компанию;

— привязка компании к контакту;

— создание и просмотр задач по контакту.

Функции, выполняемые модулем работы с компаниями:

— просмотр списка компаний;

— поиск по списку компаний и фильтрация по атрибутам;

— создание, редактирование и удаление компаний;

— возможность просмотреть связанные с компанией контакты;

— привязка нескольких контактов к компании;

— назначение основного контакта;

— создание и просмотр задач по компании.

Функции, выполняемые модулем работы с сделками:

— просмотр списка сделок;

— поиск по списку сделок и фильтрация по атрибутам;

— создание, редактирование и удаление сделок;

— возможность просмотреть связанные с сделкой компанию, контакты;

— привязка компании и контактов к сделке;

— назначение основного контакта;

— создание и просмотр задач.

Функции, выполняемые модулем работы с аналитикой:

— просмотр и выгрузка в Excel прогресса выполнения планов продаж на выбранный период;

— создание, редактирование и удаление планов продаж;

— просмотр сколько сделок на каком этапе, в том числе успешно реализованных и не реализованных.

Функции, выполняемые модулем работы с задачами:

— просмотр списка задач на сегодня, а также на ближайшие периоды;

— создание, редактирование и удаление задач;

— возможность просмотреть связанную с задачей сущность (контакт, компанию или сделку);

— привязка задач к одной из сущностей: контакт, компания, сделка.

Функции, выполняемые модулем «Рабочий стол»:

— просмотр сводной информации по текущему прогрессу продаж, активным задачам и новым сделкам.

Функции, выполняемые модулем «Статусы сделок»:

— просмотр списка этапов сделок;

— создание, редактирование и удаление этапов сделок;

— возможность настройки порядка этапов сделок.

Функции, выполняемые модулем «Группы пользователей»:

— просмотр списка групп пользователей;

— создание, редактирование и удаление групп пользователей.

Функции, выполняемые модулем «Роли пользователей»:

— просмотр списка ролей пользователей;

— создание, редактирование и удаление ролей пользователей;

— настройка прав для каждой роли.

Начиная разработку базы данных CRM-системы определим, что она содержит в себе набор таблиц данных о задействованных в функционировании системы сущностях [2]. Основными таблицами базы данных разработанной CRM-системы с их назначением стали:

1) «users» – данные о пользователях CRM-системы;

2) «contacts» – данные о контактах;

3) «companies» – данные о компаниях;

4) «leads» – данные о сделках;

5) «tasks» – данные о задачах по контактам, компаниям, сделкам, обеспечивает полиморфную связь с перечисленными сущностями;

6) «goals» – данные о планах продаж на период;

7) «events» – данные о всех действиях пользователей CRM-системы, обеспечивает полиморфную связь с различными сущностями;

8) «leads_statuses» – список статусов (этапов) сделок;

9) «groups» – список групп пользователей CRM-системы;

10) «roles» – список ролей пользователей CRM-системы с соответствующими правами.

В итоге основными направлениями разработанного web-приложения для совершенствования бизнес-процессов управления взаимоотношениями с клиентами стали: улучшение обслуживания клиентов путем сохранения информации о клиентах и истории взаимоотношений с ними, упрощение ведения сделок для менеджеров и исполнителей, анализа выполнения пользователями поставленных им или ими самими целей. Достижение этих достоинств разработанной CRM стало результатом выполнения следующих шагов:

— изучения и оценки возможностей современных CRM-систем;

— обзора стека технологий для разработки web-приложений и обоснованного выбора одного из них[1];

— проектирования общей архитектуры CRM-системы и схемы базы данных системы сопровождения продаж;

— разработки программных модулей, реализующих все необходимые в системе функции, и пользовательского интерфейса системы[2].

Библиографический список

1. *Гринберг П.* CRM со скоростью света: привлечение и удержание клиентов в реальном времени через Интернет / пер. с англ. В. Агапова. 3-е изд., испр. и доп. СПб.: Символ-Плюс, 2016. 530 с.

2. Информационные технологии: учебник / Ю.Ю. Громов, И.В. Дидрих, О.Г. Иванова и др. Тамбов: Изд-во ТГТУ, 2015. 260 с.

3. *Черкашин П. А*. Стратегия управления взаимоотношениями с клиентами (CRM). Готовы ли Вы к войне за клиента?: учеб. пособие. М.: ООО «ИНТУИТ.ру», 2004. 384 с.

А. С. Михайлова, Л. В. Кортенко
Уральский государственный экономический университет, г. Екатеринбург

Внедрение систем управления данными клиентов в медицинских организациях

Аннотация. Рассмотрена проблемы упорядочивания потоков информации внутри медицинской организации. Предложено решать задачи бизнес-процессов всех уровней предприятия медицинских услуг путем внедрения актуальной системы управления данными клиентов.

Ключевые слова: бизнес-процесс; информация; медицинские услуги; медицинские данные.

Все предприятия сервиса, оказывающие услуги физическим лицам или сотрудникам юридических лиц, нуждаются в сохранении данных постоянных, случайных и потенциальных клиентов в интересах развития своего бизнеса. И делают это разными способами: в excel, в электронной почте, в мессенджерах социальных сетей, в разрозненных программах,

[1] *Фреймворк*. URL: https://blog.skillfactory.ru/glossary/framework/ (дата обращения: 04.02.2022); Обзор лучших бэкенд фреймворков в 2022 году. URL: https://merehead.com/ru/blog/backend-development-trends-best-backend-frameworks-in-2022 (дата обращения: 04.02.2022).

[2] *ГОСТ 27.002-89.* Надежность в технике. Основные понятия. Термины и определения.

предназначенных для разных целей (подбор, бронирование, взаимодействие с поставщиками и т.п.), в лучшем случае в системах управления отношениями с клиентами (Customer Relationship Management, CRM). С другой стороны, предприятия сталкиваются с беспрецедентным усилением конкуренции за потребителей и потребности в качественных и используемых правильным образом технологиях присутствуют. Соответственно, на современных предприятиях России процесс управления данными клиентов чаще всего слабо проработан и многие предприятия теряют потенциальных и слабо мотивированных потребителей медицинских организаций по этой причине.

В последние годы наблюдается трансформация управления и перестраивания бизнес-процессов во всех областях деятельности под влиянием цифровых технологий, что интересно предприятиям, ориентированным на совершенствование и развитие, и находит соответствующий отклик в работах исследователей и разработчиков. Таким образом, новые технологии и социальные изменения в сочетании с феноменом глобализации меняют правила классического менеджмента.

Теоретическое обоснование применения информационных систем управления данными клиентов и выявление ключевых аспектов и целей этой практики крайне важно для развития соответствующих технологий. При правильном понимании и применении системы информационного обеспечения процесса управления данными клиентов, она становится важнейшим фактором достижения стратегических целей развития предприятия.

Проблемная ситуация исследования заключается в том, что информационное обеспечение деятельности медицинских организаций не соответствует поставленным текущим задачам повышения конкурентоспособности организации на рынке услуг. Происходящие в нашей стране радикальные трансформационные процессы выдвинули на первый план проблему развития клиентоориентированности, как одного из основных факторов конкурентоспособности.

Система управления медицинскими данными или медицинская информационная система (МИС) – «комплексный программный продукт, главным предназначением которого является автоматизация всех основных процессов, связанных с работой медицинских учреждений общей и узкой специализации. Автоматизированные медицинские информационные системы позволяют быстро и эффективно наладить электронный документооборот, гибко выстраивать работу с пациентами, вести оперативный учет работы административного персонала, контролировать все организационные и финансовые вопросы»[1].

[1] *Козлов А. Н.* Анализ проблемы информационной безопасности предприятий малого и среднего бизнеса. URL: http://pfo-perm.ru/Data2004/DConf04/Koz-lovAN.htm.

Рассмотрим классификацию медицинских информационных систем.

Ключевым звеном в информатизации здравоохранения является информационная система. Классификация медицинских информационных систем основана на иерархическом принципе и соответствует многоуровневой структуре здравоохранения. Различают[1]:

1) медицинские информационные системы базового уровня, основная цель которых – компьютерная поддержка работы врачей разных специальностей; они позволяют повысить качество профилактической и лабораторно-диагностической работы, особенно в условиях массового обслуживания при дефиците времени квалифицированных специалистов;

2) медицинские информационные системы уровня лечебно-профилактических учреждений;

3) медицинские информационные системы территориального уровня;

4) системы, предназначенные для информационной поддержки государственного уровня системы здравоохранения[2].

Проблемы и риски, которые решают МИС.

Использование информационных технологий в деятельности российских медицинских учреждений объективно необходимо для обеспечения доступности и качества медицинской помощи. Различным аспектам управления информацией в медицинской сфере посвящено множество публикаций[3]. Информационное взаимодействие медицинских учреждений с внешней информационной средой осуществляется с использованием различных каналов связи - системы технических средств и среды распространения сигналов для односторонней передачи данных (информации) от отправителя (источника) к получателю (приемнику). Канал связи является составной частью канала передачи данных[4].

Проблемы с информацией здравоохранения, которые решаются с помощью МИС:

— навыки и опыт в области медицинской информации (знания, инструменты, методы и фактическая база) фрагментарны и не всегда включаются в международную научную литературу;

---

[1] *Wallenius C.* Роль больших данных в достижении тройной цели системы здравоохранения. URL: https://www.sas.com/ru_ru/insights/articles/big-data/health-care-triple-aim.html.

[2] *Козлов А. Н.* Анализ проблемы информационной безопасности предприятий малого и среднего бизнеса. URL: http://pfo-perm.ru/Data2004/DConf04/Koz-lovAN.htm.

[3] *МИС* EMCImed – для комплексной автоматизации медучреждения. URL: https://emci.ua/ru/produkty/emcimed.

[4] *Медицинские* информационные системы: обзор возможностей и примеры использования // Evergreens. 2020. 17 февр. URL: https://evergreens.com.ua/ru/articles/medical-information-systems.html (дата обращения: 02.03.2022).

— поскольку данные все еще слишком редко собираются на основе общих определений индикаторов, значимый анализ и эффективное распространение собранной таким образом информации ограничены;

— между национальными системами информации и отчетности существует большое неравенство. В некоторых странах сбор данных носит фрагментарный и неполный характер, например, каждое медицинское учреждение собирает данные о пациенте, но эти данные остаются в пользовании только в данном учреждении;

— дублирование, избыточность информации;

— информатизация в здравоохранении часто осуществляется временно финансируемыми проектами, что препятствует эффективной передаче знаний и поддержанию устойчивости систем[1].

ПО мере того, как пациенты получают доступ ко все большему количеству медицинской информации, они проявляют активный интерес к вопросам выбора медицинских услуг. Пациенты стали активно оценивать услуги, пользуясь информацией из Интернета и других источников.

Это показывает, насколько важно использовать аналитические инструменты для корректировки рисков утери и недостаточности информации, чтобы предоставлять потребителям достоверную информацию для принятия обоснованных решений.

Становясь более осведомленными, пациенты не только формируют спрос на самые современные медицинские услуги, но и непреднамеренно систематизируют и предоставляют свои медицинские данные поставщикам медицинских услуг. Это способствует лучшему выполнению предписаний врачей, что очень важно при неблагоприятном развитии событий или выявлении проблем после выписки в условиях надлежащего ухода.

Практики систем здравоохранения в разных странах сильно различаются, но есть три задачи, актуальные для всех медицинских учреждений[2]:

1) улучшение методов и способов взаимодействия с пациентами (включая качество обслуживания пациентов и степень их удовлетворенности);

2) повышение показателей здоровья населения;

3) уменьшение затрат здравоохранения на душу населения.

---

[1] *Основные* понятия и термины медицинской информатики. URL: https://www.bsmu.by/downloads/kafedri/k_fiziki/2015-1/m2.pdf (дата обращения: 02.03.2022).

[2] *Медицинские* информационные системы: обзор возможностей и примеры использования // Evergreens. 2020. 17 февр. URL: https://evergreens.com.ua/ru/articles/medical-information-systems.html (дата обращения: 02.03.2022).

Основные задачи внедрения компьютерных систем:

— контроль финансовых затрат;

— лучшая организация труда;

— хорошее управление информационными потоками[1].

МИС должна обеспечивать, врачей и различные административные менеджеров и врачей возможностью хранить большой объем данных для архивирования, осуществлять поиск информации, иметь доступ к системам поддержки принятия решений, помогать медицинской диагностике, сопровождать принятие решений и др.[2]

Внедрение эффективной медицинской информационной системы позволит административному и экономическому персоналу:

— лучше понимать финансовые потребности (контроль бюджета);

— обеспечить контроль наличия медицинского, фельдшерского, административно-технического персонала и оборудования);

— обеспечить лучшее распределение ресурсов клиники с хорошим планированием обслуживания потребителей услуг;

— отслеживать и контролировать деятельность в реальном времени;

— предотвращать утечку фармацевтической и другой информации в личных целях ее пользователей.

Внедрение МИС позволит эффективным образом улучшить: методы, средства хранения, и обработку данных.

[1] *Плащевая Е. В.* Медицинские информационные системы: метод. указ. для самоподготовки студентов. Благовещенск: Амурская ГМА, 2019. 16 с.

[2] *Medesk* – МИС для частных медицинских центров. URL: https://www.medesk.net/ru.

В. Р. Науменко, С. В. Бегичева
Уральский государственный экономический университет, г. Екатеринбург

Разработка дашборда для анализа динамики цен на лекарственные препараты для лечения коронавирусной инфекции, гриппа и ОРВИ

Аннотация. Статья посвящена возможностям визуализации данных на примере BI-приложения для анализа изменения цен на лекарственные препараты для лечения коронавирусной инфекции, гриппа и ОРВИ.

Ключевые слова: бизнес-аналитика; BI-система; дашборд; лекарственные средства; коронавирусная инфекция.

В данных эпидемиологических и социально-экономических условиях повышается роль фармацевтического рынка. Пандемия коронавируса показала, что от обеспеченности фармацевтического сектора необходимыми лекарственными препаратами и их ценовой доступности для различных слоев населения могут зависеть жизни людей, в связи с чем вопросам развития отрасли сегодня уделяется большое внимание [1]. Для того, чтобы лекарственные препараты всегда были доступны, и не создавалось дефицита, необходимо грамотно делать закупки. Для этого нужно отслеживать и анализировать различные показатели, в том числе и динамику цен.

Используя BI-приложения с наглядным представлением и интерактивной аналитикой, можно проанализировать динамику показателей, посмотреть на эти данные «под другим углом», а также извлечь новые знания и улучшить показатели. Грамотно разработанная панель мониторинга – это эффективный бизнес-инструмент. В настоящее время это неотъемлемая часть инструментария любого аналитика, желающего добиться максимальной эффективности от себя и своей компании, а также отличный метод демонстрации важных показателей.

BI-системы или системы бизнес-аналитики (Business Intelligence) – это аналитические системы, которые объединяют данные из любых различных источников информации, обрабатывают их и предоставляют удобный интерфейс для всестороннего изучения и оценки полученных сведений [2]. Данные, полученные в результате такого анализа, помогают достигать поставленных бизнес-целей с помощью оптимального использования имеющихся данных. Комплексный анализ данных по всем направлениям бизнеса позволяет повысить его эффективность и снизить издержки.

Объем данных, с которыми приходится сталкиваться в сфере розничной торговли лекарственными препаратами, постоянно растет: поставки, поведение покупателей, тенденции, продажи по различным каналам и глобальный охват – вот лишь несколько категорий информации, обработка которой позволяет повысить эффективность бизнеса. Power BI – отличная BI-платформа, с помощью которой можно это реализовать.

Разрабатывать BI-приложение будем на данных несетевой аптеки Свердловской области. Аптека находится в Нижнем Тагиле, была основана в 2001 г. и 20 лет находится на рынке лекарственных средств.

На основании временных методических рекомендаций от Министерства здравоохранения Российской Федерации, а именно рекомендаций по лечению коронавирусной инфекции[1], был составлен перечень лекарств для лечения коронавирусной инфекции:

— Умифеновир;
— Ремдесивир;
— Фавипиравир;
— Интерферон-альфа.

Но так как цены на некоторые из этих препаратов достаточно высоки, чаще всего их заменяют дженериками. Дженерики – это лекарственные препараты, которые в своей основе имеет тоже количество и качество активного вещества, что и в оригинальном средстве. Поэтому для дальнейшего анализа были взяты данные по цене и количеству за 2018−2021 гг. следующих лекарственных препаратов:

— Гриппферон;
— Ксарелто;
— Арбидол;
— Триазавирин.
— Эликвис.

Так как в качестве единиц анализа могут рассматриваться позиции ассортимента, представляющие собой уникальное сочетание торгового наименования, формы выпуска и дозировки, то для определения средней цены по каждому торговому наименованию лекарственного препарата для построения BI-приложений была использована среднеарифметическая взвешенная цена.

Статистика заболевших коронавирусной инфекцией по Свердловской области была взята с сайта, основанном на данных, собранных

[1] *Временные* методические рекомендации. Профилактика, диагностика и лечение новой коронавирусной инфекции (COVID-19). URL: https://static-0.rosminzdrav.ru/system/attachments/attaches/000/049/629/original/Временные_MP_COVID-19_03.03.2020_%28версия_3%29_6-6.pdf?1583255386.

Центром системных наук и инженерии Университета Джона Хопкинса[1]. Данные по заболеваемости ОРВИ и гриппом взяты с сайта Научно-исследовательского института гриппа А.А. Смородинцева[2].

В результате получилось несколько информационных панелей.

На первом дашборде «Динамика заболеваемости» можно увидеть сравнение количества заболевших коронавирусной инфекцией и гриппом/ОРВИ (рис. 1).

Рис. 1. Динамика заболеваемости

Цель второго BI-приложения – анализ цены и количества по выбранному наименованию лекарственного препарата и временному промежутку (рис. 2).

На следующем дашборде можно выявить зависимость цен на лекарственные препараты от количества заболевших коронавирусом (рис. 3).

[1] *Coronavirus* in Sverdlovsk Oblast. URL: https://covid.observer/ru/66.

[2] *Еженедельный* национальный бюллетень по гриппу и ОРВИ. URL: https://www.influenza.spb.ru/system/epidemic_situation/laboratory_diagnostics.

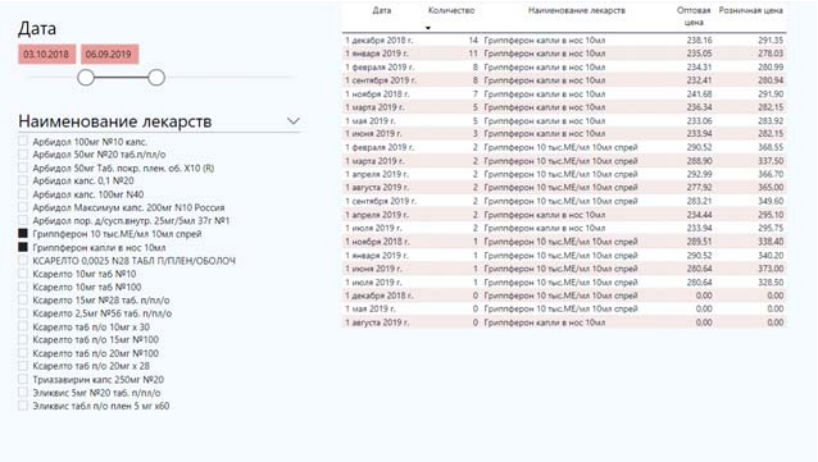


Рис. 2. Лекарственные препараты

Рис. 3. Средневзвешенные цены

На приведенном дашборде можно увидеть, что средневзвешенные цены начинают повышаться после января 2020 г., что совпадает с началом пандемии коронавируса. Можно сделать вывод о том, что с ростом количества заболевших растут и цены на данные лекарственные препараты.

Данная работа имеет практическую ценность, так как представленные информационные панели демонстрируют данные доступными и наглядными средствами. Они интуитивно понятны, формируют понимание ситуации на рынке лекарственных средств, помогая формированию выводов и тем самым побуждая к изучению имеющихся данных и выявлению проблем. Все это помогает грамотно осуществлять закупки лекарственных средств. Исследуя данные показатели, можно повысить количество продаж и в конечном итоге максимизировать прибыль организации.

Библиографический список

1. *Курилова О. О.* Анализ состояния фармацевтического рынка Российской Федерации // Региональный вестник. 2021. № 1 (57). С. 57–58.

2. Современные информационные технологии в бизнесе. Тема V. Аналитическая обработка данных. Обзор BI-систем. М.: Высшая школа экономики, 2016. URL: https://inlnk.ru/YAZjLa.

С. М. Озорнина
Уральский государственный экономический университет, г. Екатеринбург

Цифровые решения в бизнес-моделировании

Аннотация. Статья посвящена вопросам бизнес-моделирования, изучению программных продуктов для разработки и внедрения бизнес-модели в работу компаний.

Ключевые слова: бизнес-моделирование; цифровизация; планирование; импортозамещение; интернет.

Для развития и роста предприятия на определенном этапе руководитель должен позаботиться об усовершенствовании и повышении эффективности производства, улучшать качество обслуживания, принимать решения и выискивать пути снижения потерь. Основной фактор успешной работы компании – построение четкой стратегии работы.

Управление современным предприятием в рыночной экономике это сложный процесс, чтобы организовать работу компании необходимо выстроить подробную бизнес-модель, в которой изучить рынок, возможных клиентов, конкурентов, плюсы и минусы и разработать стратегию продвижения. И обеспечить взаимосвязи на всех уровнях организации.

Впервые, понятие бизнес-модели дал Пол Тиммерс в конце 90-х гг. и трактовал как чистую бизнес-концепцию, объясняющую логику ведения бизнеса фирмы в форме электронной коммерции. Он это связывал с появлением нового средства массовой информации – Интернета.

И в это время появились новые способы ведения бизнеса – в облачном пространстве (например, электронные закупки и т.д.).

Понятие бизнес-модели разные авторы трактовали по-разному, некоторые из них представлены в таблице.

Понятие бизнес-модели

Исследователь	Определение
П. Тиммерс	Бизнес-модель – это совокупность услуг, продуктов, потоков информации, а также описания разных участников бизнес-процесса, их роли в цепях создания стоимости, потенциальных выгод с описанием источников получения дохода [2]
И. Пинье и А. Остервальдер	Бизнес-модель – концептуальная модель бизнеса, иллюстрирующая процессы создания, транспортировки и реализации ценности и логику создания добавленной стоимости [2]
М. Джонсон	Бизнес-модель - «Захват чистого пространства», состоящая из таких элементов, как ключевые ресурсы и основные бизнес-процессы предприятия, ценностные предложения для потребителей, формула получения прибыли [1]
Д. Абелл	Бизнес-модель – область бизнеса, которая решает три главных взаимосвязанных между собой вопроса: - Кто является потребителем? - Какие товары и услуги можем предложить бизнесу? - Как мне это сделать эффективно?

В связи с событиями на Украине и санкциями западных стран ситуация на данный момент такова, что экономика в России претерпевает оперативное снижение по многим направлениям. И никто из российских бизнесменов не застрахован ни от убытков, ни от банкротства.

Тем не менее, предпринимательский менталитет нацелен искать даже в самой негативной финансовой ситуации не только безболезненный выход, но и новые возможности.

В связи с тем, что из Российской Федерации уходят крупные зарубежные бренды у российских предпринимателей и корпорацийпоявляется возможность заполнить освободившиеся ниши и удовлетворить потребности клиентов.

Так как никто не знает, чего стоит ждать в сложившейся ситуации при поиске своей ниши для получения дохода, в первую очередь стоит ориентироваться на потребителя и на состояние рынка. Компаниям можно направить свою деятельность в русло импортозамещения, тем самым заполнить рынок отечественными товарами и услугами, предварительно проанализировав возможных конкурентов, потребителей, партнеров, рассчитать планируемые доходы, затраты.

На сегодняшний момент это можно сделать при помощи различных программ и приложений. На российском рынке представлены следующие отечественные программы:

— *Бизнес-инженер (БИТЕК)* – инструмент для планирования деятельности предприятия и подготовки регламентированных форм документов. Эта система дает возможность подготовить бизнес-модель, а также сформировать на ее основе отчеты и документацию по различным направлениям: бизнес-процессы, методика развития, персонал, финансы и многое другое. Она дает возможность сформировать данные в виде таблиц, диаграмм, справочников, схем, матриц. Система позволяет работать с программными продуктами Microsoft Office, в частности, с графическим редактором Microsoft Visio.

— *Корпоративный навигатор (ИНТАЛЕВ)* – дает возможность развития системы управления предприятием. Эта система является платформой и набором уже готовых комплексов решений управленческих задач, то есть управленческих схем. Поддерживает изложение данных готовой бизнес-модели в таких форматах, как: справочники, диаграммы. На основе полученных данных средствами системы ИНТАЛЕВ есть возможность разработать отчеты, которые в последующем могут быть изложены в форме документа Word или в html-документы и использоваться как корпоративные регламенты. При помощи веб-модуля можно предоставить доступ к полученным бизнес-моделям определенному кругу пользователей, тем самым модель системы будет использована как корпоративный веб-портал с обновлением в режиме реального времени.

— *ОРГ-Мастер Про (Бизнес Инжиниринг Групп)* – нацелен на решение широкого круга задач по бизнес-моделированию. Дает возможность разрабатывать систему бизнес-процессов, кадровую, финансовую, информационную, организационную и прочие структуры. Данные могут быть получены в виде диаграмм и справочников. По каждой диаграмме может быть рассчитано среднее время выполнения каждого процесса. Данные, разработанные в модели, могут быть представлены в форме отчета. Все отчеты можно экспортировать в Word, Excel, html и текстовые файлы.

Следует заметить, что российские программы в первую очередь ориентированы на описание и проектирование деятельности предприятия. Они дают возможность описать каждую область деятельности.

Зарубежные разработчики напротив в первую очередь нацелены на исполнение. Их системы являются модулями в линейке программного продукта, предоставляемого производителем.

Самыми популярными зарубежными программами являются:

— *ARIS* – комплексная платформа для управления цифровой трансформацией бизнеса;

— *CA ERWin Process Modeler* – средство моделирование бизнес-процессов, предназначенное для разрешения многочисленных проблем, возникающих в сфере электронного бизнеса[1];

— *Hyperion Performance Scorecard* – система, которая дает возможность повысить качество управления за счет объединения новых бизнес-процессов с текущими;

— *IBM WebSphere Business* Modeler – платформа для создания бизнес-модели, их анализа и документирования.

Успех компаний на начальном этапе развития бизнеса зависит от разработки и внедрения новых технологий в планирование, производство и управление организацией.

В сфере менеджмента данная идея проявляется в разных формах организации бизнес-процессов, например, в бизнес-моделях.

Перед разработкой бизнес-модели компании формируют определенный бюджет и человеческие ресурсы для ее реализации. Желаемым результатом разработанного проекта служит превышение прибыли над издержками, именно для этой цели и разрабатывается бизнес-модель.

Библиографический список

1. *Галенко Е. В., Овчаренко Н. П.* Бизнес-модель для предприятий гостиничной индустрии, ориентированной на ценностные предложения для потребителей // Известия Дальневосточного федерального университета. Экономика и управление. 2017. № 2(82). С. 39−50. DOI: 10.5281/zenodo.818140.

2. *Филин С. А., Большакова К. В., Холопцева К. А.* Бизнес-модель как ключевой фактор коммерческого успеха // Экономика и управление: проблемы, решения. 2021. Т. 3, № 10(118). С. 97−105. DOI 10.36871/ek.up.p.r.2021.10.03.010.

[1] *CA ERwin* Process Modeler // Архитект Дизайн. URL: https://www.architect-design.ru/item.1011.html.

Д. Л. Осокин, М. А. Панов
Уральский государственный экономический университет, г. Екатеринбург

Обзор мирового и российского рынка электронного обучения

Аннотация. В статье рассматривается сегмент онлайн-обучения на мировом и российском рынках. Систематизированы достоинства и недостатки онлайн-обучения, названы перспективы развития рынка электронного обучения.
Ключевые слова: электронное обучение; LMS-система; повышение квалификации.

На сегодняшний день качественное корпоративное обучение востребовано как никогда: согласно опросу, проведенному LinkedIn, 94 % сотрудников заявили, что они согласились бы остаться в компании дольше, если бы компания инвестировала в их развитие[1]. Дополнением к этой статистике является тот факт, что 90 % руководства также считает, что инвестирование в развитие карьеры своих сотрудников является крайне важным условием роста компании [1].

Пользователей e-learning сегмента делят на образовательный сектор, сектор корпоративного обучения и индивидуальных пользователей.

Образовательный сектор представляет из себя частные компании, занимающиеся предоставлением обучающих услуг, и государственные образовательные учреждения.

Среди корпоративного сектора выделяются компании, у которых есть потребность на постоянной основе обучать своих сотрудников. В особенности, если у компании много филиалов. Примеры крупных российских компаний, применяющих онлайн-обучение – «Газпром», «Сбербанк», «МТС», «Татнефть» и т.д. [2].

Индивидуальные пользователи обращаются к сайтам, которые создают собственные лекционные материалы (в видео, аудио или текстовом формате), а также практические занятия. При этом, направления обучения могут быть разными в зависимости от сервиса. В качестве примеров таких сайтов можно привести openlearning, intuit, coursera.

Среди основных целей программ обучений в корпоративном и частном секторе можно выделить:

— передача опыта новым сотрудникам о текущих бизнес-процессах компании;

— развитие специфичных навыков;

— изучение программных продуктов, актуальных для компании;

[1] *Linkedin* learning workplace learning report 2018. URL: https://learning.linkedin.com/content/dam/me/learning/en-us/pdfs/linkedin-learning-workplace-learning-report-2018.pdf.

— ознакомление со стандартами компании, а также с нормативными актами и правилами распорядка.

Электронное обучение может затрагивать широкий спектр отраслевых сегментов.

В секторе корпоративного обучения (согласно статистике Skillsoft)[1] разделение по отраслям следующее:

— информационные технологии – 22 %;

— управление персоналом – 16 %;

— клиентское обслуживание – 14 %;

— бухгалтерия/финансы и маркетинг/продажи – по 9 %;

— инженерные знания – 3 %;

— другие отрасли – 27 %.

E-learning также применим ко многим специальностям в государственном секторе (иногда с разграничением времени очного и онлайн формата).

Наиболее важными плюсами электронного обучения являются:

— уменьшение временных затрат. Как преподавателю, так и студенту не нужно добираться до аудитории. Дистанционное образование сокращает время обучения на 37−46 % (согласно статистике Cedar Group)[2];

— уменьшение затрат. Нет необходимости оплачивать проезд, место проживания, аренду помещения и расходы преподавателя. Стоимость онлайн обучения оценивается меньше стоимости очной на 31−43 % (согласно статистике Cedar Group);

— студент может изучать курс в удобное ему время. Отсутствие зависимости от преподавателя;

— каждый студент проходит изучение курса в своем индивидуальном темпе;

— согласно исследованиям, временные затраты на запоминание материала на 17−24 % выше аналогичных показателей очной формы[3];

— наполнение курса удобно актуализировать, непосредственный процесс обучения более прозрачен, наличие статистических данных и количество просмотров материала не имеет ограничений.

В основном, на глобальном рынке электронного образования лидируют компании из США, а также Европы (70 % всех систем). Самая популярная информационная система – Blackboar (она имеет закрытый

[1] *Research*: Globe for Corporate Learning, 2021. URL: https://www.skillsoft.com/resources/aragon-research-globe-for-corporate-learning.

[2] *Rich* Data Exploration at Cloud Scale. URL: https://raweb.inria.fr/rapportsactivite/RA2020/cedar/index.html.

[3] Там же.

программный код), а также Sakai и Moodle (имеют открытый программный код). Согласно статистике Zacker, из двухсот лучших мировых университетов (согласно данным The World University Rankings)[1] на текущий момент более 65 % из них пользуются продукцией Blackboard.

Отечественный рынок в данный момент включает в себя более 35 компаний, которые предоставляют продукты для дистанционного обучения (по версии smart-edu). Эти компании разрабатывают как комплексные LMS (система управления обучением) системы, так и виртуальные класса и редакторы создания курсов. Направление программного обеспечения для разработки, изменения и управления онлайн курсами меньше всего развито.

Среди российских компаний в сегменте онлайн обучения можно отметить следующие: Competentum, WebSoft, Новый Диск, Прометей Redlab, Гиперметод. Самые крупные из них, представленные на рынке – Websoft, Competentum и Гиперметод [3].

Среди основных направлений развития мирового рынка онлайн обучения можно выделить:

— применение социальных сетей для образования;

— применение SAAS решений;

— применение обучения на мобильных устройствах.

Данные пункты уже давно присутствуют в информационном поле, но тем не менее, в настоящее время потенциал этих направлений начинает раскрываться в создаваемых программных продуктах. К примеру, социальные сети уже несколько лет применяются для обучения, но только недавно до крупных компаний, занимающихся разработкой онлайн платформ для образования, пришло осознание того, что для многих людей социальные сети стали неотъемлемой частью жизни. В течение следующих нескольких лет ожидается рост количества приложений для обучения с применением социальных сетей [4].

Среди основных направлений развития российского рынка онлайн обучения также можно выделить:

— обучение на мобильных устройствах;

— интеграции с социальными сетями;

— применение SAAS решений.

С каждым годом развитие рынка мобильных устройств приносит что-то новое в индустрию онлайн обучения, тем самым развивая сегмент обучения на мобильны устройствах. На текущий момент большинство контента онлайн платформ можно изучить любом на мобильном

[1] *QS* Stars: Online Learning. URL: https://www.topuniversities.com/qs-stars/qs-stars/qs-stars-online-learning.

устройстве. Курсы, которые можно проходить на мобильных устройствах, требуют специфичного подхода к разработке. Не каждое программное обеспечение будет работать на всех устройствах одновременно. Данное направление развивается. В настоящий момент в России насчитывается примерно 85 млн пользователей мобильного интернета (по версии РАЭК)[1], основной возраст находится в рамках 16–22 лет. Также уже на рынке начинают появляться приложения, интегрированные с социальными сетями. Это объясняется широкой интеграцией людей молодого и старшего поколения с социальными сетями.

Так как рынок развивается, дистанционное обучение будет пользоваться спросом как в государственном, так и в корпоративном секторе. На текущий момент, внедрение дистанционного обучения – актуальная тема для многих российских учебных заведений. Можно сделать вывод о том, что данный рынок и дальше будет увеличивать количество потребителей, постепенно уменьшая долю очного формата обучения во всех секторах.

Библиографический список

1. *Андреева Л. Г., Бурукина О. А., Воробьева И. А., Денисов А. Р., Маркова В. А., Новикова В. П., Степанова М. М.* Онлайн-платформа для формирования компетенций в корпоративных системах обучения // Образование и наука. 2016. № 1. С. 76–94.

2. *Долженко Р. А.* Корпоративное обучение персонала в коммерческом банке // Кадровик. 2012. № 1. С. 79–83.

3. *Тебекин А. В.* Стратегическое управление персоналом: учебник. М.: КноРус, 2020. 720 с.

4. *Хахмович А. И.* Мотивация к обучению: как эффективно применить корпоративную СДО // Управление человеческим потенциалом. 2012. № 2. С. 130–143.

[1] *Итоги* Российского интернет форума 2021. URL: https://2021.rif.ru/news/itogi-rossijskogo-internet-foruma-2021.

Г. И. Попова, М. И. Петин
НИУ «Высшая школа экономики», г. Москва

Влияние нефинансовых факторов на стоимость FinTech стартапов

Аннотация. Рассматривается влияние нефинансовых показателей на оценку стоимости FinTech стартапов в развитых странах. Обсуждается развитие современной экономики в условиях цифровизации и растущий интерес инвесторов к венчурным вложениям. FinTech стартапы анализируются как часть активно развивающейся цифровой экономики, которая стремится улучшить финансовую деятельность через внедрение цифровых технологий. Сделаны выводы о значимых детерминантах стоимости FinTech стартапов.

Ключевые слова: Fintech; стартап; венчурный капитал; цифровые финансы; оценка стоимости; цифровые технологии.

В современном стремительно растущем, нестабильном и технологичном мире традиционный бизнес должен быть гибким и готовым к инновационным решениям, таким как введение цифровых технологий. Более того, с увеличением масштабов использования цифровых данных и перехода на электронный документооборот, все чаще обсуждается вопрос информационной безопасности и защиты данных. Исключением не стала и финансовая отрасль, в которую активно внедряются современные цифровые технологии. Таким образом, FinTech можно рассматривать как абсолютно новую финансовую отрасль, целью которой является модернизация финансовой деятельности через применение различного рода новых цифровых технологий и разработок [1; 2].

Наше исследование будет направлено на изучение роли разных нефинансовых факторов в оценке FinTech стартапов.

Гипотезы. Венчурное инвестирование является одним из самых высоко рисковых финансовых инструментов, поэтому венчурные инвесторы серьезно подходят к выбору развивающихся бизнесов. Часто, они опираются не только на объективные показатели бизнеса, например, такие как рентабельность и прогноз роста выручки, но и на ряд субъективных факторов, таких как медийность компании, опыт, возраст и уровень образования CEO.

Для выявления зависимости и уровня влияния выбранных факторов на оценку FinTech стартапов, мы будем исследовать группы гипотез на компаниях из развитых стран.

Поскольку часто высокий уровень образования менеджмента, а именно, CEO, позволяет достичь определенных знаний в понимании устройства рынка и навыков в управлении, то:

H1. FinTech стартап в развитых странах более привлекателен для венчурных инвесторов если у его CEO есть степень PhD или MBA.

В венчурных инвестициях важно на ранних этапах находить баланс между интересами инвестора и потребностями компании, чтобы избежать неприятных конфликтов и споров в будущем. Поэтому можно сделать вывод, что найти общий язык с одним человеком в руководстве компании сложнее, чем провести переговоры с несколькими людьми с разными мнениями и прийти к консенсусу. Тогда,

H2. FinTech стартап с несколькими фаундерами более привлекателен для венчурных инвесторов.

В эпоху цифровых технологий и популярности телекоммуникаций компания с потенциалом на медийность сможет скорее завоевать рынок и поднять выручку. Поэтому,

H3. Медийные FinTech стартапы более привлекательны для венчурных инвесторов.

Если руководство уже имело опыт в настройке и достижении целей бизнеса и знает, как развивать бизнес, то инвесторов с большей вероятностью заинтересуют вложения именно в такую компанию. Тогда,

H4. Чем выше опыт менеджмента FinTech стартапа, тем он более привлекателен для венчурных инвесторов.

Методология. В целях исследования мы используем модель, оцененную методом наименьших квадратов (МНК) для анализа того, какие факторы являются значимыми при инвестировании в FinTech-предприятия.

Первичные данные, использованные в настоящем исследовании, были собраны на CrunchBase, ведущей платформе, предоставляющей информацию о стартапах. Также в рамках исследования были использованы данные с портала LinkedIn для сбора информации о CEO: опыт работы, наличие степеней PhD и MBA.

Мы собрали данные о 395 компаниях из Северной Америки, Европы и Азии. После исключения выбросов в выборке осталось 372 компаний. В нашу выборку попали компании со следующими признаками: компания является прибыльной; компания разрабатывает продукт, связанный с FinTech-индустрией; компания основана не позднее 2018 г.; компания хотя бы раз привлекала венчурные инвестиции.

В качестве зависимой переменной было решено взять натуральной логарифм суммы привлеченных инвестиций (ln_funding). В качестве объясняющих были выбраны следующие переменные:

1) натуральный логарифм от выручки компании (по данным CrunchBase) – финансовый фактор, который призван учитывать масштабы деятельности компании (ln_sales);

2) дамми-переменные для обозначения индустрии, в которой оперирует FinTech-компания: криптовалюта и блокчейн (crypto), банки (banking), электронная коммерция (e-commerce), платежные сервисы (payments), бухгалтерский учет (accounting);

3) количество основателей компании (num_founders), количество взятых раундов инвестиций (num_rounds), количество работников (employees);

4) медийность компании – учитывается через количество упоминаний компании в СМИ (num_articles);

5) дуализм CEO – 1, если CEO является основателем компании, 0 – иначе (ceo_duality), и опыт работы CEO в годах (ceo_exp);

6) дамми переменные для обозначения наличия у CEO образования или квалификации: MBA (ceo_mba), PhD (ceo_phd), магистерское образование (ceo_master);

7) количество патентов у компании (patents) и зарегистрированных торговых марок (trademarks).

Основываясь на описательной статистике (рис. 1), мы можем сказать, что средний FinTech-стартап имеет двух основателей, привлекал три раунда инвестиций с общем суммой привлеченных инвестиций 45,51 млн долларов и имеет в среднем 0,07 патентов, 0,5 торговых марок и 11,7 упоминаний в средствах массовой информации.

Variable	Obs	Mean	Std. dev.	Min	Max
funding	372	45.51755	125.6897	.09	1551.589
sales	372	46.45699	301.6984	5.5	5500
num_founders	372	2.405914	1.29034	0	10
employees	372	55.19355	97.54753	6	751
num_articles	372	11.69624	27.59207	0	449
patents	372	.0698925	.367782	0	3
trademarks	372	.5134409	1.338758	0	12
num_rounds	372	3.005376	1.884816	1	12
ceo_duality	372	.8978495	.303254	0	1
ceo_phd	372	.1370968	.3444127	0	1
ceo_mba	372	.1612903	.3682939	0	1
ceo_exp	372	8.149771	4.137706	2.047536	23.58595
ceo_master	372	.3252688	.4691061	0	1
crypto	372	.1317204	.338642	0	1
banking	372	.1263441	.3326842	0	1
ecommerce	372	.0241935	.1538566	0	1
payments	372	.1155914	.3201649	0	1
accounting	372	.0134409	.115308	0	1

Рис. 1. Описательная статистика

В нашей выборке 32,5 % всех CEO имеют степень магистра, при этом 13,7 % CEO получили степень PhD, а 16,1 % закончили программы MBA. Если говорить об индустриальном разрезе, то большинство компаний из нашей выборке оперируют в области криптовалют, банковского дела и платежных сервисов – 13,2; 12,6 и 11,6 %, соответственно.

Примечательно, что в нашей выборке средние значения по переменным funding и sales составляют 45,5 и 46,5 млн долл., при этом стандартное отклонение для этих двух переменных составляет 125,7 и 301,7, соответственно. Вызвано это большим количеством некрупных компаний с выручкой и привлеченными инвестициями в размере менее 10 млн долл. и крупных компаний, выручка и инвестиции которых превышают 1 млрд долл.

Результаты исследования. После тестирования нескольких моделей, была определена окончательная модель OLS, которая представлена далее:

ln_funding = -0.56 + 0.21ln_sales + 0.14num_founders + 0.01employees + 0.14trademarks + 0.27num_rounds + 0.07ceo_exp + 0.45banking

Из рис. 2 видно, что помимо указанной выше модели, также были протестированы модели со всеми упомянутыми ранее переменными, а также различные комбинации переменных. По информационным критериям AIC и BIC модель 2 оказалась самого высокого качества.

Variable	model1	model2	model3	model4
ln_sales	.20586019**	.20686365***	.20742657***	.19716845**
num_founders	.14092166**	.14121076**	.14246949**	.13725706**
employees	.00687987***	.00681402***	.00687673***	.0068443***
num_articles	.00195165			.00216732
patents	.32451559			.33372578
trademarks	.13250267**	.14306164**	.14202248**	.13627773**
num_rounds	.26563857***	.26922536***	.2700036***	.26829988***
ceo_duality	-.03441811			-.0062922
ceo_phd	.1755193			.15079987
ceo_mba	.03786897			.01932432
ceo_exp	.06345994***	.06657982***	.0671261***	.0667707***
ceo_master	-.17875507			-.16863185
crypto	.03980163		.06814271	
banking	.4608432*	.45075351*	.45303633*	
ecommerce	-.4230554		-.42786154	
payments	.06166544		.03701605	
accounting	-.11107112		-.00706194	
_cons	-.50973324	-.56205945*	-.57913096*	-.48337923
N	372	372	372	372
r2	.32903523	.32061394	.32194644	.32181682
r2_a	.29681376	.30754882	.30122813	.29914775
aic	1445.1516	1429.7915	1437.0612	1439.1323
bic	1515.6917	1461.1426	1484.0879	1490.0779

Legend: * p<.1; ** p<.05; *** p<.01

Рис. 2. Оцененные модели

Дополнительно мы провели тест на мультиколлинеарность, используя VIF-test. Средний VIF составил 1,05, что означает отсутствие мультиколлинеарности в модели. Также мы протестировали модель на гетероскедастичность и получили значение p-value больше 0,05. Таким образом, мы не отклоняем гипотезу о гомоскедастичности.

На основе построенной модели, мы можем сказать, что значимыми детерминантами инвестиций являются выручка, количество фаундеров, количество работников, торговые марки, число раундов инвестиций, опыт CEO и работа компании в банковской отрасли.

Выводы

По итогам проведенного исследования была построена модель, в которой рассмотрены ключевые детерминанты, влияющие на оценку FinTech-стартапов. В ходе исследования были подтверждены гипотезы о том, что объем привлеченного финансирования зависит от количества фаундеров и от личных характеристик CEO, в частности от его профессионального опыта. При этом в нашей выборке было выявлено, что медийность компании не является значимым фактором при предоставлении финансирования. Вероятно, такой результат был получен из-за того, что в выборку были включены компании различных бизнес-моделей.

Библиографический список

1. *Никонов А. А., Стельмашонок Е. В.* Анализ внедрения современных цифровых технологий в финансовой сфере // Научно-технические ведомости СПбГПУ. Экономические науки. 2018. Т. 11, № 4. С. 111–119. DOI: 10.18721/JE.11408.

2. *Dhochak M., Doliya P.* Valuation of a Startup: Moving Towards Strategic Approaches // Journal of Multi-Criteria Decision Analysis. 2020. Vol. 27, issue 1–2. P. 39–49. DOI: 10.1002/mcda.1703.

А. А. Турышев
Уральский государственный экономический университет, г. Екатеринбург

Создание программного продукта для автоматизированного мониторинга и поиска в режиме реального времени информации о сбоях в сервисах финансовых организаций

Аннотация. Предлагается описание программного продукта, отслеживающего доступность сервисов сайта банка. Предложенный в статье автоматизированный сервис служит для обработки и анализа веб-сайтов и определяет недоступности и ошибки ресурсов в реальном времени.

Ключевые слова: интернет-ресурс; сайт; доступность; банк; программный продукт.

Мы живем в мире информационных технологий (далее – ИТ) и с каждым годом сервисы для работы в сети-интернет увеличиваются вместе с пользователями данных ресурсов [1]. Посредством увеличения пользователей интернет-сервисов возникает проблема в увеличении интернет-трафика, который генерируют пользователи в результате своей интернет-деятельности. В результате огромных нагрузок на серверах финансовых организаций (далее – ФО), возникают технические сбои, которые влекут за собой финансовые потери. Чтобы избежать финансовые потери ФО предлагается разработка автоматизированного сервиса для обработки и анализа веб-сайтов для определения недоступности и ошибок ресурсов в реальном времени.

Цель работы – провести подбор возможных инструментов и средств о наличии сбоя у финансовых организаций и разработать программный продукт, для автоматизированного мониторинга и поиска в режиме реального времени информации о сбоях в приложениях и сервисах финансовых организаций.

Для разработки программного продукта был использован язык программирования Python и фреймворк PyQt5 для создания кроссплатформенных приложений.

1. Методы для определения недоступности интернет-ресурсов

Недоступные интернет-ресурсы – это ресурсы при запросе, к которым был получен ответ с информацией о некорректной работе или ответ не получен вовсе.

Существуют различные запросы (см. таблицу) для определения недоступности интернет-ресурсов.

Наиболее часто употребляемые запросы

Запрос	Описание
HEAD	Проверяет существование ресурса, служит для извлечения метаданных
GET	Идемпотентный запрос, получающий общие данные о ресурсе [3]
POST	Применяется для передачи пользовательских данных ресурсу

Информация о некорректности работы будет получена по средствам комплексной обработки ответа от интернет-ресурса.

В ходе разработке программы были задействованы три типа методов для выявления недоступности интернет-ресурса:

— программно-аппаратный;

— интеллектуальный;

— поведенческого надзора[1].

Для успешной реализации программно-аппаратного типа был задействованы следующие методы:

а) Status code (Код состояния).

Технически status code часть ответа на запрос пользователя. Он приходит, когда мы переходим по определенной ссылке или обращаемся к URL[2]. При обработке пользовательского запроса сервер самостоятельно формирует и отдает трехзначный цифровой код (рис. 1), который свидетельствует о состоянии ресурса;

Рис. 1. http(s) статус коды

[1] *Банк России*. Поведенческий надзор. URL: https://cbr.ru/protection_rights/behavioral_surveillance.

[2] *Ivb.unact.* URL (Uniform Resource Locator) / Waybackmachine. URL: https://web.archive.org/web/20060511175638/http://ivb.unact.ru/glossary/url.html.

б) Ping (Пинг).

Ping – утилита командной строки для проверки сетевых соединений в TCP/IP. Команда ping с помощью отправки фиксированный по размеру сообщений с эхо-запросом по протоколу ICMP проверяет соединение и замеряет время двусторонней связи на уровне протокола IP с другим компьютером (сервером), поддерживающим TCP/IP [1];

в) Page loading (Время загрузки страницы).

Метод, замеряющий время полной загрузки страницы, по своей сути схож с ping-ом, исключаю только то, что ping не может измеряться для репозиториев сайта и то, что пинг измеряет время двусторонней связи определенного малого количества информации (байт);

г) Bytes (Количество байт).

Технически bytes часть ответа, присылаемая пользователю под заголовком Content-Length (Длина содержимого). В котором получателю приходит размер тела объекта в октетах. Тут следует пояснить, что октеты в отличии от байтов это только 8 бит информации, когда в широком понимании байт может быть и 10, 12 и т.п. битами, но в данном случаи для удобства русскоговорящих читателей данный метод назван «Bytes».

Для успешной реализации интеллектуального типа был задействованы следующие методы:

а) Type ping (Тип пинга).

Оценочное суждения значения ping-а, заданное в условиях программы;

б) Speed (Скорость).

Относительная скорость погрузки страницы (формула 1), которая рассчитывается из разности размера тела объекта на время его загрузки.

$$Speed = \frac{Bytes}{Page\ loading}$$

Для успешной реализации типа поведенческого надзора был задействован метод Checking by reviews (проверка по отзывам). Данный метод предназначается для поиска негативных отзывов о не работающем сайте с ресурса для обратной связи.

2. Описание разработанного программного продукта для определения недоступности интернет-ресурсов

Разработанный программный продукт предназначен по принципу ООП, где каждое окно является классом для проверки сайтов на их доступность [2].

После запуска программы открывается окно главного экрана (рис. 2).

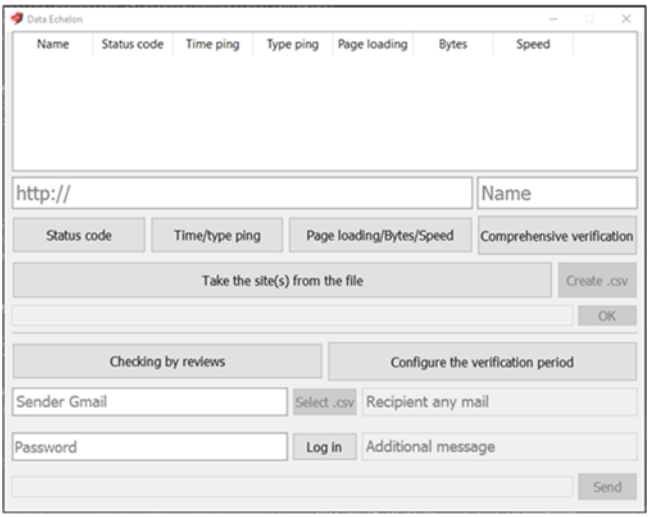


Рис. 2. Главный экран разработанного программного продукта

После чего у пользователя появляются два сценария работы программы или ручной, или автоматизированный. При этом сохраняется возможность работы в двух режимах одновременно, поскольку функции программы написаны для многопоточных задач. Сама программа будет работать пока ее главное окно не будет закрыто.

2.1. Ручной сбор данных

Начнем со сценария, рассчитанного для ручного сбора данных, основные функции которого представлены в верхней части главного экрана (см. рис. 2).

Нажимая на кнопки с соответствующим названием метода(-ов), предварительно введя URL и название, в таблице по центру экрана сверху будут отображаться данные, собранные с ресурса. Также, можно предварительно подгрузить CSV файл с URL и названием банков для, более быстрой проверки.

После работы в ручном режиме, можно сохранить всю информацию из таблицы в CSV файл, нажав на соответствующую кнопку.

Также внизу главного экрана присутствует возможность отправки сохраненного файла по почте С дополнительным сообщением, но при этом необходимо авторизоваться Gmail, так как именно данный сервис

предоставляет возможность отправки электронных писем по средствам сторонних программ.

Использование почтового клиента внутри приложения может снизить риск утечек информации компании-эксплорера.

2.2. Автоматизированный сбор данных

Также, в приложении реализованы функции для работы в автоматизированном процессе. Одна из таких функций – это настройка периода проверки, у которой есть собственное окно (рис. 3) всплывающее при нажатии определенной кнопки на главном экране.

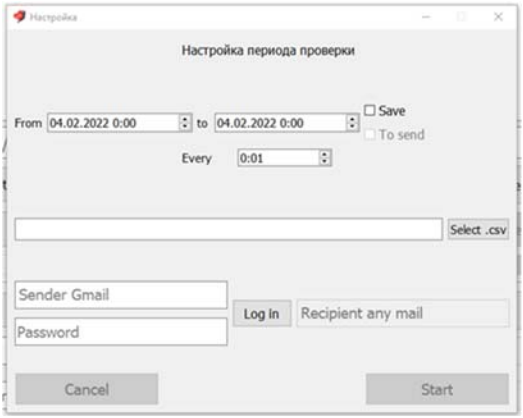


Рис. 3. Окно настройки периода проверки сайтов

Обязательны условием для работы в данном окне это выбор файла откуда будут браться ссылки и название банков. Также, необходимо указать корректный период проверки, иначе появится выплывающее окно (рис. 4), и указать через какой промежуток времени она должна происходить.

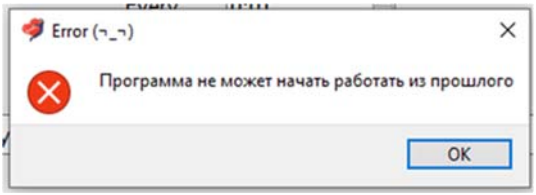


Рис. 4. Всплывающее окно при неверно указанных промежутках проверки

При желании пользователя, по завершению каждого цикла проверки есть возможность не только сохранять CSV файл с данными, но и отсылаться его на указанную почту, условия корректного заполнения полей для отправки электронных писем точно такие же как на главном экране.

Поскольку, программа является многопоточной, то программных сбоев в работе программы нет. Так как, в данном окне первый поток выполняет роль отрисовщика окна, второй поток выполняет основный цикл сбора, сохранения и передачи информации, а третий поток отслеживает, чтоб основной цикл запускался в определенное пользователем время.

Также, к автоматизированным функциям относится проверка по отзывам работы сервисов банка, окно (рис. 5) которой открывается нажатием соответствующей кнопки.

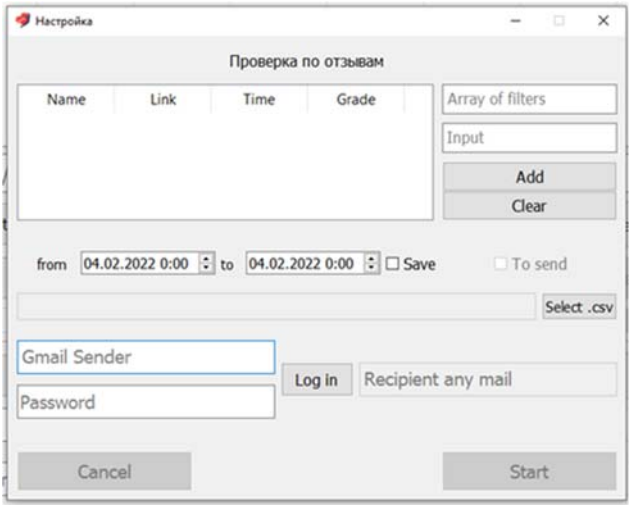


Рис. 5. Окно проверки отзывов пользователей определенных ресурсов

Для начала работы в данном окне нужно импортировать файл с названием и URL банков, в соответствующую строку ввести ключевые слова или словосочетания по их поиску в отзыве и добавить их в массив «фильтров». Список отзывов берется с сайта banki.ru, который признан лучим агрегатом для обратной связи с банками.

После чего нужно выбрать дату с какого по какое число программа должна будет проверять отзывы на предмет содержания ключевых слов. Если в отзыве будет найдено введенное слово или словосочетание, то

в таблицу в левой верхней части экрана запишется сводка о отзыве, название банка, которому был адресован отзыв, ссылка на отзыв, время, когда он был оставлен и оценка пользователя от 1 до 5. Так как, программа предназначена для поиска негативных отзывов о не работе сайта или ресурсов банка, то в качестве ускорения работы программы выбираются оценки от 1 до 2.

Следует заметить, что сценарии авторизации и сохранения сводки по отзывам точно такие же, как и в окне настройки периода проверки.

Выводы

В рамках данной работы были проведено исследование проблем недоступности интернет-ресурсов банков, разбор http-запросов, целевой парсинг данных с сайта banki.ru, создание многопоточных скриптов, как следствие – написание кроссплатформенного приложения для мониторинга доступности ресурсов сайтов банка на языке программирования Python с помощью фреймворка PyQt.

Библиографический список

1. *Бэрри П.* Изучаем программировании на Python: учеб. пособие. М.: Изд-во «Э», 2017. 624 с.

2. *Стригунов В. В.* Введение в компьютерные сети: учеб. пособие / науч. ред. Э. М. Вихтенко. Хабаровск: Изд-во «Тихоокеан», 2016. 103 с.

3. *Fielding R. T., Reschke J. F.* Idempotent Methods. URL: https://datatracker.ietf.org/doc/html/rfc7231#section-4.2.2

П. С. Конюхова
Уральский государственный экономический университет, г. Екатеринбург

Практика кибербезопасности для пользователей социальных сетей

Аннотация. Проводится исследование угроз кибербезопасности для пользователей социальных сетей с точки зрения пользователя. Представленное исследование показывает, что в платформе социальных сетей существует множество киберугроз, таких как потеря производительности, киберзапугивание, кибер-преследование, кража личных данных, перегрузка социальной информацией, непоследовательный личный брендинг, ущерб личной репутации, утечка данных, вредоносное программное обеспечение, перебои в обслуживании, взломы и несанкционированный доступ к учетным записям в социальных сетях. Исследование показывает, что демографические факторы, например, возраст, пол и уровень образования, не обязательно влияют на осведомленность пользователей Интернета о киберпространстве.

Ключевые слова: киберпреступность; киберугроза; социальная сеть.

Интернет стал одним из основных каналов коммуникации в современную эпоху, и социальные сети занимают значительную долю используемых возможностей. Большинство стран признали, что кибербезопасность стала одной из наиболее важных проблем, возникших за последние несколько лет в связи с расширением использования сети Интернет и социальных сетей [2]. Это может быть в связи с тем, что частое использование социальных сетей стало новой тенденцией, охватывающей широкий круг людей за короткий промежуток времени. Кроме того, возникновение новых платформ для общения, с менее продуманной системой защиты информации, привели к уязвимости от киберугроз в социальных сетях в большем количестве. Пользователи не могут полностью полагаться на технологии для защиты от киберугроз при использовании сети Интернет или социальных сетей. Таким образом, пользователи несут ответственность за самозащиту с их стороны.

Эволюция киберпреступлений в ИТ-индустрии началась в конце 1970-х гг. В то время он превратился из простого спама в гораздо более продвинутые формы, такие как вирусы и вредоносные программы. В наши дни слово «киберпреступность» охватывает широкий спектр виртуальных незаконных действий, совершаемых киберпреступниками с помощью любого источника, подключенного к сети Интернету. Эксперты говорят, что преступники часто стремятся к легким целям с наименьшим сопротивлением. Доверчивые пользователи часто становятся мишенями хакеров, а киберпреступники используют креативные

и различные способы сбора у них персональных данных [3]. Интернет стал неотъемлемой частью общества, и он стал основой для подключения и обмена информацией в наши дни. Это привело к тому, что всемирная сеть стала мишенью различных киберугроз, начиная от киберпреступлений и заканчивая кибершпионажем, кибертерроризмом и кибервойнами. Киберпреступления охватывают различные киберугрозы, включая, мошенничество, преследование, нарушение авторских прав, домогательства, угрозы, хакерские атаки, вирусы и многое другое [3]. Воздействие киберугроз меняется в зависимости от глобализации, уровня среды безопасности, осведомленности и уровня образования администраторов и пользователей данной информационно-коммуникационной среды. Эти киберугрозы могут варьироваться от потери конфиденциальности, личных, конфиденциальных и секретных данных и потери средств или крипто валют, до причинения вреда здоровью или жизни человека.

Кибербезопасность в социальных сетях

Социальные сети – это совокупность электронных коммуникационных платформ, используемых онлайн-пользователями для создания онлайн-сообществ. Люди используют эти платформы для обмена информацией, идеями, и личными сообщения друг с другом. Социальные сети обеспечивают открытость для профилей пользователей и данных, которыми они делятся в профиле. Однако такая открытость угрожает раскрытию или взлому профилей пользователей. Большинство пользователей социальных сетей сейчас полюбили делиться своими идеями и опытом с широким кругом друзей и друзей-друзей с помощью видео и фотографий [1]. Люди, которые размещают информацию в Интернете, в основном не думают о связанных с ней рисках безопасности. Однако это действие может добровольно раскрыть неизвестным людям больше личной информации, чем они ожидали. Сотрудникам следует быть более осторожными в отношении того, чем они делятся в социальных сетях, поскольку число случаев мошенничества в области социальной инженерии растет постепенно в наши дни [4]. Эти данные могут быть использованы против них и их компании вместе с другими личными данными, которые киберпреступники собрали в результате других нарушений данных потребителей.

Выводы

Кибербезопасность в контексте социальных сетей является актуальной темой для обсуждения, учитывая ее большую базу пользователей по всему миру [1]. Несмотря на то, что на различных платформах социальных сетей существует встроенная система безопасности, ее может быть недостаточно для защиты пользователей. Это происходит из-за человеческой ошибки, когда существует возможность открытия бэкдоров

для начала кибератак. Осведомленность и поведение пользователей играют важную роль в снижении воздействия человеческих ошибок. Влияние таких факторов, как возраст, пол и уровень образования пользователей, на их осведомленность о кибербезопасности в функциях безопасности платформ социальных сетей неясно. Кроме того, важно выявить рекомендуемые методы кибербезопасности для пользователей социальных сетей, основанные на влиянии вышеупомянутых переменных.

Библиографический список

1. *Майдыков А. А., Исаров О. Б.* Национальные интересы – актуальные проблемы противодействия использованию интернета террористическими и экстремистскими организациями // Национальные интересы: приоритеты и безопасность. 2015. № 38 (323). С. 44–51.

2. *Мелешкина И. И., Бегичева С. В.* Кибербуллинг и астротурфинг как виртуальная агрессия // Современные информационные технологии: проблемы и перспективы развития: материалы I Междунар. науч.-практ. конф. (Екатеринбург, 25 апреля 2017 г.). Екатеринбург: УИУ РАНХиГС, 2017. С. 108–113.

3. *Тультаева И. В., Каптюхин Р. В., Тультаев Т. А.* Воздействие социальных сетей на коммуникационные процессы в современном обществе // Бизнес. Образование. Право. 2014. № 4. С. 84–88.

4. *Kovtun D.* Assessment of Congruence of Unstructured Data Using Text Mining Technology // Proceedings – 2021 IEEE 23rd Conference on Business Informatics, CBI 2021 – Main Papers: 23 (Virtual, Online, 2021, Sept. 1–3). P. 163–166. DOI: 10.1109/CBI52690.2021.10067.

Т. Н. Мосина
Уральский государственный экономический университет, г. Екатеринбург

Угрозы кибербезопасности в инфраструктурах умного города

Аннотация. В статье рассмотрены угрозы кибербезопасности в инфраструктурах умного города. Автор приходит к выводу о необходимости создания банка данных о возможных рисках для разработки эффективной стратегии безопасности умных городов.

Ключевые слова: кибербезопасность; киберугроза; умный город; кибератака.

Цифровые технологии развиваются с поразительной скоростью. Они охватывают большинство сфер жизнедеятельности общества, в том числе градостроительство, что отражает концепция умного города.

Умный город – это инструментальная, взаимосвязанная и интеллектуальная среда. Термин «инструментальная» означает способность получать различные данные о жизни города и цифровой инфраструктуре

в режиме реального времени через подключенные устройства, измерительные датчики и персональные системы. Термин «взаимосвязанная» означает способность интегрировать данные на цифровых платформах, обмениваясь ими с различными цифровыми городскими сервисами. Термин «интеллектуальная» означает обработку данных для принятия оптимального решения с помощью передовых сервисов аналитики, моделирования и визуализации.

В России также развивается концепция умного города, которая включает: городское управление; инновации для городской среды; интеллектуальные системы общественной безопасности; инфраструктуру сетей связи; умное ЖКХ; «умный» городской транспорт; интеллектуальные системы экологической безопасности; туризм и сервис. В проекте участвуют более 200 городов.

С ростом умных городов возрастает риск кибербезопасности: комплексные кибератаки на критическую инфраструктуру путем прерывания работы автоматизированных систем управления, взлом связи между «умными» устройствами IoT/IIoT, блокирование узлов VANET (автономные автомобили, внедорожная инфраструктура), а также незаконное получение личных данных. Тема безопасности при построении умного города очень актуальна, именно поэтому целью данной статьи является выявление и обозначение рисков кибербезопасности умного города [1].

Концепция умного города предполагает объединение цифровой и физической инфраструктур в единую глобальную систему [4]. Взлом или заражение одного подключенного к сети устройства открывает возможность заражения многих других устройств, что приводит к каскадному ущербу, вызывая массовую кражу данных граждан.

Например, большое распространение «умных» систем находит в современных ЖК комфорт- и бизнес-класса в Москве и Санкт-Петербурге. Сервисы на базе интернета вещей для квартир ЖК позволяют управлять освещением, климат-контролем, безопасностью, бытовой техникой и мультимедиа через приложение. Но, как указывалось ранее, «умные» системы могут быть подвергнуты угрозам [2]. Так, нарушение систем умного освещения может привести к утечке информации, что в конечном счете приведет к получению личных данных жильцов: финансовых, медицинских и других. Для того чтобы этого не произошло, нужно уделять особое внимание кибербезопасности умного города.

Кибератаки на сети умного города можно разделить на пассивные и активные [5]. Пассивная кибератака обычно нарушает конфиденциальность. Злоумышленник подслушивает и перехватывает информацию, передаваемую по сети, не совершая при этом никаких деструктивных дей-

ствий, что крайне затрудняет его обнаружение. Активная атака направлена на взаимодействие с информационным потоком, нарушение целостности и доступности. Активный злоумышленник изменяет или скрывает/сбрасывает пакеты данных, нарушая логику работы сети. Они могут быть организованы как внешним, так и внутренним злоумышленником [3]. Другой возможной классификацией атак является классификация по нарушению одного из традиционных требований безопасности: конфиденциальности, целостности и доступности, а также аутентификации и ответственности.

Наибольший ущерб наносят сетевые атаки, поскольку они нарушают работу всей интеллектуальной инфраструктуры [6]. Чем большую площадь занимает атака, тем больший урон она наносит системе. Рассмотрим основные кибератаки, направленные на нарушение динамической маршрутизации сети:

Атаки типа «отказ в обслуживании» (DoS). Узел злоумышленника создает большое количество сообщений, которые могут быть размножены в результате широковещательной рассылки, что приводит к перегрузке канала передачи данных и деградации вычислительных ресурсов узлов сети для обработки всех сообщений, созданных злоумышленником. Таким образом, злоумышленник способен нарушить связь в сети умного города.

Распределенная DoS (DDoS) атака. Узлы злоумышленника начинают свои атаки из разных мест в разное время. Например, вредоносные узлы, расположенные рядом с целевым узлом, могут одновременно отправить на него поток сообщений и тем самым изолировать его от других сетей.

Атака «черная дыра» (The Black hole attack). Узел злоумышленника перехватывает и отбрасывает полученные пакеты, которые должны быть переданы другим узлам. Этот вид атаки особенно эффективен при нарушении политики доверия в динамической сети.

Атака «серой дыры» (The Grey hole attack). Если узел нарушителя отбрасывает все полученные пакеты, он может быть обнаружен соседними узлами. Поэтому злоумышленник частично отбрасывает пакеты.

Атака типа «Раковина» (The Sinkhole Attack). Узел нарушителя может быть предпочтительнее для соседних узлов в целях организации оптимального маршрута. В динамической сети узел может рассылать маршрутные сообщения, информируя своих соседей о том, что он является лучшим узлом для отправки пакетов на базовую станцию. Это позволяет злоумышленнику стать сетевым концентратором и собирать все пакеты, адресованные базовой станции.

Атака типа «червоточина» (The Wormhole Attack). Злоумышленник перехватывает пакеты данных и пересылает их другому вредоносному узлу, который находится в другой части сети, эта передача происходит вне полосы канала. Эта атака вредна тем, что позволяет избежать действительных маршрутов и утечки пакетов данных.

Атака Sybil. Злоумышленник представляет несколько узлов сети одновременно для других узлов, что становится проблемой безопасности для протоколов динамической маршрутизации, поскольку может повлиять на алгоритмы маршрутизации на основе голосования и балансировки нагрузки.

Реализация только одной атаки из приведенного выше списка может привести к сбоям в работе системы, что может вызвать негативные последствия: угрозу здоровью людей, экологическую катастрофу или отключение электроэнергии на производстве.

Выводы

Развитие цифровых технологий позволяют улучшить как качество оказываемых услуг, так и качество жизни людей, это отражает концепция умного города. С ростом популярности автоматизации и «умных городов» они также все больше подвергаются киберугрозам. Отказ в доступе или вторжение в частную жизнь автоматизированной системы может нанести серьезный ущерб отдельным гражданам и повлечь за собой значительные расходы как на индивидуальном, так и на государственном уровне. Также может возникнуть риск для здоровья, если будут скомпрометированы системы, обрабатывающие чрезвычайные события (например, аварии и пожары).

Тема безопасности при построении умного города имеет огромное значение, именно поэтому в данной статье были выявлены и обозначены риски кибербезопасности в инфраструктурах умного города. В дальнейшем это может помочь разработать эффективную стратегию безопасности умного города.

Библиографический список

1. *Баранова Е. К., Бабаш А. В.* Информационная безопасность и защита информации: учеб. пособие. М.: РИОР, 2018. 400 с.

2. *Демидов Р. А., Зегжда П. Д., Калинин М. О.* Анализ угроз кибербезопасности в динамических сетях передачи данных с применением гибридной нейросетевой модели // Проблемы информационной безопасности. Компьютерные системы. 2018. № 2. С. 27–33.

3. *Шаньгин В. Ф.* Информационная безопасность компьютерных систем и сетей: учеб. пособие. М.: Форум, 2018. 256 с.

4. *Kovtun D., Tovmasyan N., Nazarov A*. Trends and conditions for the development of green energy in the Russian Federation // E3S Web of Conferences (Almaty, 2021, May 20–21). DOI: 10.1051/e3sconf/202127001040.

5. *Pavlenko E., Zegzhda D*. Sustainability of cyber-physical systems in the context of targeted destructive influences // Proc. 2018 IEEE Industrial Cyber-Physical Systems (ICPS). DOI: 10.1109/icphys.2018.8390814.

6. *Zegzhda D., Stepanova T.* Achieving Internet of Things security via providing topological sustainability // Proceedings of the Science and Information Conference (SAI) (London, UK, 2015, July 28–30). P. 269–276.

А. Р. Мулланурова, Д. Б. Ковтун
Уральский государственный экономический университет, г. Екатеринбург

Стратегии обеспечения кибербезопасности в высших учебных заведениях

Аннотация. Статья посвящена проблемам разработки стратегий кибербезопасности в высших учебных заведениях, создающих тяжелое бремя для организаций.

Ключевые слова: кибербезопасность; стратегия управления; киберугроза; высшее образование.

С развитием технологий угрозы кибербезопасности в последние годы только растут. Их постоянное и быстрое изменение ложится тяжелым бременем на организации. Практически каждая крупная отрасль сталкивается с проблемами кибербезопасности, однако сектор высшего образования особенно уязвим.

Существует несколько причин уязвимости системы высшего образования с точки зрения безопасности. Во-первых, риски, связанные с кибератаками, выходят за рамки финансовых потерь для мира высшего образования. Действительно, в высших учебных заведениях хранится огромный объем конфиденциальной информации, такой как личные дела студентов, важные данные исследований и ценная интеллектуальная собственность. Потеря данных может представлять серьезную угрозу и нанести значительный ущерб репутации вуза. Во-вторых, в высших учебных заведениях часто располагается критически важная инфраструктура, требующая большого количества пользователей, поэтому любые инциденты в области кибербезопасности могут иметь катастрофические последствия. В-третьих, исторически сложилось так, что вузы были доступны общественности, их сети также были открыты. Однако после резкого перехода к удаленной работе и онлайн-обучению в связи с пандемией, все больше персональных устройств, не предоставленных университетом, подключаются к сети и системам вуза, и ставки на кибербезопасность повышаются.

К сожалению, многие существующие исследования по кибербезопасности имеют ограниченную справочную ценность для руководителей высших учебных заведений, поскольку они обычно ориентированы на технологии. В публикациях часто отсутствует общесистемный взгляд на кибербезопасность в вузах. Поэтому моя статья призвана восполнить этот пробел в литературе, изучить стратегии кибербезопасности в высших учебных заведениях с точки зрения системы и предоставить полезные выводы для руководителей вузов, работающих над этими стратегиями [2].

В новом десятилетии отражается ряд изменений и новое развитие технологий [5]. Они связаны с облачными вычислениями, мобильными технологиями и искусственным интеллектом [1]. Вопросы конфиденциальности систем также представляют собой более значимую, чем когда-либо проблему.

Отчасти из-за простоты управления и низкой стоимости все большее число учреждений и организаций переносят свои системы и инфраструктуру в облако, передавая хостинг поставщикам облачных услуг. Киберпреступники используют методы социальной инженерии, такие как фишинг, подмена веб – сайтов и шпионаж в социальных сетях, чтобы украсть учетные данные пользователей и впоследствии получить несанкционированный доступ к важной информации, хранящейся в облачной сети. Нарушение данных может произойти так, что пользователи даже не поймут, что их учетные записи были похищены.

В последние годы стремительное развитие технологий искусственного интеллекта расширило ландшафт угроз и увеличило возможности атак, выведя борьбу за кибербезопасность на новый уровень. Киберпреступники могут использовать искусственный интеллект, отличающийся автоматизацией и самообучением, что может затруднить обнаружение, охват и идентификацию уязвимых приложений, устройств и сетей для масштабирования своих атак.

Хотя и не существует единого метода решения для кибербезопасности, есть стратегии, которые могут помочь высшим учебным заведениям решить проблемы кибербезопасности.

Укрепление управления кибербезопасностью. Данный подход требует привлечения внимания высшего руководства к кибербезопасности. Помимо участия высшего руководства, воля и поведенческая приверженность руководства также имеют решающее значение. Кроме того, руководство должно осознать, что, хотя кибербезопасность является неотъемлемым компонентом управления информационными технологиями, она больше не должна быть исключительно обязанностью ИТ-отделов, а должна быть в центре внимания усилий всего учреждения.

Повышение осведомленности о кибербезопасности. вузы должны реагировать на тот факт, что человеческий фактор является самым слабым звеном в современном ландшафте кибербезопасности. Исследователи и эксперты утверждают, что формирование культуры кибербезопасности необходимо для изменения отношения, восприятия и привития хорошего поведения в сфере безопасности. Формирование культуры кибербезопасности также имеет решающее значение для поддержки планомерной реализации планов и политик, связанных с безопасностью. Для формирования такой культуры кибербезопасности подчеркнута необходимость регулярного общения, обучения, тренингов и повышения осведомленности в области безопасности.

Реагирование на угрозы на основе искусственного интеллекта. Учитывая, что технологии искусственного интеллекта в последние годы расширили ландшафт угроз и увеличили возможности атак, вузам необходимо подготовиться к реагированию на киберугрозы на его основе. Реальный случай подобной кибератаки произошел в марте прошлого года. Управляющему компании позвонил человек и, представившись гендиректором, попросил о переводе 220 000 евро. Голос был идентичен и управляющий, абсолютно уверенный в том, что звонок от генерального директора, осуществил перевод [4].

Таким образом, было предложено несколько мер для борьбы с угрозами на основе искусственного интеллекта. Эти меры включают внедрение системы обнаружения вторжений в сеть и системы обнаружения вторжений на хост. Эти системы могут обеспечить значительное повышение эффективности обнаружения, поддержку автоматизации этапов расследования, а также повышение надежности алгоритмов и мониторинга поведения человека и машины.

Важно отметить, что кибербезопасность – это и проблема управления. Поэтому организации должны хорошо разбираться в технологических компонентах, а также в компаниях и уязвимостях [3].

Внедрение новых и более сложных мер безопасности. Единый вход в систему позволяет пользователям проходить аутентификацию один раз для последующего доступа к различным приложениям в разных ИТ-системах учреждения. Установление гарантии идентичности означает уверенность в том, что человек является тем, за кого себя выдает, поскольку одного пароля для этого недостаточно. Необходимо добавить еще один уровень факторов для проверки личности.

В качестве современной альтернативы паролям в вузах может быть опробована многофакторная аутентификация – метод аутентификации, при котором человеку предоставляется доступ к системе после предъявления двух или более доказательств, подтверждающих его личность [6].

Такая система контроля разрешений доступа пользователя динамически выбирает наилучшие механизмы для аутентификации пользователя в зависимости от контекстных факторов, принимая во внимание обстоятельства пользователя, такие как географическое положение, должностные обязанности, модели поведения в прошлом, близость к устройствам и время суток, чтобы определить, зачем пользователю нужен доступ и что он будет с ним делать.

Внимание к использованию мобильных устройств. Широко распространенная зависимость от мобильных устройств и размытая грань между личным и профессиональным использованием этих устройств поставили перед кибербезопасностью вузов серьезные задачи. Высшие учебные заведения должны уделять особое внимание управлению связанными с ними рисками кибербезопасности. В частности, специалисты по безопасности вузов должны лучше понимать, как происходит удаленная работа и онлайн обучение, чтобы удовлетворить эти сценарии, обеспечивая при этом соблюдение требований кибербезопасности.

Шифрование является простой стратегией защиты от различных сценариев риска, таких как утечка данных при использовании личных устройств. Вузы должны разработать четкие политики и руководства, которые помогут определить надлежащее использование шифрования и соответствующих методов управления ключами.

Выводы

Цифровой скачок новых технологий сопровождается повышенной уязвимостью. Новые формы кибер-атак будут продолжать испытывать потенциал кибербезопасности вуза. В ответ на потенциальные риски кибербезопасности в новом десятилетии и уникальные обстоятельства вузов, которые могут поставить под вопрос применимость многих существующих организационных методов управления кибербезопасностью, данное исследование предлагает общесистемный подход с приоритетными стратегиями. Стратегии включают: укрепление управления кибербезопасностью, повышение осведомленности о кибербезопасности, реагирование на угрозы на основе искусственного интеллекта, внедрение новых и более сложных мер безопасности, внимание к использованию мобильных устройств.

Хотя перечисленные выше стратегии не являются всеобъемлющими и не могут предотвратить каждую атаку, в масштабах всей системы они представляют собой относительно простые средства, которые могут быть использованы для получения значительных преимуществ в борьбе высшего образования с потенциальными киберугрозами.

Библиографический список

1. *Бегичева С. В., Товмасян Н. Д.* Возможности интеллектуального анализа данных в процессе моделирования деятельности Института государственного и муниципального управления УрГЭУ // BI-технологии в оптимизации бизнес-процессов: сб. ст. Междунар. науч.-практ. очно-заоч. конф. (Екатеринбург, 2 декабря 2015 г.). Екатеринбург: УрГЭУ, 2015. С. 110–113.
2. *Диогенес Ю., Озкайя Э.* Кибербезопасность: стратегии атак и обороны / пер. с англ. Д.А. Беликова. М.: ДМК Пресс, 2020. 326 с.
3. *Коллинз М.* Защита сетей. Подход на основе анализа данных / пер. с англ. А.В. Добровольская. М.: ДМК Пресс, 2020. 308 с.
4. *Мельников Д. А.* Организация и обеспечение безопасности информационно-технологических сетей и систем: учебник. М.: КДУ, 2015. 598 с.
5. *Kovtun D., Tovmasyan N., Nazarov A.* Trends and conditions for the development of green energy in the Russian Federation // E3S Web of Conferences (Almaty, 2021, May 20–21). DOI: 10.1051/e3sconf/202127001040.
6. *Pinheiro J.* Review of cyber threats on Educational Institutions // Proceedings of the Digital Privacy and Security Conference (Washington, DC, USA, 15 January 2020).

Д. В. Санников
Югорский государственный университет, г. Ханты-Мансийск

Проблемы цифровой трансформации системы управления университетом в эпоху цифровой экономики

Аннотация. В статье рассматриваются основные этапы перехода текущей модели управления университетом к модели управления, основанной на данных. Обосновываются проблемы, предпосылки и ожидаемые итоги цифровой трансформации университета, связанные с переходом к цифровой экономике.

Ключевые слова: университет; цифровая трансформация; модель управления на основе данных; цифровизация; реинжиниринг; бизнес-процесс; компетентностный профиль; искусственный интеллект.

Организация системы управления образовательным процессом, а значит и процессом управления всем университетом, в эпоху цифровой экономики требует от текущей управленческой команды изменений уже сейчас, при этом изменения в программу развития университета, ровно как и в стратегию цифровой трансформации, необходимо вносить еще и по ходу их реализации. Большие данные, платформенные решения, компетентностные профили обучающихся и искусственный интеллект,

казавшийся в допандемийный период (COVID-19) чем-то далеким, сегодня стали темой ежедневных обсуждений[1] не только на уровне бизнеса, но и на уровне такой консервативной организации, как университет[2].

Ключевой проблемой для осуществления цифровой трансформации большинства университетов является отсутствие как таковой цифровой модели выпускаемого продукта, то есть выпускника, имеется ввиду наличие компетентностного профиля, портфолио и результатов успеваемости, так как, как правило, данные о выпускнике – это результаты академической успеваемости, в то время как видится важным обеспечить возможность работодателя выбрать для себя подходящего работника, по сути необходимо создать своеобразную витрину выпускников со всеми их достижениями и регалиями.

Другой не менее важной проблемой университета на пути к цифровой трансформации является отсутствие понятных метрик, в том числе указанных выше, для принятия адекватных управленческих решений, ведь если в бизнесе ключевой параметр – это прибыль, то в университете это может быть как средний балл ЕГЭ, уровень доходов от научных исследований, так и банальная численность студентов очной формы обучения, и здесь каждый университет должен выбрать свой наиболее значимый для себя набор метрик.

Следующей проблемой можно назвать, как ни парадоксально, наличие большого числа умных и самодостаточных людей (научно-педагогические работники), которым порой достаточно сложно договорится между собой, не говоря уже о том, что необходимо сформировать единую стратегию развития университета, которая, как и любая другая стратегия, предполагает синхронизацию, координацию и отказ от отдельных финансируемых ранее направлений деятельности. Данная проблема способна серьезно обостряться, когда руководство университета не имеет ясного представления от том, куда, зачем и как движется университет в своем развитии.

Следующей проблемой следует назвать постепенный процесс транс-формации учебного плана студента, содержащего определенный набор дисциплин в учебном плане, который является набором компетенций, то есть студенту необходимо не просто прослушать дисциплины и получить положительную оценку, но и сформировать в себе совместно с преподавателем конкретную компетенцию определенного качества,

---

[1] *Стратегия* цифровой трансформации отрасли науки и высшего образования. М., 2021. URL: https://minobrnauki.gov.ru/upload/iblock/e16/dv6edzmr0og5dm57dtm0wyllr6uwtujw.pdf?ysclid=l26l3hbfmh

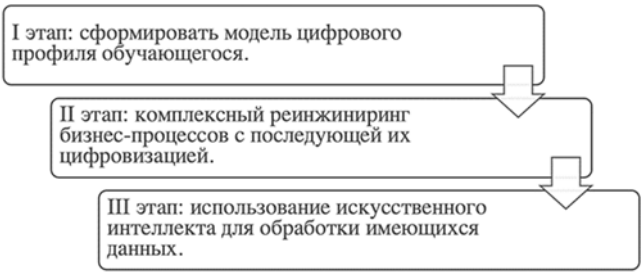
[2] *Онлайн-курс* «Управление университетами». Первый в мире онлайн-курс по трансформации университетов. URL: https://www.skolkovo.ru/programmes/15102020-online-kurs-upravlenie-universitetami.

руководителю образовательной программы по своей сути необходимо уйти от представления об учебном плане, как наборе дисциплин, создав «скелет» компетенций, которые необходимо сформировать у обучающихся конкретного направления подготовки, а также обеспечить наличие верифицированной методики оценки сформированности компетенции. В результате знаниевая компонента образования является «фоном», на основе которого формируется компетенция, тем самым позволяя устраивать открытый конкурс для включения тех или иных дисциплин в учебный план конкретного направления подготовки, то есть руководитель образовательной программы предлагает, например, сформировать условную компетенцию «N» с помощью 3 дисциплин, а преподаватели университета заявляются на эту «N» компетенцию со своими дисциплинами, в результате возникает необходимость создания совета образовательной программы, ответственного за выбор конкретных курсов для включения в учебный план.

Еще одной проблемой можно назвать проблему интеграции массовых открытых онлайн-курсов в образовательное пространство университета, так как с одной стороны они позволяют обеспечить массовость, снизить расходы на образование для университета и т.д., а с другой стороны данные курсы обеспечивают формирование лишь знаниевой компоненты у обучающихся, при этом совершенно не обещая обеспечить сформированность той или иной компетенции.

Все это является проблемами для цифровой трансформации системы управления университетом, не говоря уже о нарастающей конкуренции со стороны образовательных платформ («Яндекс.Практикум», Skillbox и т.д.) и борьбе между собой (между университетами) за сохранение своего существования в особенности для небольших региональных университетов, так как имеется устойчивый тренд на укрупнение университетов. По нашему мнению, процесс управления университетом в цифровой экономике потребует (см. рисунок): во-первых, создания и формирования компетентностого профиля обучающегося, включающего сведения об успеваемости, уровне сформированности компетенции, данных портфолио и результатах трудоустройства; во-вторых, перехода к управлению на основе данных, а значит, требуется не просто получить данные, но и провести цифровизацию своих внутренних бизнес-процессов с целью сбора и хранения всевозможных данных [1]; в-третьих, перейти к использованию искусственного интеллекта не просто для анализа данных, а для построения образовательной модели, основанной на data-driven подходе, то есть использовании информации для принятия управленческих решений [2], например о ситуации на

рынке труда и компетентностном профиле обучающегося, что тем самым позволит помочь последнему выстраивать персональную траекторию развития.



Этапы перехода университета к новой модели управления

Важность формирования компетентностного профиля обучающегося как исходной точки смены управленческого подхода связана с тем, что это позволит перейти еще и к иной модели работы с научно-педагогическими работниками университета, основанной на образовательном результате, то есть сформированности компетенции, что существенно отличается от оценки за знаниевые компоненты, формируемые на основе конкретной дисциплины. В результате научно-педагогический работник превращается в своеобразного «тренера», специализирующегося на формировании определенной компетенции на основе определенного материала конкретной дисциплины. Последним шагом в реализации первого этапа и важнейшим условием успеха последующих этапов построения модели должны стать данные о трудоустройстве выпускника, которыми обладает Пенсионный фонд Российской Федерации, без интеграции с данными которого, построение модели управления образовательным процессом видится достаточно сомнительным.

Таким образом, подводя итоги работы, необходимо сказать, что управление университетом должно неизбежно перейти к модели управления, основанной на данных, при этом в конкуренцию с университетами вступают различные образовательные платформы и в некоторых случаях даже среднее профессиональное образование, что в условиях новых экономических реалий требует существенной оптимизации бизнес-процессов университета с их заведением в разного рода цифровые решения. Главнейшей задачей видится построение измеряемой модели выпускаемого университетом «продукта» – выпускника, так как в отсутствии конкретных метрик, измеряющих успех образовательного

процесса, невозможно никакое построение модели управления университетом.

Библиографический список

1. *Трофимов В. В., Трофимова Л. А.* О концепции управления на основе данных в условиях цифровой трансформации // Петербургский экономический журнал. 2021. № 4. С. 149–155.
2. *Фиофанова О. А.* Управление на основе больших данных в сфере образования // Государственная служба. 2021. Т. 23, № 3. С. 86–91.

Р. Г. Тихончук
Администрация города Евпатории Республики Крым

Резильентность как принцип управления региональными экономическими системами

Аннотация. Обобщаются недавние исследования по теории резильентности: систематизируются подходы к пониманию резильентности, уточняются факторы резильентности российской экономики к шокам различной природы. Автор делает вывод о необходимости внедрения принципа резильентности стратегического управления в целях использования шоков как новых возможностей формирования структуры, обеспечивающей высокую способность к восстановлению.

Ключевые слова: резильентность; устойчивое развитие; шокоустойчивость; рискориентированное управление.

Исследования процесса стратегического управления региональных экономических систем выявили необходимость адекватного применения и усиления использования принципа такого планирования как резильентность. Это выявляет необходимость смены парадигмы динамики экономических систем от сложившегося понимания «устойчивого развития» к их резильентности. Развитие процесса стратегирования смещает приоритеты на исследование свойств сложных экономических систем, связанных со способностью к их шокоустойчивости (резильентности), определяемой международными организациями как «способность системы к мобильной перегруппировке своих элементов и ключевых ресурсов для достижения динамической устойчивости на новом уровне развития в ответ на внезапные внутренние или внешние возмущения»[1]. Подход, применяемый Всемирным банком, определяет сущность резильентности экономической системы на макроуровне как совокупность «(1) мгновенной резильентности – способности ограничивать величину

[1] *OECD*, SIDA. Resilience systems analysis: Learning and recommendations report. Paris: OECD Publishing, 2017.

немедленных потерь дохода для заданного размера капитальных потерь; и (2) динамической резильентности − способности быстро восстанавливаться» [3].

Теория резильентности связана с изучением экономической динамики, неотъемлемой частью которой являются шоки. Классифицируя шоки, приводящие к экономическим кризисам, выделяют природные и техногенные, глобальные экономические, политические, быстрые технологические, иные изменения, как пандемия. По характеру возникновения шоков можно разделить их на резкие одномоментными (такие как природная катастрофа), и медленно текущие (как технологические изменения и вызываемые ими большие циклы Кондратьева). Национальная экономика, регион, отрасль или предприятие как экономическая система разного уровня в условиях шока дает соответствующий определенный отклик. Система, в большей мере обладающая свойством резильентности, быстрее выйдет из рецессии, полностью восстановится и может продолжить рост.

В. В. Акбердина формулирует два подхода к пониманию резильентности в аспекте экономической динамики: технический (равновесный), предполагающий возвращение к ранее существовавшей точке равновесия с основным критерием − скоростью возвращения в исходное состояние, что зависит интенсивности и продолжительности воздействия на экономическую систему. Второй подход – экосистемный (эволюционный), базирующийся на непрерывной адаптации к постоянно меняющимся условиям и имеющий критерием эластичность экономической системы.

На основе определения экономической резильентности системы как «способность экономики полностью восстанавливаться после воздействия шоков различной природы за счет внутренних адаптивных свойств» [1, с. 10], следует подчеркнуть принципиальное отличие резильентности от устойчивости: постшоковость и предсобытийность, проявления этих свойств соответственно. Исходя из приведенного понимания экономической резильентности как «способности системы поглощать или смягчать потери, реконфигурироваться и обновляться», факторы резильентности нужно искать внутри самой системы. Следуя холистическому подходу к экономическим системам [2, с. 12], выделяют две группы факторов: (1) «врожденные» (например, сложившийся эволюционный путь, структура экономики, особенности рынка труда, способность предприятий заменять исходные ресурсы теми, которые были сокращены внешним шоком, или способность отраслевых рынков перераспределять ресурсы в ответ на ценовые сигналы); (2) «приобретенные» – именно адаптивность как способность в кризисных ситуациях дополнительными усилиями сглаживать последствия кризиса (к ним могут быть

отнесены государственная политика, национальная инновационная система, доступное финансирование и др.).

Среди факторов резильентности российской экономики к шокам различной природы в России исследованы такие «врожденные» факторы как наличие значительных резервов и мобильность капитала между финансовым и промышленным сектором, а также адаптивные факторы, связанные с антикризисной политикой государства в 2008 г. В период санкций факторами резильентности экономики России выступили огромный потенциал промышленности и исследовательского сектора, реализовавшим политику импортозамещения. В период кризиса 2020 г. Россия, опираясь на преобладание крупного бизнеса с государственным участием и внутристрановой локализации цепочек добавленной стоимости внутри преодолела кризисом гораздо лучше, чем ведущие глобальные игроки.

Соглашаясь с выводами о принципиальном отличии понятий «резильентность экономики» и «устойчивость экономики», мы придерживаемся мнения, что концепты «управление рисками» или «рискориентированное управление» показывают недостаточную практическую полезность, поскольку ошибок при принятии решений не становится меньше. Более того, требуется смена парадигмы, основанная не на рисках, а на внутрисистемных факторах и ресурсах, формирующих потенциал резильентности и требующих разработки адекватных цифровых инструментов мониторинга.

Таким образом, развитие потенциала резильентности экономической системы предполагает необходимость внедрения одноименного принципа стратегического управления в целях использования шоков как новых возможностей формирования структуры, обеспечивающей высокую способность к восстановлению.

Библиографический список

1. *Акбердина В. В.* Резильентность экономики: факторы устойчивости к шокам // Стратегии развития социальных общностей, институтов и территорий: материалы VII Междунар. науч.-практ. конф. (Екатеринбург, 19–20 апреля 2021 г.): в 2 т. Екатеринбург: Изд-во Урал. ун-та, 2021. Т. 1. С. 8–15.

2. *Сурнина Н. М.* Пространственная экономика: проблемы теории, методологии и практики. Екатеринбург: Изд-во УрГЭУ, 2003. 281 с.

3. *Hallegatte S.* Economic Resilience: Definition and Measurement (May 1, 2014). World Bank Policy Research Working Paper No. 6852. Available at SSRN: https://ssrn.com/abstract=2432352.

А. А. Якушина
Уральский государственный экономический университет, г. Екатеринбург

Избавление от компромисса между удобством использования и безопасностью: поведенческий подход

Аннотация. Предлагается теоретическая перспектива использования компромисса удобства использования и безопасности информационных систем. Исследование направлено не на поиск технических решений, применимых к определенному типу систем, а на представление общей перспективы, которую можно назвать «кибербезопасностью, основанной на поведении».

Ключевые слова: кибербезопасность; анализ поведения; жетонная экономика; геймификация.

Основной мыслью любой литературы по кибербезопасности является обратно пропорциональная зависимость между удобством использования и безопасностью: более защищенные системы обязательно будут менее простыми в использовании, а удобные системы будут более уязвимыми для угроз [2].

За последние полвека для улучшения взаимодействия между пользователем и технологиями, использования устройств без усилий и сокращения процесса обучения было приложено множество усилий. С распространением процедур, которые можно выполнять онлайн, потребность в разработке технологий, ориентированных на пользователя, значительно увеличилась [1]. Сегодня Интернет используется для выполнения задач, которые раньше выполнялись за пределами киберпространства. Теперь люди покупают услуги и продукты, получают информацию и общаются с помощью приложений на персональных устройствах. Более половины населения мира ежедневно пользуется Интернетом как для деловых, так и для частных целей, и возможности для киберпреступлений, естественно, пропорциональны распространенности онлайновой деятельности. Непосредственным примером вмешательства в процесс улучшения взаимодействия человека и технологий, связанного с кибербезопасностью, является сохранение учетных данных для входа в систему с целью не запоминать их и входить в систему без автоматического ввода этих данных. В условиях повышения удобства использования такая практика увеличивает вероятность того, что злоумышленник получит доступ к системе и библиотеке сохраненных паролей. И наоборот, такие процедуры, как создание сложных паролей или их постоянная смена, повышают безопасность, но делают взаимодействие человека и системы более сложным. Кроме того, это приводит к тому, что пользователь начинает применять методы, нарушающие безопасность, например, писать пароль на листочке, который наклеен на компьютер.

Проблема заключается в совмещении безопасности с процедурами и интерфейсами, способными улучшить жизнь обычных пользователей.

Кибербезопасность – это защита конфиденциальности, целостности и доступности информации в киберпространстве. В частности, она представляет собой ту часть информационной безопасности, которая в основном сосредоточена на защите цифровой информации от любых угроз, которые могут возникнуть при использовании Интернета [2].

Внимание, уделяемое кибербезопасности, постоянно растет, особенно в связи с распространением Интернета. Оно также возросло в связи с глобальной пандемией COVID-19. Организациям и компаниям пришлось внедрить практику работы из дома, что привело к использованию работниками устройств (иногда даже личных) и соединений, не имеющих стандартных мер безопасности, предоставляемых компаниями, что привело к росту кибератак и рисков для корпоративных данных.

Кибератака – это любое действие, предпринятое для подрыва работы компьютерной сети с целью нарушения политической и национальной безопасности. Таким образом, это нарушение нормальной работы компьютера и потеря информации в результате серии злонамеренных действий. Кибер-атаки осуществляются с целью распространения дезинформации, блокирования определенных услуг, доступа к конфиденциальной информации, шпионажа, кражи данных и финансовых потерь.

При использовании термина «удобство использования» трудно избежать таких выражений, как «простота использования» или «интуитивность».

Как правило, эффективность совпадает с достижением целей, результативность – со временем, которое требуется для выполнения задачи, а удовлетворенность – с субъективными оценками пользователей. Таким образом, удобство использования не является характеристикой самого продукта, а зависит от характеристик пользователей системы, от цели, которую они намереваются достичь, и от контекста, в котором используется продукт. Поэтому при проектировании технологий нельзя игнорировать знание потребностей, ограничений и потенциальных возможностей пользователей, а также тщательный анализ задач, который необходимо проводить при использовании устройства в каждом контексте.

Безопасность информационных технологий также должна быть удобной для использования; выражение «удобная безопасность» означает управление информацией о безопасности в дизайне пользовательского интерфейса.

Безопасность, таким образом, не является функциональностью, отделенной от удобства использования, но связана с ним, и цель разработ-

чика должна заключаться в обеспечении как безопасности, так и удобства использования, не допуская, чтобы одно нарушало другое. Поскольку последствия неправильного управления этим компромиссом могут привести к тому, что процедуры либо подвержены высокому риску нарушения, либо, наоборот, слишком сложны. В последнем случае чрезмерные усилия по обеспечению безопасного поведения могут привести к появлению менее безопасных альтернативных моделей поведения.

Среди различных взглядов, принятых в психологии для объяснения поведения людей и составления прогнозов, анализ поведения играет первостепенную роль. Поведенческий подход основан на идее, что последствия играют решающую роль в формировании повторяющегося поведения. Человек, играющий в игровые автоматы, будет продолжать играть, если ранее он уже выигрывал. Таким образом, когда поведение выбирается по его подкрепляющим последствиям, частота его применения увеличивается. И наоборот, поведение, которое не сопровождается подкрепляющими последствиями, уменьшается в частоте, вплоть до исчезновения [4]. Этот процесс называется «оперантное обусловливание», и он является основным способом, с помощью которого организмы изменяют свое поведение на протяжении всей жизни. Например, мы набираем номер телефона, чтобы пообщаться с человеком, которого хотим услышать. Общение с человеком, в данном случае, является подкреплением, а последствие поведения - основополагающим элементом в его определении. Для того, чтобы поведение можно было определить, как оперантное, не обязательно набирать номер телефона, нажимая кнопки на клавиатуре, просить сделать это другого человека или применять любой другой способ, если все эти действия в итоге приведут к одному эффекту.

Так как анализ поведения может быть полезен при решении проблем киберугроз?

Изначально нужно пересмотреть роль удобства в определении использования инструментов и процедур безопасности.

Инструменты безопасности являются необходимым, но недостаточным условием для создания безопасной системы. Тем не менее, даже при условии доступности инструмента, далеко не всегда он применяется. Например, наблюдается низкий уровень обновления программного обеспечения, несмотря на высокий уровень его установки, что говорит о поведении человека, как о решающем факторе в профилактике нарушений кибербезопасности.

Если пользователи не понимают или не знают о рисках безопасности, они более склонны к некорректному поведению. Более того, пользователи могут знать о рисках, но не знать о правильном поведении. Действительно, чем сложнее инструмент, основанный на таких понятиях,

как криптография, ключи доступа и цифровая подпись, тем большим препятствием он становится, так что люди пытаются его обойти. Когда пользователи чувствуют себя подавленными требованиями системы, они могут отказаться, как от мер безопасности, так и от самой системы. Следовательно, удобство использования системы становится критическим фактором, объясняющим, почему люди ведут себя небезопасно [3].

Как уже было сказано, компромисса между безопасностью и удобством использования невозможно избежать, однако есть предположение, что его можно использовать для разработки стратегий проектирования и улучшения безопасности. В этом решающей становится поведенческая перспектива.

Например, существует много литературы на тему «геймификации»: использование игровых форм для достижения целей обучения. Принцип геймификации заключается в использовании динамики и механики игр, таких как накопление очков, достижение уровней, получение наград и демонстрация значков. До появления термина «геймификация» в литературе такая динамика была известна как «токен-экономика». Экономика токенов – это довольно сложная система подкрепления, основанная на накоплении токенов, которые в конечном итоге могут быть обменены на товары, услуги или привилегии. Принцип работы такой экономики схож с денежной системой: это набор правил, определяющих стоимость объекта, не имеющего внутренней ценности (как монета или банкнота).

Экономика токенов строится на шести основных элементах [5]:

— целевое поведение: поведение, необходимое для получения токенов;

— условие получения токенов: процедура, посредством которой токен обуславливается как подкрепление;

— выбор подкрепления: метод, с помощью которого определяются действия, получаемые в результате обмена токенами;

— график производства токенов: график подкрепления, посредством которого выпускаются токены;

— график производства обмена: график, определяющий, когда токены могут быть обменены на бонусы;

— график обмена токенов: график, определяющий стоимость бонусов в жетонах.

В совокупности, все эти элементы создают систему, подкрепляющую интерес пользователя к конкретному действию за вознаграждение, что является теоретическим решением исследуемого компромисса.

Все это – лишь попытка понять, возможно ли применение токен-экономики в сфере кибербезопасности, поэтому исследовательская программа в этой области требует множества шагов для оценки влияния как можно большего числа переменных.

Выводы

Ключевым моментом данного размышления является то, что системы безопасности, основанные на экономике токенов, могут быть реализованы путем усиления безопасного поведения, то есть, предлагая удобство использования в качестве бонуса безопасного поведения. На практике это будет модель безопасности на основе поведения, эффективно использующая компромисс между удобством использования и безопасностью вместо попыток уменьшения разрыва между двумя этими потребностями.

Основополагающими для продолжения исследования и возможной реализации могут послужить следующие вопросы:

– будет ли внедрение системы токен-экономики эффективным для повышения уровня безопасного поведения в контексте кибербезопасности, если задача состоит в обнаружении подозрительной активности в стандартных условиях? Экономика токенов успешно используется в различных областях, поэтому причин исключать то, что она может проявить свои положительные эффекты и в контексте кибербезопасности, нет;

— будет ли возможный положительный эффект от такой программы ограничен получением токенов, или он сохранится и после ее завершения? Очень важно оценить, необходимо ли дальнейшее поддержание эффекта безопасного поведения;

— какой график подкрепления наиболее эффективен для достижения эффекта? График бонусов может быть основан на количестве произведенного поведения или на интервале, необходимом для достижения подкрепления;

— добавит ли что-нибудь наказание за небезопасное поведение? Подкрепление – очень мощный механизм, гораздо мощнее наказания, но сочетание этих двух стратегий вполне возможно приведет к более эффективным результатам.

После определения закономерностей в поведении пользователей следующим шагом должен стать переход от теоретических исследований к реализации стратегий. Однако предложенное решение направлено не на поиск технических решений, применимых к определенному типу систем, а на представление общей перспективы, которую можно назвать «кибербезопасностью, основанной на поведении». В этой статье подчеркивается то, что для решения подобного рода проблем, необходимо выходить за установленные рамки.

Библиографический список

1. *Бегичева С. В., Назаров А. Д., Назаров Д. М.* Облачные технологии в практике управления малым и средним бизнесом. Екатеринбург: Изд-во УрГЭУ, 2017. 103 с.

2. *Azhar M. Q., Bhatia S., Gagne G., Kari C., Maguire J., Mountrouidou X., Tudor L., Vosen D., Yuen T. T*. Securing the Human: Broadening Diversity in Cybersecurity // Proceedings from 2019 ACM Conference on Innovation and Technology in Computer Science Education (Scotland: Aberdeen. July 15 2019). DOI: 10.1145/3304221.3325537.

3. *Kadzin, A. E*. Single-Case Research Designs: Methods for Clinical and Applied Settings. 3rd ed. Oxford: Oxford University Press, 2020.

4. *Pierce W. D., Cheney C. D.* Behavior Analysis and Learning: A Biobehavioral Approach. 6th ed. A Psychology Press Book, 2017.

5. *Whitty M., Grobler M., Janicke H.* Risks, Mitigations and Interventions of Mass Remote Working during the COVID-19 Pandemic. Perth, Australia: Cyber Security Cooperative Research Centre, 2020.

Содержание

Информационная безопасность и компьютерные технологии

Цифровые решения для бизнеса и общества

Проблемы трансформации и риски цифрового общества

Цифровая трансформация общества и информационная безопасность

Материалы
Всероссийской научно-практической конференции

(Екатеринбург, 18 мая 2022 г.)

Печатается в авторской редакции
и без издательской корректуры

Компьютерная верстка *К. А. Терехиной*

Поз. 71. Подписано в печать 15.09.2022.
Формат 60 × 84 $^{1}/_{16}$. Гарнитура Таймс. Бумага офсетная. Печать плоская.
Уч.-изд. л. 5,3. Усл. печ. л. 5,6. Печ. л. 6,0. Заказ 436. Тираж 12 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