УДК 330.341

В. Б. Криштаносов
Белорусский государственный технологический университет

УГРОЗЫ И РИСКИ ЦИФРОВОЙ ЭКОНОМИКИ НА СЕКТОРАЛЬНОМ УРОВНЕ

Выявлены основные подходы к оценке рисков, связанных с внедрением современных цифровых технологий, включая общие технологические компоненты (IoT, BDA, AI, Blockchain, Cloud) и бизнес-операционные (производственные) системы на уровне определенных секторов и отраслей. Выделены наиболее уязвимые производственные системы с точки зрения киберугроз, риски взлома которых потенциально могут нанести максимальный урон деятельности предприятий. Обоснованы взаимосвязанности в оцифрованных средах двух соответствующих основных сетей: информационной и производственной (в промышленности, энергетике, сельском и коммунальном хозяйствах, телекоммуникациях, логистике, финансовом секторе, торговле), которые обусловливают увеличение поверхности атаки и предоставляют больше возможностей для их распространения. Сделаны эмпирические оценки рисков и угроз по основным видам кибератак по методологии CIA. Выявлены наиболее распространенные киберугрозы в динамике их распространения.

Ключевые слова: цифровизация, риски и угрозы, сектора и отрасли.

Для цитирования: Криштаносов В. Б. Угрозы и риски цифровой экономики на секторальном уровне // Труды БГТУ. Сер. 5, Экономика и управление. 2022. № 1 (256). С. 28–52.

V. B. Kryshtanosau
Belarusian State Technological University

THREATS AND RISKS OF DIGITAL ECONOMY AT THE SECTORAL LEVEL

There were identified the main approaches to the risk assessment associated with the introduction of modern digital technologies, including general technological components (IOT, BDA, AI, Blockchain, Cloud) and business operating (production) systems at the level of certain sectors and the branches. There were highlighted the most vulnerable industrial systems from the point of view of cyber threats, the risks of hacking of which can potentially apply the maximum damage to enterprises. It has been substantiated the reasonable interconnections in digitized environments of two relevant main networks: information and industrial (in industry, energy, agricultural and communal farms, telecommunications, logistics, financial sector, trade), which manifests the increase in the surface of the attack and more opportunities to distribute them. There have been made the empirical assessments of risks and threats in the main types of cyberatak on CIA methodology. There have been identified the most common cyber threats in the dynamics of their spread.

Key words: digitalization, risks and threats, sectors and industries.

For citation: Kryshtanosau V. B. Threats and risks of digital economy at the sectoral level. *Proceedings of BSTU, issue 5, Economics and Management*, 2022, no. 1 (256), pp. 28–52 (In Russian).

Введение. Цифровизация экономики ведет к формированию не только макроэкономических рисков, но и рисков, затрагивающих определенные сектора, отрасли, а также имеющих потенциал для мультиотраслевого / мультисекторального распространения. Кроме того, цифровые технологии, в том числе Big Data, AI / ML, позволяют отдельным компаниям на секторальном уровне агрегировать большие массивы персональных данных клиентов для целей ценовой дискриминации.

Следует отметить, что цифровизация отраслей современной экономики предполагает внедрение комплекса информационных систем, включающих общие технологические компоненты (IoT, BDA, AI, Blockchain, Cloud) и бизнес-операционные (производственные) системы (табл. 1).

Основная часть. Согласно эмпирическим оценкам рисков и угроз по основным системам управления и интеллектуализации, наиболее уязвимыми системами с точки зрения киберугроз, риски взлома которых потенциально могут нанести максимальный урон деятельности предприятий, являются: PDM, SCADA, CAM, MES, BPM, системы AI, IoT и роботизированные устройства конвейера.

Ключевыми блоками рисков имплементации технологических решений IoT, Cloud, AI, BDA, Blockchain, как показано в табл. 2 (см. на с. 30–31), в экономическую, социальную, общественную системы считаются: кибербезопасность систем, конфиденциальность данных, отсутствие общих стандартов и совместимость.

Таблица 1

Цифровые технологические решения в рамках концепции «Новая экономика 2.0» (разработано автором)

Промышленность / Industry 4.0	Финансовый сектор / FinTech	Энергетика / Smart Grid	Сельское хозяйство / Agriculture 4.0	Строительство / Smart Construction	Транспорт и логистика / Smart Supply Chain	Торговля / E-Commerce
IoT, BDA, AI, Blockchain, Cloud	BDA, Blockchain, AI, Cloud	BDA, Blockchain, IoT, Cloud	IoT, Cloud	IoT, Cloud	BDA, IoT, Cloud	BDA, Cloud
PDM, MES ERP, CAD, CAE, CAPP, SSM, CRM, PLC / CALS, SCADA, CAM, KM, 3D, TQM, BPM, Rob	ERP, RPA, SSM, CRM, KM	ERP, SSM, CRM, SCADA, CAM, KM, BPM	PLC / CALS, AITS	BIM, KM, BPM, Rob	ERP, SSM, CRM, KM, BPM	ERP, SSM, CRM, PLC / CALS, KM

Примечание. 3D – аддитивные технологии и системы; AI – искусственный интеллект; AITS – система идентификации, регистрации, прослеживаемости животных и продукции животного происхождения; BDA – аналитика больших данных; BIM (Building Information Modeling) – системы информационного моделирования в области промышленного и гражданского строительства; BPM (Business Perfomance Managment) – процессное управление организацией; CAD, CAE (Computer-Aided Design; Computer-Aided Engineering) – системы цифрового проектирования и моделирования; CAPP (Computer-Aided Process Planning) – системы планирования производства; Cloud – облачное производство; ERP (Enterprise Resource Planning) – цифровая система планирования ресурсов предприятия; IoT – Интернет вещей; KM (Knowledge Management) – управление знаниями и навыками на различных уровнях управления; MES (Manufacturing Execution System) – цифровая система управления производственными процессами; PDM (Product Data Management) – системы управления инженерными данными; PLC / CALS (Product Life Cycle, Continuous Acquisitionand Lifecycle Support) – системы управления жизненным циклом промышленного продукта; SCADA, CAM (Supervisory Control And Data Acquisition, Computer-Aided Manufacturing) – системы автоматизации цеховых процессов; SSM, CRM – системы продажи и управления сервисом; SCM (Supply Chain Management) – системы управления цепочками поставок; TQM (Total Quality Managment) – модули общего управления качеством; Rob – робототехнические (роботизированные) системы и автоматы.

Важно отметить, что системы IoT [1] связаны при наличии реальных активов, объединенных в сети и контролируемых через Интернет, не только с экономическими или социальными рисками и угрозами, но и с физической безопасностью граждан. Таким образом, представляется возможным рассматривать данные технологии в разрезе киберфизической безопасности. Кроме того, системы IoT [2] являются гетерогенными по своей природе, что увеличивает сложность механизмов безопасности и конфиденциальности.

Для таких секторов, как промышленность, сельское хозяйство, энергетика (включая ядерную энергетику), логистика (включая транспортную инфраструктуру), городское управление, выделяют риски, связанные с внедрением технологий IoT, в том числе кибербезопасность, обеспечение конфиденциальности данных, отсутствие нормативных стандартов и, соответственно, несовместимость гетерогенных систем, лакуны в законодательном регулировании.

Кроме того, системы IoT в настоящее время обрабатываются централизованными облачными системами управления данными, что увеличивает их уязвимость, актуализируя проблематику целостности, конфиденциальности и доступности информационной защиты данных от несанкционированного доступа, изменения или удаления [16]. Существует риск безопасности прикладных приложений и промышленных облачных платформ в условиях ограниченности их полноценной изоляции от внешних сетей[1]. Внедрение облачных технологий в таких секторах, как банковский, телекоммуникаций, производственные предприятия, формирует следующий корпус угроз и рисков: безопасность используемого программного обеспечения, надежность инфраструктуры, обеспечение безопасности хранения цифровых данных, сетевая безопасность, гарантия анонимности данных, обеспечение целостности, конфиденциальности и доступности информации.

В целом следует отметить, что расширение открытого, взаимосвязанного и интеллектуального развития в производственной, сельскохозяйственной, транспортной, энергетической сферах, торговле и коммунальном хозяйстве сталкивается с серьезными проблемами безопасности [17].

Таблица 2

Уязвимости современных технологий, интегрированных в цифровые концепты (разработано автором на основе [3–16])

Показатель	Цифровые риски и угрозы в разрезе технологий				
	IoT	Cloud	AI	Big Data	Blockchain
Кибер-безопасность[2]	DDoS[3]	Потеря управления над отдельными блоками цифровых данных, передаваемых под контроль облачному провайдеру	Взлом и нарушение работы алгоритмов	Взлом и несанкционированный доступ к коммерчески чувствительной информации	Риски на уровне транзакций
	MC[4]	Уязвимость интерфейса управления	Принятие ошибочных решений системами в рамках FinTech, высокие потенциальные финансовые издержки		
	SC	Безопасность ПО, инфраструктуры, хранения, сети, среды облачных вычислений			
	Шпионаж				
Конфиденциальность	Отсутствие строгих правил в отношении сбора и использования данных	Генерирование рисков в области защиты данных для клиентов и поставщиков облачных услуг	–	Получение несанкционированного доступа к персональным данным	Использование общедоступных систем Blockchain не дает возможности полного контроля и конфиденциальности
	Отсутствие многофакторных моделей, обеспечивающих прозрачность и выполнение	Неполное удаление данных		Получение несанкционированного доступа к коммерческой информации	
	Ограниченные ресурсы для разработки IoT-устройств, разработанных в соответствии с реализацией принципов конфиденциальности	Скрытая идентификация, пробелы в процедурах повторной идентификации или деанонимизации		Получение несанкционированного доступа к государственным секретам	
	Отсутствие защиты данных, собираемых устройствами IoT				
Стандартизация	Отсутствие единых стандартов (различные стандарты IEEE, IETF, ITU, ISO, IEC, 3GPP)	Недостаточное количество инструментов, процедур, стандартных форматов данных или интерфейсов служб, которые могли бы гарантировать переносимость данных, приложений и услуг. Это может затруднить для клиента переход от одного поставщика к другому	–	–	Отсутствие общепризнанной стандартизации

Окончание табл. 2

Показатель	Цифровые риски и угрозы в разрезе технологий				
	IoT	Cloud	AI	Big Data	Blockchain
Совместимость	Отсутствие стандартов функциональной совместимости	–	–	–	–
	Отсутствие стандартных конфигураций для взаимодействия с большим количеством IoT-устройств				
Правовое регулирование	Отсутствие защиты информации в нормативных актах в сфере трансграничного обмена данными	–	Отсутствие защиты потребителей от использования манипулятивных AI-технологий	Отсутствие защиты конкурентной среды от попыток монополизации рынков за счет обладания эксклюзивной информацией Big Data	Распределенная природа приложений Blockchain, позволяющая охватывать несколько юрисдикций
	Отсутствие законодательства о дискриминационном использовании данных IoT		Отсутствие защиты работников и потребителей от внедрения AI со стороны корпораций		
	Отсутствие законодательства об использовании данных для борьбы с преступностью				

Примечание. DDoS – атаки систем IoT с помощью сети ботов; MC – вредоносный контроль над незащищенными элементами системы IoT; SC – сканирование системы IoT с помощью специального оборудования с целью кражи цифровых данных; шпионаж – использование уязвимости системы для проникновения в систему и кражи информации.

Технологические инновации способствуют интеграции Интернета и традиционных отраслей, подключению большого количества производственного оборудования и систем управления к сети. Сложность оцифрованных производственных (торговых, транспортных) сред фактически определяется наличием двух взаимосвязанных основных сетей: информационной и производственной (торговой, транспортной) [18]. Результирующие взаимосвязанности в оцифрованных средах создают увеличенную поверхность атаки и больше возможностей для их распространения.

Кибератака может распространяться по всей информационной сети и наносить значительный ущерб как информационной, так и производственной сети[5]. Таким образом, ущерб, вызванный кибератакой, не только снижает функциональность самого атакованного сетевого узла, но также может распространяться как в информационных, так и в производственных сетях из-за их взаимосвязанности. Кроме того, промышленные системы управления (ICS) традиционно функционировали в изолированных средах. С развитием информационных и коммуникационных технологий и функциональных требований все больше ICS переводятся в общедоступную сеть для обеспечения удаленного контроля и надзора за инфраструктурами [19]. Данный фактор увеличивает вероятность внешнего злонамеренного проникновения во внутренние системы управления предприятиями.

Тенденция внедрения интеллектуальных систем в энергетические системы (как на уровне интеллектуальных диспетчерских систем, так и систем управления) актуализировала проблематику рисков цифровизации для стабильного функционирования не только данного направления в секторальном разрезе, но и национальных экономик в целом. Smart Grid характеризуется быстрым двусторонним потоком информации между составными элементами сети, блоками генерации, передачи, распределения и потребителями[6] [20]. Распределенные гетерогенные энергогенерирующие мощности, гибкие нагрузки и внешние природные и антропогенные факторы влияют на безопасность и стабильную работу электрических сетей [21]. Важно отметить, что концепция Smart Grid предполагает цифровизацию основных четырех компонентов энергосистемы: энергогенерирующих мощностей, энергопередачи, распределения и конечного потребления, каждый из которых является уязвимым для разного вида внешних атак. Проведенное в 2016 г. исследование [22] о зарегистрированных атаках в США показало, что энергетическая инфраструктура являлась целью таких атак в 54% случаев [23].

Важно отметить, что электроэнергетика является составной частью критической национальной инфраструктуры, которая определяет стабильность функционирования жизненно важных сфер в контексте, в том числе экономической безопасности государства. Любая система может стать критической, когда уязвимости становятся угрозами, вызывающими различные виды разрушительного воздействия на социальные системы, энергетику, безопасность, здоровье населения и важные элементы общества[7]. Отказ инфраструктуры или недоступность услуг может привести к значительным разрушениям и оказать негативное влияние на промышленное производство, безопасность жизни и имущества[8] [24]. Данный сбой может распространиться на другие части, вызывая каскадные сбои во многих других связанных инфраструктурах с нарастающими негативными последствиями в экономике. В последние годы отмечается тенденция увеличения количества выявленных взломов систем управления критической инфраструктуры с целью вывода ее из строя либо шпионажа[9]. Реализация концепции Smart City сталкивается с угрозами безопасности под воздействием кибератак по причине хрупкости системы и широких возможностей для утечки данных [25, 26]. Кроме того, отмечается проблема информационных островов в случае расширения изоляции данных и несовместимости между различными системами и организациями[10] [25]. Intellectual Transport Systems (умные транспортные системы) [27] в рамках концепции Smart City становятся все более интеллектуальными благодаря цифровым технологиям. Транспортные средства, оснащенные системами компьютерного зрения, различными видами датчиков и камер, обмениваются друг с другом информацией в режиме реального времени. В этой связи целостность данных является основной проблемой безопасности, связанной с безопасностью интеллектуальной транспортной системы.

Дальнейшая цифровизация сектора телекоммуникаций выражается в росте мошеннических операций с использованием поддельных идентификационных данных (например, банков, налоговых органов) для совершения нежелательных звонков и отправления сообщений, что приводит к финансовым потерям[11] [28]. Одним из самых опасных с точки зрения потери финансовых ресурсов и затрагивающих как регулятора, так и поставщиков телекоммуникационных услуг является мошенничество с обходом или мошенничество с SIM Box[12]. Данный вид преступлений распространен в регионах или странах, где тарифы на международную связь значительно выше, чем местные звонки на стационарный или мобильный номер. Мошенники размещают устройство SIM Box, которое

позволяет перенаправлять вызовы от международного вызывающего абонента к вызываемому абоненту, маскируя звонок как происходящий с местных мобильных или телефонных фиксированных станций, таким образом, обходя сборы, уплачиваемые регулятору за международный / междугородний вызов.

Blockchain интегрируется как в традиционные отрасли на базе концепций Industry 4.0, Smart Grid, Smart Supply Chain и пр., так и главным образом в FinTech-индустрию. Среди рисков внедрения данной технологии выделяют плохую защиту криптовалютной индустрии, что создает потенциал для кражи криптовалютных активов пользователей, в особенности с применением специально разработанного вредоносного ПО [29]. Взломы как биржевых, так и криптовалютных кошельков стали более распространенными и масштабными как на уровне криптовалютных биржевых платформ[13], так и FinTech-организаций[14]. Согласно исследованию CipherTrace [30], в 2018 г. с биржевых площадок было похищено 950 млн долл. США (360% к уровню 2017 г.). В отличие от регулируемых бирж, на большинство криптобирж не распространяются обычные требования к достаточности капитала, предусмотренные финансовым регламентом [31]. Большинство криптобирж недостаточно капитализированы, и в случае нарушения безопасности эти биржи не покрываются страховкой и не имеют достаточных финансовых возможностей для покрытия потерь. По причине высокого инвестиционного риска и возможностей для мошенничества ряд юрисдикций, таких как Китай и Южная Корея, в 2017 г. запретили ICO. Согласно отчету Ernst & Young за декабрь 2017 г., из общего объема средств, привлеченных ICO в размере 4 млрд долл. США, около 10% похищены киберпреступниками [32].

Вместе с тем, как показали результаты исследования CipherTrace, в 2020 г. значительно сократилось число преступлений, связанных с криптовалютной индустрией [33]. Аналитики определили, что данный показатель снизился на 57% в 2020 г. Объем криминальных операций в криптосфере сократился ориентировочно до 1,9 млрд долл. США[15]. В 2019 г. незаконная деятельность составила 2,1% от всего объема транзакций с криптовалютой, или около 21,4 млрд долл. США переводов. Вместе с тем в 2020 г. доля незаконных операций с криптовалютой упала до 0,34%, или на 10 млрд долл. США в объеме транзакций [34].

Инструментарий банковских кибератак предполагает использование вредоносных программ (включая банковские троянские программы[16]) и различных специализированных форм кибератак (включая DDoS[17]), направленных на уязвимости системы онлайн-банкинга [35–38][18].

Так, согласно отчету «Лаборатории Касперского» за 2021 г. [39], выделяются следующие киберугрозы в банковской сфере:

1) перепродажа доступа к банковским системам[19];

2) атаки программ-вымогателей на банковские сети[20];

3) разработка специального программного обеспечения для атаки коммерческих VPN-провайдеров и устройств, работающих в инфраструктуре их клиентов. Кроме того, злоумышленники создавали микропрограммы для сканирования сетей и сбора данных;

4) заражение Интернет-банков троянцами[21];

5) атаки финансовых приложений, включая приложения криптовалютных бирж[22];

6) кража данных платежных карт[23];

7) вредоносное программное обеспечение для атак на POS-терминалы и банкоматы[24].

По данным Сбербанка России, ежедневно фиксируется более 100 кибератак на инфраструктуру и финансовые сервисы банка, совершается более 10 тыс. попыток мошенничества в отношении клиентов [40]. В 2021 г. зафиксирована «самая мощная в мире атака на финансовый сектор» распределенного типа DDoS на 12 крупных финансовых организаций России, а также процессинговые компании и Интернет-провайдеры. Для увеличения мощности атаки кибепреступниками использовалась инфраструктура IoT [41].

Согласно данным Центрального банка России, в II квартале 2021 г. объем операций без согласия клиентов вырос по сравнению с аналогичным периодом 2020 г. на 23%, при этом объем украденных средств превысил 3 млрд рос. руб. (рост на 38%) [42]. При этом среди типов цифровых атак доминируют атаки с элементами социальной инженерии и фишинговые атаки. Среди стран, подвергшихся значительным кибератакам в 2006–2020 гг., лидируют США, Великобритания, Индия, ФРГ и Южная Корея.

С учетом выявленных угроз и ограничений современных технологических решений на уровне отраслей интеграция цифровых концептов генерирует следующие риски (табл. 3).

Таким образом, с учетом специфики внедряемых цифровых систем на уровне отраслей представляется возможным сформировать следующую матрицу киберугроз в зависимости от секторов (см. табл. 4 на с. 37–41).

В настоящее время, как показал проведенный анализ, среди наиболее распространенных и опасных инструментов кибератак выделяют вредоносные программы (ВП), целевые кибератаки (APT) и DDoS-атаки.

Таблица 3

Риски и угрозы цифровизации на уровне отраслей (разработано автором на основе [1, 17, 18, 20, 21, 23, 25–27, 43–52])

Концепция	Промышленность	Финансовый сектор	Энергетика	Сельское хозяйство	Транспорт и логистика	Торговля	Коммунальное хозяйство
RGTS	–	Сбой по причине эндогенных или экзогенных факторов, который несет прямые финансовые убытки в банковском секторе	–	–	–	–	–
FinTech	–	Прямые финансовые потери от взлома и хищения криптоактивов криптобирж, мошенничество при ICO, кража персональных данных, цифровых данных платежных карт, атаки POS-терминалов и банкоматов	–	–	–	–	–
Industry 4.0	Кибератаки (DDoS), блокировка систем управления производством, кража (фальсификация) коммерческой информации (шпионаж), интеллектуальной собственности. Атаки на промышленное оборудование, включая роботов, приводят к росту рисков в отношении промышленных активов, финансовых показателей, бизнес-репутации, жизни и здоровья работников, пользователей[25] и потребителей[26]	–	–	–	Нарушение функциональной работы цепочек поставки[27]	Взлом коммерческой информации о покупателях продукции и поставщиках	–

Продолжение табл. 3

Концепция	Промышленность	Финансовый сектор	Энергетика	Сельское хозяйство	Транспорт и логистика	Торговля	Коммунальное хозяйство
Agriculture 4.0	–	–	–	Сбой систем, который может привести к прямым финансовым убыткам и сокращению сельскохозяйственного производства	–	–	–
Smart Grid	Дестабилизация энергетической системы, вызывающая каскадный негативный эффект в промышленности	–	Скоординированные кибератаки[28], которые могут одновременно нацеливаться на достаточное количество критически важного энергогенерирующего оборудования, чтобы вызвать каскадные эффекты и в конечном итоге привести к краху энергосистемы; атаки программ-вымогателей, которые препятствуют стабильной работе системы и осуществлению энергопередачи; кибератаки приводят к нарушению работы подстанций и прекращению обслуживания клиентов	–	–	–	–
Smart Supply Chain	Сбои систем транспорта и логистики, которые могут привести к срыву поставок, возможной остановке производства и финансовым убыткам	–	–	–	Сбои систем транспорта и логистики, приводящие к финансовым убыткам		–

Окончание табл. 3

Концепция	Промышленность	Финансовый сектор	Энергетика	Сельское хозяйство	Транспорт и логистика	Торговля	Коммунальное хозяйство
E-Commerce	–	–	–	–	–	Сбои систем, которые приведут к сокращению объемов торговли, прямым финансовым убыткам	–
Smart City	–	–	–	–	–	–	Кибератаки диспетчерских систем, которые приведут к сбоям в работе всей системы, нарушая целостность обмена информацией и конфиденциальность цифровых данных пользователей
Intellectual Transport Systems (VANET)	–	–	–	–	Изменение цифровых данных в автономных транспортных средствах, которое может привести не только к имущественному ущербу, но и физической угрозе для водителей и пешеходов[29]	–	–

Таблица 4

Эмпирические оценки рисков и угроз по основным видам кибератак по методологии CIA (разработано автором)

Название атаки	Узел атаки	Отрасль, сфера деятельности либо экономики	Уровень риска взлома и сопутствующего ущерба в работе предприятий		
			низкий	средний	высокий
АЗС – атака захвата сеанса, при которой злоумышленник влияет на сеанс связи между узлами / транспортными средствами	Системы IoT	Industry 4.0, Smart City, Intellectual Transport Systems, Smart Grid	–	–	+
АИЭЗ – атака на инфраструктуру электронного здравоохранения	Информационные системы	Здравоохранение	–	–	+
АИСИ – атака с использованием методов социальной инженерии	Личные данные клиентов и работников предприятий и организаций	Финансовая и страховая деятельность, сектор ИКТ, оптовая и розничная торговля, государственное управление и оборона, обязательное социальное обеспечение	–	+	–
АКИ – атака на критическую инфраструктуру	Информационные и производственные системы объектов критической инфраструктуры	Промышленность, энергетика, системы жизнеобеспечения, информационные и телекоммуникационные системы, банковская система, транспортная система, информационные системы органов государственного управления, здравоохранение	–	–	+
АП – атака через посредника (Man in the Middle) – предполагает размещение злоумышленника между двумя взаимодействующими законными узлами / транспортными средствами, подслушивает их связь и вводит ложную информацию или изменяет сообщение между ними	Системы IoT	Industry 4.0, Smart City, Intellectual Transport Systems, Smart Grid	–	–	+
АПР – атака на промышленных роботов	Системы управления оборудованием	Промышленность, Industry 4.0	–	–	+
АРИИ – атака раскрытия идентификационной информации – направлена на нарушение требований аутентификации и конфиденциальности	Базы данных	Банковский сектор, сектор ИКТ, органы государственного управления, системы здравоохранения, Smart City, Intellectual Transport Systems, E-Government	–	+	–
АЦП – атака цепочки поставок	Данные о поставщиках и клиентах	Промышленность, Industry 4.0, транспорт и логистика, Smart Supply Chain	–	+	–

Продолжение табл. 4

Название атаки	Узел атаки	Отрасль, сфера деятельности либо экономики	Уровень риска взлома и сопутствующего ущерба в работе предприятий		
			низкий	средний	высокий
АЧ – атака червоточины, при которой два вредоносных узла участвуют в сети для создания частного туннеля, называемого червоточиной, где первый вредоносный узел на одном конце передает данные второму вредоносному узлу на другом конце, что приводит к нарушению безопасности для пакетов	Системы IoT	Industry 4.0, Smart City, Intellectual Transport Systems	–	+	–
АЧД – атака черная дыра, при которой злоумышленник обманывает протокол маршрутизации, представляя себя как узел с кратчайшим путем к узлу назначения, таким образом, вместо того, чтобы полагаться на процесс обнаружения маршрута, все узлы начинают доверять поддельному маршруту, и в конечном итоге пакеты данных перехватываются вредоносным узлом	Системы IoT	Industry 4.0, Smart City, Intellectual Transport Systems, Smart Grid	–	+	–
ВП – вредоносные программы, такие как черви, вирусы, трояны, вымогатели, бэкдоры, шпионское ПО и т. д., – использовались мошенниками для организации атак на компьютерные системы с целью нарушения конфиденциальности, целостности передаваемых данных и доступности услуг, предлагаемых базовой инфраструктурой	Информационные системы, базы данных	Промышленность, энергетика, строительство, водоснабжение, финансовый сектор, сектор ИКТ, транспортный сектор, торговля, системы государственного управления, образование, здравоохранение, Smart City, Intellectual Transport Systems, CBDC, E-Government	–	–	+
ВБК / ВКК – взломы биржевых и криптовалютных кошельков	Инфраструктуры криптовалют	FinTech	+ Криптокошельки крипторынка	–	+ Криптокошельки CBDC

Продолжение табл. 4

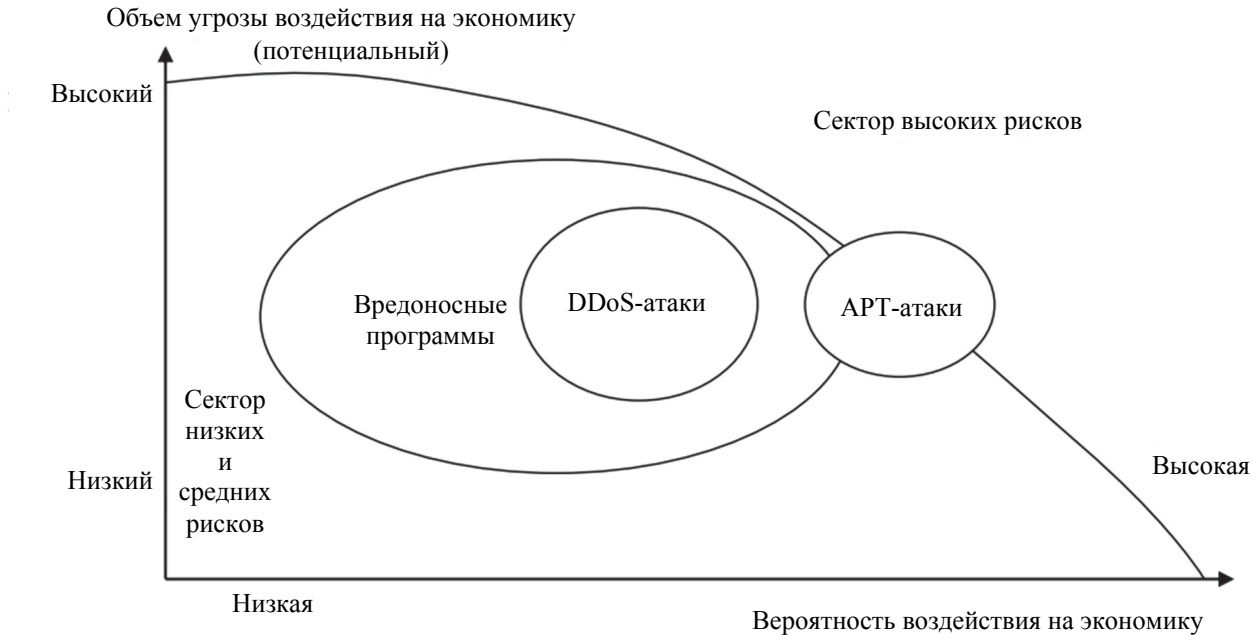
Название атаки	Узел атаки	Отрасль, сфера деятельности либо экономики	Уровень риска взлома и сопутствующего ущерба в работе предприятий		
			низкий	средний	высокий
ДТ – двойная трата – предполагает возможность пользователю выполнять несколько транзакций с одной и той же криптовалютой	Инфраструктуры криптовалют	FinTech	+	–	–
ИПИД – использование поддельных (краденых) идентификационных данных	Платежные, сервисные системы	FinTech, RTGS, банковский сектор, сектор ИКТ, цифровые системы государственного управления, E-Government	–	+	–
ККиС – коммерческий кибершпионаж и саботаж для получения коммерческих секретов и конкурентного преимущества	Базы данных	Промышленность, банковский сектор, сектор ИКТ, транспорт и логистика, торговля, Industry 4.0	–	+	–
Кр – криптоджекинг – предполагает несанкционированное использование чужих компьютеров для майнинга криптовалюты	Сетевое оборудование	FinTech	+	–	–
КЦД – кража цифровых (личных) данных, в том числе с использованием целевых кибератак	Базы данных	Промышленность, банковский сектор, сектор ИКТ, торговля, системы государственного управления, образование, здравоохранение, E-Government, Smart City, Intellectual Transport Systems, Industry 4.0, Smart Grid, FinTech	–	+	–
М – использование сервисов (миксеров), предназначенных для скрытия взаимосвязи между адресами в последовательных транзакциях, скрытия владельцев криптоактивов и их происхождения	Крипторынки	FinTech	+	–	–
МА – маскарадная атака – предполагает маскировку злоумышленником своей личности, чтобы действовать в качестве легитимного узла с намерением генерировать ложные сообщения в сети или модифицировать полученное сообщение	Системы IoT	Industry 4.0, Smart City, Intellectual Transport Systems, Smart Grid	–	+	–

Продолжение табл. 4

Название атаки	Узел атаки	Отрасль, сфера деятельности либо экономики	Уровень риска взлома и сопутствующего ущерба в работе предприятий		
			низкий	средний	высокий
MAP – атака маршрутизации – предполагает перехват сообщений в сети Blockchain	Инфраструктура Blockchain	FinTech	+	–	–
МО – мошеннические операции	Платежные системы и сервисы	Банковский сектор, FinTech, Smart Grid, E-Commerce, CBDC	+	–	–
MOSIM – мошенничество с обходом или мошенничество с SIM	Биллинговые системы	Сектор ИКТ	+	–	–
ПАТ – прослушивание и анализ трафика	Системы IoT	Smart City, Intellectual Transport Systems	+	–	–
ПВSCADA – программы взлома систем управления производством	Производственные системы	Промышленность, энергетика, водоснабжение, Smart Grid, Industry 4.0	–	–	+
ПИА – поддельная информационная атака, которая направлена на передачу ложной информации по сети	Системы IoT	Smart Supply Chain, Smart Grid, Industry 4.0, Smart City, Intellectual Transport Systems	–	+	–
ПУОИ – потеря управления при использовании облачной инфраструктуры	Облачная инфраструктура	Промышленность, энергетика, банковский сектор, сектор ИКТ, транспорт, торговля, системы государственного управления, здравоохранение, Industry 4.0, FinTech	–	–	+
УАИ – узловая атака имитации – направлена на нарушение аутентификации в сети	Системы IoT	Industry 4.0, Smart City, Intellectual Transport Systems, Smart Grid	–	+	–
УАСУ – удаленные атаки на системы управления трафиком с поддержкой Интернета вещей	Системы IoT	Industry 4.0, Smart City, Intellectual Transport Systems, Smart Grid	–	+	–
ФА(0) – фишинговая атака, целью которой является объект критической инфраструктуры	Сетевые системы, базы данных	Промышленность, энергетика, водоснабжение, финансовый сектор, сектор ИКТ, транспортный сектор, торговля, системы государственного управления, образование, здравоохранение, Industry 4.0, Smart City, Intellectual Transport Systems, Smart Grid	–	–	+
ФА(1) – фишинговая атака, целью которой является юридическое лицо			–	+	–
ФА(2) – фишинговая атака, целью которой является клиент юридического лица			+	–	–

Окончание табл. 4

Название атаки	Узел атаки	Отрасль, сфера деятельности либо экономики	Уровень риска взлома и сопутствующего ущерба в работе предприятий		
			низкий	средний	высокий
ЭУПО – эксплуатация уязвимостей ПО	Информационные системы	Промышленность, энергетика, водоснабжение, финансовый сектор, сектор ИКТ, транспортный сектор, торговля, системы государственного управления, образование, здравоохранение, Industry 4.0, Smart City, Intellectual Transport Systems, Smart Grid	–	+	–
APT – целевые кибератаки	Информационные системы	Промышленность, энергетика, водоснабжение, финансовый сектор, сектор ИКТ, системы государственного управления, здравоохранение, Industry 4.0, Smart City, Intellectual Transport Systems, Smart Grid	–	–	+
DDoS-атаки – атаки, генерирующие избыточный трафик, что препятствует доступу пользователей к ресурсу или услуге	Сетевые системы	Энергетика, финансовый сектор, сектор ИКТ, транспортный сектор, торговля, системы государственного управления, образование, здравоохранение, Industry 4.0, Smart City, Intellectual Transport Systems, Smart Grid	–	+	–
Eclipse – атака, которая предполагает изоляцию конкретного узла одноранговой сети с целью получения контроля всех исходящих соединений узла	Инфраструктура Blockchain	FinTech	+	–	–
GPS – атака, направленная на взлом управления положением транспортных средств с помощью имитаторов GPS, которые выдают более сильные сигналы, чем исходная спутниковая система GPS	Инфраструктура IoT	Smart City, Intellectual Transport Systems	+	–	–
Sybil – атака узла IoT, при которой используются несколько идентификаторов для компрометации основной части сети	Инфраструктура IoT, криптосфера	Smart City, Intellectual Transport Systems, FinTech	+	–	–



Матрица рисков на уровне экономики для различных киберинструментов (разработано автором)

1. Вредоносные программы, такие как черви, вирусы, трояны, вымогатели, бэкдоры, шпионское ПО и т. д., использовались мошенниками для организации атак на компьютерные системы с целью нарушения конфиденциальности, целостности передаваемых данных и доступности услуг, предлагаемых базовой инфраструктурой[30] [38, 53].

2. Целевые кибератаки[31] (APT) предполагают скрытое внедрение в ИТК-сектор организации, как правило, с целью кражи данных и промышленного шпионажа.

3. DDoS-атаки имеют целью отключение компьютерных систем или сетей[32] [63].

Специфика использования кибератак различного вида в отношении экономических, социальных и общественных объектов воздействия позволяет провести следующий сравнительный анализ их характеристик (табл. 5).

Используя методологию McKinsey [66], представляется возможным построить следующую матрицу рисков на уровне макроэкономики для различных инструментов киберпреступлений (рисунок). Как показано на рисунке, в секторе особых рисков для макроэкономики находятся все инструменты кибератак, одноко воздействие различается. Наибольшая вероятность ущерба и уязвимости объектов для стабильности национальной экономической системы исходит от APT-атак, нацеленных на наиболее крупные и значимые индивидуальные объекты инфраструктуры и управления.

DDoS-атаки ориентированы главным образом на специфические сегменты бизнеса и управления, поэтому на уровне компаний их воздействие не является критическим. Вместе с тем в случае атаки государственных инфраструктурных объектов и систем управления ущерб может быть серьезным (с учетом косвенных, репутационных и вторичных издержек). Вредоносные программы являются наиболее распространенным инструментом киберпреступлений, однако средняя вероятность прорыва систем защиты и отсутствие фокуса в отношении объектов воздействия делает этот инструментарий менее критическим, чем APT, но более значимым по сравнению с DDoS-атаками.

Заключение. Таким образом, риски цифровизации на базовом уровне отраслей и предприятий обусловлены, в том числе, внедрением технологий IoT, BDA, AI, Blockchain, Cloud, а также бизнес-операционных (производственных) систем. Для цифровых инноваций и метатехнологий, в том числе концепций Industry 4.0, Agriculture 4.0, Smart Grid, Smart Supply Chain, E-Commerce и Smart City, предполагается формирование оцифрованных сред в форме двух взаимосвязанных сетей: информационной и производственной. Результирующие взаимосвязи в оцифрованных производственных средах создают увеличенную поверхность атаки и больше возможностей для их распространения.

С учетом специфики внедряемых цифровых систем на уровне отраслей сформирована матрица секторальных киберугроз. Среди наиболее распространенных и опасных инструментов кибератак выделены вредоносные программы, целевые кибератаки и DDoS-атаки. Проведен сравнительный анализ характеристик различных данных киберинструментов с учетом их потенциальной направленности в отношении секторов и сегментов экономики, а также разработана матрица рисков на уровне экономики для различных киберинструментов.

Таблица 5

Сравнительный анализ характеристик различных киберинструментов и их потенциальной направленности по секторам и сегментам экономики (разработано автором)

Характеристики киберинструментов	Вредоносные программы	APT-атаки	DDoS-атаки
Уровень охвата атакуемых объектов	Широкий	Узкий	Широкий
Сегрегация по секторам и сегментам атаки	Низкая	Высокая	Средняя
Зависимость от наличия внутренних и / или внешних уязвимостей атакуемых объектов	Высокая	Специальная*	Низкая
Стоимость подготовки и реализации кибератаки	Низкая / средняя (в зависимости от конкретного инструмента)	Высокая	Высокая
Длительность предварительной подготовки	Низкая / средняя (в зависимости от конкретного инструмента)	Высокая	Средняя
Потенциальная направленность по секторам и сегментам экономики	Широкий спектр отраслей и сегментов экономики, в том числе компании сектора ИКТ, МСП, промышленные компании с низкой степенью киберзащиты и высокой степенью цифровизации бизнес-процессов, сектор государственного управления, медицинские учреждения, финансовые организации, образовательные учреждения, управление критической инфраструктурой	Узкий сектор наиболее защищенных в цифровом плане секторов и сегментов экономики, в том числе крупные ИТ-компании, банковские учреждения, органы государственного управления, промышленные предприятия сектора ВПК, управление критической инфраструктурой	Ограниченный перечень компаний, секторов и сегментов экономики, чьи бизнес-операции (специфика функционирования) предполагают необходимость нахождения онлайн в режиме 24 / 7, например сервисные услуги компаний, онлайн-сервисы органов государственного управления, компании ИКТ, медицинские учреждения и спасательные (специальные) службы

* Предполагает длительную детальную подготовку (разведку) с целью выявления уязвимостей систем или персональных данных.

[1]В 2020 г. производитель электроники Garmin стал жертвой вируса-вымогателя WastedLocker, который зашифровал внутреннюю сеть компании и некоторые производственные системы. В результате кибератаки были заблокированы функциональные операции внутренних сервисов, колл-центра, сайта и промышленного производства (http://cybersafety.ru/2020/07/russkie-hakery-evil-corp-paralizovali-proizvoditelya-umnyh-chasov-garmin/27/07/2020).

[2]По мнению Минобороны США, в настоящее время у производителей IoT-оборудования практически отсутствует стимул для разработки функций безопасности в программном обеспечении своих продуктов [4].

[3]В ботнете IoT различные скомпрометированные интеллектуальные объекты IoT, такие как камеры, датчики и носимые устройства, зараженные вредоносным ПО, позволяют злоумышленнику контролировать интеллектуальные объекты IoT для выполнения действий как в традиционном ботнете. Основное различие между традиционным ботнетом и бот-сетями IoT заключается в том, что в последнем случае зараженные устройства IoT продолжают распространять свое вредоносное ПО на многие другие устройства. Ботнет IoT имеет больший масштаб по сравнению с традиционным ботнетом. В 2016 г. в США была осуществлена DDoS-атака под названием «Mirai», в результате которой было заражено большое количество устройств IoT, включая видеорегистраторы и камеры видеонаблюдения. Эти скомпрометированные устройства затем использовались для инициирования DDoS-атак против поставщика услуг DNS «DYN» путем загрузки массива трафика данных в формате поисковых запросов DNS [56].

[4]При наличии уязвимостей программного обеспечения злоумышленник может получить действительный ключ сеанса или каким-либо образом перехватить сетевой трафик. Таким образом, злоумышленник может контролировать всю систему. Проведенный анализ трафика даркнета в мае 2018 г. выявил цифровые данные с более 129 тыс. уникальных устройств IoT, распределенных в 199 странах (основными из которых были Мексика (14%), Бразилия (12%), Китай (9%), Индонезия (5%), Россия (4%), США (4%), Вьетнам (4%)), размещенных в 43 различных секторах. Наиболее затронутыми секторами стали провайдеры Интернет-услуг, телекоммуникаций [12].

[5]По данным отраслевого регулятора Великобритании Make UK, в 2018 г. 24% британских производителей понесли финансовые или иные убытки в результате кибератак [57].

[6]Например, «умный» счетчик может передавать информацию с сайта клиента на компьютер поставщика услуг. Если этот поток информации должен осуществляться по беспроводной сети или через общедоступные сети, каналы данных, возможно, должны быть защищены. Данный массивный поток данных может представлять серьезные проблемы кибербезопасности.

[7]В 2013 г. была взломана плотина Боумен-авеню в Нью-Йорке (США), и хакерам удалось получить контроль над шлюзами. Исследования показали, что они могли легко изменить параметры, связанные с потоком воды, или даже изменить количество химических веществ, используемых при обработке воды, до катастрофического эффекта, что привело бы к разрушительным последствиям. В 2016 г. хакеры проникли в систему управления водоканала Kemuri Water Company (США) и изменили уровни химикатов, используемых для обработки водопроводной воды, манипулируя клапанами, контролирующими поток химикатов. В 2016 г. целенаправленная DDoS-атака отключила тепло и горячую воду в двух жилых домах Финляндии в середине финской зимы [23]. В 2018 г. по данным службы безопасности Украины, была осуществлена кибератака на станцию очистки воды ООО «Аульский хлорный завод» (обслуживает население в Украине, Молдове и Беларуси), организованная иностранным государством. При атаке использовалось вредоносное программное обеспечение VPNFilter, которое заразило не менее 500 тыс. маршрутизаторов и устройств IoT. Продолжение кибератаки могло привести к срыву технологических процессов и возможной аварии [58]. Эксперты «Ростелеком» обнаружили двукратный рост числа хакерских атак на стратегические предприятия в России в 2020 г. Киберпреступники, как правило, пытались завладеть почтой топ-менеджеров предприятий и перехватить контроль над инфраструктурой. Рост такого рода атак на стратегические предприятия обусловлен переходом на удаленную работу сотрудников и образованием уязвимостей в информационной инфраструктуре. Центр мониторинга и реагирования на кибератаки Solar JSOC компании «Ростелеком-Солар» за январь – ноябрь 2020 г. зафиксировал больше 200 профессиональных хакерских атак на российские компании (двукратный рост по сравнению с 2019 г.), в том числе 30 атак со стороны группировок наиболее высокого уровня, работающих на иностранные государства. Чаще всего профессиональные группировки пытались взломать объекты критической информационной инфраструктуры: банки, атомные предприятия, объекты здравоохранения, электроснабжения, военные объекты и организации государственного управления (https://www.kommersant.ru/doc/4593929). В мае 2021 г. крупнейшую трубопроводную компанию США Colonial Pipeline атаковала группа хакеров DarkSide. Washington Post считает, что DarkSide – это группа хакеров из Восточной Европы. Трубопровод Colonial Pipeline проходит по побережью Мексиканского залива на юг и восток США. Паника вокруг атаки вызвала нехватку газа на юго-востоке и повысила обеспокоенность о растущей угрозе программ-вымогателей (https://www.washingtonpost.com/business/2021/05/08/cyber-attack-colonial-pipeline/). Атака на крупнейшего переработчика мяса в США (компанию JBS) была совершена 30 мая 2021 г. Из строя были выведены пять мясоперерабатывающих заводов, которые обеспечивают 25% национальных поставок говядины и 20% свинины. Выведя из строя заводы, хакеры потребовали выкуп так же, как это было с атакой на Colonial Pipeline. По словам спикера Белого дома Карин Жан-Пьера, за атакой на JBS стоят, по всей видимости, российские хакеры (https://echo.msk.ru/news/2847776-echo.html).

[8]Неудачная кибератака на нефтехимический завод в Саудовской Аравии в августе 2017 г. была призвана не только сабботировать работу завода, но и вызвать взрыв, который мог привести к человеческим жертвам. Однако ошибка в компьютерном коде, использованном злоумышленниками, предотвратила взрыв. В октябре 2017 г. DDoS-атаки на транспортную сеть в Швеции привели к задержке движения поездов [23].

[9]По данным исследования компании «Ростелеком-Солар», каждая десятая критически значимая информационная инфраструктура в России скомпрометирована вредоносным ПО. Речь идет о госорганах, банках, оборонных и транспортных объектах (https://www.kommersant.ru/doc/4838304?tg).

[10]В Китае, где «умные города» начали развиваться после 2010 г., отмечена проблема обмена данными и интеграции. Например, в г. Нанкине из-за несовместимых форматов данных и стандартов между системами метро и автобусов местным органам власти пришлось понести дополнительные расходы в размере 100 млн юаней для их интеграции в рамках общей платежной системы.

[11]По данным Ассоциации по борьбе с мошенничеством в связи (Communications Fraud Control Association – CFCA), в телекоммуникационной отрасли по всему миру накоплено около 2,25 трлн долл. США убытков [59]. Нежелательные звонки или спам-звонки позволяют мошенникам зарабатывать более 38 млрд долл. США в год, что составляет около 1,69% общего дохода от телекоммуникаций. Основными категориями мошенничества в телекоммуникационных сетях являются: фальсификация SMS (0,8 млрд долл. США), фишинг и фарминг (1,6 млрд долл. США), атака обратного вызова (Вангири) (1,8 млрд долл. США).

[12]В результате мошенничества среднегодовые убытки составляют 4,3 млрд долл. США.

[13]Основанная в 2010 г. в Гонконге платформа обмена криптовалютами Bitfinex пострадала от серии кибератак, крупнейшая из которых привела к краже около 700 тыс. биткоинов в 2014 г. Это составило около 473 млн долл. США и является вторым по величине взломом обмена биткоинов. В декабре 2017 г. киберпреступники похитили биткоины на сумму около 70 млн долл. США у NiceHash – платформы для торговли цифровыми валютами, расположенной в Словении. В январе 2018 г. киберпреступники взломали биржу криптовалют Coincheck Inc. и похитили около 530 млн токенов NEM. В сентябре 2020 г. была взломана криптобиржа KuCoin, похищено более 150 млн долл. США в криптовалюте (https://whattonews.ru/vzlomana-kriptobirzha-kucoin-pohishheno-bolee-150-mln-v-kriptovaljute/). Российская криптовалютная биржа Livecoin в декабре 2020 г. объявила о своем закрытии после резкого прекращения операций. Биржа подверглась спланированной атаке, в результате которой она потеряла контроль над всеми своими серверами. В рамках инцидента хакерам удалось захватить инфраструктуру Livecoin и изменить цены на бирже до аномально высоких значений (https://cointelegraph.com/news/after-alleged-hack-russian-crypto-exchange-livecoin-shuts-down).

[14]DAO была основана как организация венчурного капитала на основе Ethereum, которая позволяла создавать и внедрять DApps (децентрализованные приложения) на своей платформе. В мае 2016 г. краудфандинг для DAO привлек более 150 млн долл. США. Программный изъян DAO позволил киберпреступникам украсть 50 млн долл. США.

[15]Например, в 2019 г. преступники совершили с цифровыми активами сделки на общую сумму до 4,5 млрд долл. США.

[16]TrickBot – первый и единственный банковский троян, предназначенный для клиентов крупных банков, которые охватывают множество географических и языковых зон по всему миру. Сначала TrickBot предназначался для финансовых учреждений, расположенных в Великобритании, Австралии и Швейцарии. В настоящее время операторы TrickBot проводят свои атаки перенаправления против банков в 19 разных странах [60].

[17]Финансовый ботнет – это распределенная сеть зараженных компьютеров, которой можно удаленно управлять с одного и того же сервера управления и контроля с целью атаки на финансовых клиентов [61].

[18]В результате кибератаки на банк JPMorgan Chase в 2016 г. было взломано около 76 млн учетных записей. DDoS-атака на HSBC в 2018 г. привела к двухдневному простою в системах онлайн-банкинга данного кредитного учреждения [62]. В 2021 г. мошенничество с Интернет-банкингом в Великобритании выросло на 117% по объему и на 43% по стоимости по сравнению с уровнем 2020 г. [38].

[19]Существует рынок предложений по удаленному доступу к различным банковским системам по всему миру. Как правило, киберпреступники получают доступ через уязвимости, а затем перепродают его злоумышленникам, преследующим свои финансовые интересы, например операторам программ-вымогателей.

[20]Различные группы вымогателей проводили целевые атаки на банки по всему миру, например в Коста-Рике, Чили и на Сейшельских островах. Эти три случая широко освещались в СМИ. За атаки в Коста-Рике несет ответственность группа Maze, а за атаками в Чили стояла группа REvil (Sodinokibi). При этом жертва нападения, заплатившая выкуп, не появляется в списке организаций, подвергшихся атаке.

[21]Примерами, подтверждающими данную тенденцию, являются такие программы, как Ginp, Ghimob, Anubis и Basbanke.

[22]Примером служит семейство Ghimob.

[23]Примером являются атаки Magecart 3.0.

[24]Группа Prilex, распространяющая вредоносное ПО по модели MaaS, начала перехватывать данные, которыми обмениваются платежные терминалы. Вредоносное программное обеспечение CESSO стало предоставляться как услуга для атак на банкоматы Diebold, Wincor и NCR и кражи денежных средств в евро, долларах США, валютах латиноамериканских стран.

[25]Аддитивное производство имеет ряд уязвимостей, связанных с технологией AM, усугубляемой ее цифровой природой, может потенциально позволить злонамеренным агентам вносить внутренние дефекты, такие как поры или внутренние геометрические неточности, ставя под угрозу механические и функциональные свойства продукта, без возможности их обнаружения традиционными методами квалификации [63]. В то же время очень важно учитывать потребности, связанные с задачами проектирования и проверки киберфизических систем [64].

[26]Механические детали внутри роботов, такие как захваты, двигатели, шестерни, колеса или поршни, которые позволяют роботам перемещать, захватывать и поднимать предметы, представляют серьезную угрозу, если ими управляют злоумышленники.

[27]Такие предприятия, как Fiat, Chrysler, T-Mobile USA, IRS, CVS, Costco, Бостонский медицинский центр и др., пострадали от кибератак по причине взлома их сторонних поставщиков.

[28]Кибератаки на критическую инфраструктуру классифицируются на четыре основных типа: атака на устройства, атака на цифровые данные, атака на конфиденциальность и сетевая атака [23, 47, 48]: а) атака на устройства направлена на компрометацию и управление сетевым устройством. Часто это начальный этап крупной атаки, когда одно взломанное устройство используется в качестве точки входа для запуска дальнейших атак и взлома остальной части интеллектуальной сети (например, скомпрометированный датчик может использоваться для отправки вируса, замаскированного под подлинные данные обнаружения, и, следовательно, распространения его по остальной части сети и заражения всей сети); б) атака на цифровые данные направлена на незаконное изменение или удаление цифровых данных или команды управления в трафике сети связи, чтобы ввести в заблуждение систему управления для принятия неправильных решений / действий (например, когда клиент манипулирует интеллектуальным счетчиком, чтобы изменить свои данные о потреблении, чтобы отразить меньшие суммы в своем счете за электроэнергию); в) атака на конфиденциальность направлена на извлечение персональной информации пользователей; г) сетевая атака, как правило, осуществляется в форме отказа в обслуживании (DoS) и

направлена на использование или перегрузку коммуникационных и вычислительных ресурсов сети критической инфраструктуры. В декабре 2015 г. хакерам удалось захватить контроль над подключенной системой управления энергосистемой Украины, успешно взломав систему надзора и сбора данных (supervisory control and data acquisition SCADA) сети с помощью вредоносного программного обеспечения BlackEnergy. Это вызвало массовое отключение электроэнергии, в результате которого более 700 тыс. человек остались без электричества на несколько часов [65]. В июле 2017 г. была атакована электрическая сеть, которая поставляет электроэнергию в Великобританию и Ирландию. Кибератака была направлена на проникновение в системы управления питанием, чтобы они могли отключить всю или часть электросети. Это было сделано с использованием поддельных электронных писем, предназначенных для некоторых старших сотрудников энергетической компании. Электронные письма содержали техническую информацию о Smart Grid, предназначенную для того, чтобы выдавать их за подлинную почту, но на самом деле предназначались для незаконной информации или для того, чтобы пользователи нажимали на ссылки для запуска вредоносного программного обеспечения в так называемой фишинг-атаке.

[29]В специализированной литературе [66, 67] кибератаки на системы VANET подразделяют на активные и пассивные в зависимости от их характера. Активные атаки – это те, в которых злоумышленник активно участвует в атаке для извлечения конфиденциальной информации из сети. В случае пассивной атаки злоумышленник пассивно собирает информацию о сети, не вмешиваясь в нее и не вводя какую-либо информацию в сеть. Раскрытие идентификационных данных является примером пассивной атаки.

[30]Отчет «Лаборатории Касперского» за 2015 г. показал, что из-за атак вредоносных программ за два года из финансовых учреждений всего мира было украдено до 1 млрд долл. США (http://25zbkz3k00wn2tp5092n6di7b5k.wpengine.netdna-cdn.com/files/2015/02/Carbanak_APT_eng.pdf). Количество вредоносных программ увеличилось на 358% в 2020 г., а количество программ-вымогателей возросло на 435%, при этом общая стоимость криптовалюты, полученная по адресам программ-вымогателей, увеличилась в 4 раза [38].

[31]Целевые кибератаки позволяют создавать возможности для достижения целей посредством различных векторов нападения (например, информационных, физических и обманных). Эти цели обычно включают установление и расширение своего присутствия внутри информационно-технологической инфраструктуры целевой организации для осуществления намерений извлечения информации, срыва или создания помех критическим аспектам выполняемой задачи, программы или службы.

[32]DoS – отказ в обслуживании; атаки DoS с происхождением из нескольких источников называются атаками распределенного отказа в обслуживании – DDoS.

Список литературы

1. The 5G business potential. Ericsson. Stockholm: Ericsson AB., 2017. 10 p. URL: https://www.terminsstarttelekom.se/upload/termin/pdf/pres475.pdf (date of access: 10.02.2019).

2. Securing IoTs in distributed Blockchain: Analysis, requirements and open issues / S. Moin [et al.] // Future Generation Computer Systems. 2019. No. 100. P. 32546–343. URL: https://doi.org/10.1016/j.future.2019.05.023 (date of access: 14.03.2019).

3. Singh S., Jeong Y.-S., Park J. A Survey on Cloud Computing Security: Issues, Threats, and Solutions // Journal of Network and Computer Applications. 2016. No. 75. P. 200–222. DOI: 10.1016/j.jnca.2016.09.002.

4. GAO. Internet of Things. Enhanced assessments and guidance are needed to address security risks. DOD United States Government Accountability Office Report to Congressional Committees. GAO-17-668. July 2017. URL: https://www.gao.gov/assets/690/686203.pdf (date of access: 17.08.2020).

5. Kumar N., Mallick P. Blockchain technology for security issues and challenges in IoT // International Conference on Computational Intelligence and Data Science (ICCIDS 2018). Procedia Computer Science. 2018. No. 132. P. 1815–1823. DOI: 10.1016/j.procs.2018.05.140.

6. Chatfield A., Reddick C. A framework for Internet of Things-enabled smart government: A case of IoT cybersecurity policies and use cases in U.S. federal government // Government Information Quarterly. 2018. No. 36 (2). P. 12. DOI: 10.1016/j.giq.2018.09.007.

7. Atlam H., Wills G. Intersections between IoT and distributed ledger // Advances in Computers. 2019. Vol. 115. P. 74–113. DOI: 10.1016/bs.adcom.2018.12.001.

8. Mylrea M. Smart energy-internet-of-things opportunities require smart treatment of legal, privacy and cybersecurity challenges // Journal of World Energy Law and Business. 2017. No. 10 (2). P. 147–158.

9. Tweneboah-Koduah S., Skouby K., Tadayoni R. Cybersecurity threats to IoT applications and service domains // Wireless Personal Communications. 2017. No. 95 (1). P. 169–185.

10. Zeadally S., Das A., Sklavos N. Cryptographic technologies and protocol standards for internet of things // Internet of Things. 2021. No. 14. P. 11. DOI: 10.1016/j.iot.2019.100075.

11. Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches / M. Hasan [et al.] // Internet of Things. 2019. No. 7. P. 14. DOI: 10.1016/j.iot.2019.100059.

12. Comprehending the IoT cyber threat landscape: A data dimensionality reduction technique to infer and characterize Internet-scale IoT probing campaigns / M. Pour [et al.] // Digital Investigation. 2019. No. 28. P. 40–49. DOI: 10.1016/j.diin.2019.01.014.

13. IoT architecture challenges and issues: Lack of standardization / S. Al-Qaseemi [et al.] // Proceedings of FTC 2016 – Future technologies conference 2016. United States. San Francisco, 2016. P. 731–738.

14. Hogan M., Piccarreta B. NIST interagency report (NISTIR) 8200, interagency report on status of international cybersecurity standardization for the Internet of Things (IoT). URL: https://csrc.nist.gov/publications/detail/nistir/8200/draft (date of access: 20.02.2022).

15. Minoli D., Occhiogrosso B. Blockchain mechanisms for IoT security // Internet of Things. 2018. No. 47-2. P. 1–13. DOI: 10.1016/j.iot.2018.05.002.

16. Tumpe M., Jagdev B. Investigating Security Issues in Cloud Computing // Complex, Intelligent and Software Intensive Systems (CISIS): Eighth International Conference IEEE. Birmingham, 2–4 July 2014. Birmingham, 2014. P. 141–146.

17. Edge computing: A survey / W. Khan [et al.] // Future Generation Computer Systems. 2019. No. 97. P. 219–235. DOI: 10.1016/j.future.2019.02.050 0167-739X.

18. Estimating the impact of IT security incidents in digitized production environments / O. Burger [et al.] // Decision Support Systems. 2019. No. 127 (10). P. 11. DOI: 10.1016/j.dss.2019.113144.

19. Asghar M., Hu Q., Zeadally S. Cybersecurity in industrial control systems: Issues, technologies, and challenges // Computer Networks. 2019. No. 165. P. 16. DOI: 10.1016/j.comnet.2019.106946.

20. Sorini A., Staroswiecki E. Cybersecurity for the smart grid // The Power Grid: Smart, Secure, Green and Reliable / edited by B. D'Andrade. Elsevier, 2017. P. 233–252. DOI: 10.1016/B978-0-12-805321-8.00008-2.

21. A review of machine learning for new generation smart dispatch in power systems / L. Yin [et al.] // Engineering Applications of Artificial Intelligence. 2020. No. 88. P. 12. DOI: 10.1016/j.engappai.2019.103372.

22. Impact of Cyber-Attacks on Critical Infrastructure / K. Thakur [et al.] // IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), High Performance and Smart Computing (HPSC) and Intelligent Data and Security (IDS). New York, April 2016. DOI: 10.1109/BigDataSecurity-HPSC-IDS.2016.22.

23. Kimani K., Oduol V., Langat K. Cyber Security Challenges for IoT-based Smart Grid Networks // International Journal of Critical Infrastructure Protection. 2019. No. 25. P. 18. DOI: 10.1016/j.ijcip.2019.01.001.

24. Tariq N., Asim M., Khan F. Securing SCADA-based Critical Infrastructures: Challenges and Open Issues // Procedia Computer Science. 2019. No. 155. P. 612–617. DOI: 10.1016/j.procs.2019.08.086.

25. Lam P., Ma R. Potential pitfalls in the development of smart cities and mitigation measures: An exploratory study // Cities. 2018. No. 91. P. 146–156. DOI: 10.1016/j.cities.2018.11.014.

26. Townsend A. Smart cities: Big data, civic hackers, and the quest for a new utopia. New York: WW Norton & Company, 2013. 400 p.

27. Doku R., Rawat D. Big Data in Cybersecurity for Smart City Applications // Smart Cities Cybersecurity and Privacy / edited by D. Rawat. 2019. P. 103–112. DOI: 10.1016/B978-0-12-815032-0.00008-1.

28. Consumer-facing technology fraud: Economics, attack methods and potential solutions / M. Ali [et al.] // Future Generation Computer Systems. 2019. No. 100. P. 408–427. DOI: 10.1016/j.future.2019.03.041.

29. Nian L., Lee D., Chuen K. Introduction to Bitcoin // Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data / edited by D. Lee. Elsevier, 2015. P. 6–30.

30. Cryptocurrency anti-money laundering report / CipherTrace. Cryptocurrency Intelligence. 2019. URL: https://ciphertrace.com/q4-2019-cryptocurrency-anti-money-laundering-report/ (date of access: 25.07.2020).

31. Falliere N., Murchu L., Chien E. W32.stuxnet. dossier. URL: https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf (date of access: 20.02.2021).

32. Chen K. Information asymmetry in initial coin offerings (ICOs): Investigating the effects of multiple channel signals // Electronic Commerce Research and Applications. 2019. Vol. 36 (4). P. 11. DOI: 10.1016/j.elerap.2019.100858.

33. Число преступлений, связанных с криптовалютами, снизилось на 57%. URL: https://coinspot.io/analysis/chislo-prestuplenij-svyazannyh-s-kriptovalyutami-snizilos-na-57/ (дата обращения: 18.08.2021).

34. Crypto Crime Report 2021. URL: https://go.chainalysis.com/2021-Crypto-Crime-Report.html (date of access: 03.04.2021).

35. A flow-based approach for Trickbot banking trojan detection / A. Gezer [et al.] // Computers & Security. 2019. No. 84. P. 179–192.

36. Szopinski T. Factors affecting the adoption of online banking in Poland // Journal of Business Research. 2016. No. 69 (11). P. 4763–4768. DOI: 10.1016/j.jbusres.2016.04.027.

37. Lopez P., Martin H. Hardware Trojans against virtual keyboards on e-banking platforms – A proof of concept // AEU-International Journal of Electronics and Communications. 2017. No. 76. P. 146–151. DOI: 10.1016/j.aeue.2017.04.003.

38. The Global Risks Report, 2022 / World Economic Forum. URL: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf (date of access: 19.01.2022).

39. Киберугрозы для финансовых организаций в 2021 году. Отчет Лаборатории Касперского GReAT от 1 декабря, 2020. URL: https://securelist.ru/cyberthreats-to-financial-organizations-in-2021/99420/ (дата обращения: 08.08.2022).

40. Мошенники не щадят банковских клиентов // Коммерсантъ. 2021. 9 июля. URL: https://www.kommersant.ru/doc/4897743?tg (дата обращения: 10.08.2021).

41. Буйлов М., Дементьева К., Степанова Ю. Интернет вещей пришел за деньгами. Российские банки отразили крупнейшую DDoS-атаку // Коммерсантъ. 2021. 3 сент. С. 7.

42. Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств / Банк России. URL: https://www.cbr.ru/analytics/ib/review_2q_2021/ (дата обращения: 08.10.2021).

43. Cyber attack models for smart grid environments / P. Eder-Neuhauser [et al.] // Sustainable Energy, Grids and Networks. 2017. 22 p. URL: http://dx.doi.org/10.1016/j.segan.2017.08.002 (date of access: 04.12.2019).

44. Bhardwaj A., Avasthi V., Goundar S. Cyber security attacks on robotic platforms // Network Security. 2019. October. P. 13–19. DOI: 10.1016/S1353-4858(19)30122-9.

45. Papakostas N., Newell A., Hargaden V. A novel paradigm for managing the product development process utilising blockchain technology principles // CIRP Annals – Manufacturing Technology. 2019. No. 68. P. 137–140.

46. Simon J., Omar A. Cybersecurity investments in the supply chain: Coordination and a strategic attacker // European Journal of Operational Research. 2020. Vol. 282 (1). P. 161–171. DOI: 10.1016/j.ejor.2019.09.017.

47. Ferrag M., Ahmim A. Security Solutions and Applied Cryptography in Smart Grid Communications. Hershey: PA. IGI Global, 2016. 464 p. DOI: 10.4018/978-1-5225-1829-7.

48. Securing Smart Grid: Cyber Attacks, Countermeasures, and Challenges / X. Li [et al.] // IEEE Communications Magazine. 2012. Vol. 50, no. 8. P. 38–45. DOI: 10.1109/MCOM.2012.6257525.

49. Kitchin R. Getting Smarter About Smart Cities: Improving Data Privacy and Data Security. Dublin; Ireland: Data Protection Unit: Department of the Taoiseach, 2016. 82 p.

50. McClure S., Scambray J., Kurtz G. Hacking exposed: Network security secrets and solutions. Berkeley; California: Osborne/McGraw-Hill, 2001. 703 p. URL: https://theswissbay.ch/pdf/Gentoomen%20Library/Security/Hacking%20Exposed-Network%20Security%20-%20Secrets%20%26%20Solutions%2C%202nd%20Ed.pdf (date of access: 23.02.2020).

51. Bailey T., Maruyama A., Wallance D. The energy-sector threat: How to address cybersecurity vulnerabilities // McKinsey Report. 2020. November. P. 12. URL: https://www.mckinsey.com/~/media/mckinsey/business%20functions/risk/our%20insights/the%20energy%20sector%20threat%20how%20to%20address%20cybersecurity%20vulnerabilities/the-energy-sector-threat-how-to-address-cybersecurity-vulnerabilities-f.pdf?shouldIndex=false (date of access: 11.12.2020).

52. Об утверждении перечня угроз безопасности, актуальных при обработке биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным физического лица в информационных системах организаций, осуществляющих идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц, за исключением единой информационной системы персональных данных, обеспечивающей обработку, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица, а также актуальных при взаимодействии государственных органов, органов местного самоуправления, индивидуальных предпринимателей, нотариусов и организаций, за исключением организаций финансового рынка, с указанными информационными системами, с учетом оценки возможного вреда, проведенной в соответствии с законодательством Российской Федерации о персональных данных, и учетом вида аккредитации организации из числа организаций, указанных в частях 18.28 и 18.31 статьи 14.1 Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»: приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 01.09.2021 № 902 // Официальный интернет-портал правовой информации. URL: http://publication.pravo.gov.ru/File/GetFile/0001202111030007?type=pdf (дата обращения: 07.01.2022).

53. Mahdavifar S., Ghorbani A. Application of deep learning to cybersecurity: A survey // Neurocomputing. 2019. No. 347. P. 149–176. URL: https://doi.org/10.1016/j.neucom.2019.02.056 0925-2312 (date of access: 05.11.2020).

54. Maestre V. Swarm and Evolutionary Computation. 2017. 15 p. URL: http://dx.doi.org/ 10.1016Zj.swevo.2017.07.002 (date of access: 25.03.2019).

55. Tirole J. Economics for the Common Good // Princeton University Press. 2017. 576 p. URL: https://gdsnet.org/Tirole2019FrontMatterChapt1.pdf (date of access: 04.12.2018).

56. PoRX: A reputation incentive scheme for blockchain consensus of IioT / E. Wang [et al.] // Future Generation Computer Systems. 2020. No. 102. P. 140–151. DOI: 10.1016/j.future.2019.08.005.

57. Heritage I. Protecting Industry 4.0: challenges and solutions as IT, OT and IP converge // Network Security. 2019. October. P. 6–9. DOI: 10.1016/S1353-4858(19)30120-5.

58. Mansfield-Devine S. Nation-state hacking threat to everyone // Computer Fraud & Security. 2018. August. P. 17–20. DOI:10.1016/S1361-3723(18)30077-0.

59. Communications Fraud Control Association (CFCA). Announces Results of Worldwide Telecom Fraud Survey. 2016. URL: https://goo.gl/H1VLae (date of access: 14.02.2019).

60. Kessem L., Widens T. Its attack scope in Spain, Brings redirection attacks to local banks. July 19, 2017. URL: https://securityintelligence.com/TrickBot-habla-espanol-trojan-widens-its-attack-scope-in-spain-brings-redirection-attacks-to-local-banks (date of access: 07.12.2018).

61. A taxonomy of botnet behavior, detection, and defense / S. Khattak [et al.] // IEEE Communications Survey & Tutorials. 2014. Vol. 16 (2). P. 898–924.

62. InsurTech and FinTech: Banking and Insurance Enablement / T. Yan [et al.] // Handbook of Blockchain, Digital Finance, and Inclusion. 2018. Vol. 1. P. 249–281. DOI: 10.1016/B978-0-12-810441-5.00011-7.

63. Cyber-physical Vulnerabilities in Additive Manufacturing Systems: A Case Study Attack on the STL file with human subjects / L. Sturm [et al.] // Journal of Manufacturing Systems. 2017. No. 44. P. 154–164.

64. Stark M., Kind S., Neumeyer S. Innovations in Digital Modelling for Next Generation Manufacturing System Design // CIRP Annals Manufacturing Technology. 2017. No. 66 (1). P. 169–172.

65. Lee R., Assante M., Conway T. Analysis of the Cyber Attack on the Ukrainian Power Grid / Electricity Information Sharing and Analysis Center. E-ISAC, 2016. URL: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2016/05/20081514/E-ISAC_SANS_Ukraine_DUC_5.pdf (date of access: 07.11.2017).

66. Sharma S., Kaushik B. A survey on internet of vehicles: Applications, security issues & solutions // Vehicular Communications. 2019. September. P. 1–44.

67. Manvi S., Tangade S. A survey on authentication schemes in VANETs for secured communication // Vehicular Communications. 2017. No. 9. P. 19–30.

References

1. The 5G business potential. Ericsson. Stockholm, Ericsson AB., 2017. 10 p. Available at: https://www.terminsstarttelekom.se/upload/termin/pdf/pres475.pdf (accessed 10.02.2019).

2. Moin S., Karim A., Safdar Z., Safdar K., Ahmed E., Imran M. Securing IoTs in distributed Blockchain: Analysis, requirements and open issues. *Future Generation Computer Systems*, 2019, no. 100, pp. 32549–343. Available at: https://doi.org/10.1016/j.future.2019.05.023 (accessed 14.03.2019).

3. Singh S., Jeong Y.-S., Park J. A Survey on Cloud Computing Security: Issues, Threats, and Solutions. *Journal of Network and Computer Applications*, 2016, no. 75, pp. 200–222. DOI: 10.1016/j.jnca.2016.09.002.

4. GAO. Internet of Things. Enhanced assessments and guidance are needed to address security risks. DOD United States Government Accountability Office Report to Congressional Committees. GAO-17-668. July 2017. Available at: https://www.gao.gov/assets/690/686203.pdf (accessed 17.08.2020).

5. Kumar N., Mallick P. Blockchain technology for security issues and challenges in IoT. *International Conference on Computational Intelligence and Data Science (ICCIDS 2018). Procedia Computer Science*, 2018, no. 132, pp. 1815–1823. DOI: 10.1016/j.procs.2018.05.140.

6. Chatfield A., Reddick C. A framework for Internet of Things-enabled smart government: A case of IoT cybersecurity policies and use cases in U.S. federal government. *Government Information Quarterly*, 2018, no. 36 (2), p. 12. DOI: 10.1016/j.giq.2018.09.007.

7. Atlam H., Wills G. Intersections between loT and distributed ledger. *Advances in Computers*, 2019, vol. 115, pp. 74–113. DOI: 10.1016/bs.adcom.2018.12.001.

8. Mylrea M. Smart energy-internet-of-things opportunities require smart treatment of legal, privacy and cybersecurity challenges. *Journal of World Energy Law and Business*, 2017, no. 10 (2), pp. 147–158.

9. Tweneboah-Koduah S., Skouby K., Tadayoni R. Cybersecurity threats to IoT applications and service domains. *Wireless Personal Communications*, 2017, no. 95 (1), pp. 169–185.

10. Zeadally S., Das A., Sklavos N. Cryptographic technologies and protocol standards for internet of things. *Internet of Things*, 2021, no. 14, p. 11. DOI: 10.1016/j.iot.2019.100075.

11. Hasan M., Islam M., Zarif I., Hashem M. Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches. *Internet of Things*, 2019, no. 7, p. 14. DOI: 10.1016/j.iot.2019.100059.

12. Pour M., Bou-Harb E., Varma K., Neshenko N., Pados D., Choo K.-K. Comprehending the IoT cyber threat landscape: A data dimensionality reduction technique to infer and characterize Internet-scale IoT probing campaigns. *Digital Investigation*, 2019, no. 28, pp. 40–49. DOI: 10.1016/j.diin.2019.01.014.

13. Al-Qaseemi S., Almulhim H., Almulhim M., Chaudhry S. IoT architecture challenges and issues: Lack of standardization. *Proceedings of FTC 2016 – Future technologies conference 2016.* United States, San Francisco, 2016, pp. 731–738.

14. Hogan M., Piccarreta B. NIST interagency report (NISTIR) 8200, interagency report on status of international cybersecurity standardization for the Internet of Things (IoT). Available at: https://csrc.nist.gov/publications/detail/nistir/8200/draft (accessed 20.02.2022).

15. Minoli D., Occhiogrosso B. Blockchain mechanisms for IoT security. *Internet of Things*, 2018, no. 47-2, pp. 1–13. DOI: 10.1016/j.iot.2018.05.002.

16. Tumpe M., Jagdev B. Investigating Security Issues in Cloud Computing. *Complex, Intelligent and Software Intensive Systems (CISIS): Eighth International Conference IEEE*. Birmingham, 2014, pp. 141–146.

17. Khan W., Ahmed E., Hakak S., Yaqoob I., Ahmed A. Edge computing: A survey. *Future Generation Computer Systems*, 2019, no. 97, pp. 219–235. DOI: 10.1016/j.future.2019.02.050 0167-739X.

18. Burger O., Hackel B., Karnebogen P., Toppel J. Estimating the impact of IT security incidents in digitized production environments. *Decision Support Systems*, 2019, no. 127 (10), p. 11. DOI: 10.1016/j.dss.2019.113144.

19. Asghar M., Hu Q., Zeadally S. Cybersecurity in industrial control systems: Issues, technologies, and challenges. *Computer Networks*, 2019, no. 165, p. 16. DOI: 10.1016/j.comnet.2019.106946.

20. Sorini A., Staroswiecki E. Cybersecurity for the smart grid. *The Power Grid: Smart, Secure, Green and Reliable*; edited by B. D'Andrade. Elsevier, 2017, pp. 233–252. DOI: 10.1016/B978-0-12-805321-8.00008-2.

21. Yin L., Gao Q., Zhao L., Zhang B., Wang T., Li S., Liu H. A review of machine learning for new generation smart dispatch in power systems. *Engineering Applications of Artificial Intelligence*, 2020, no. 88, p. 12. DOI: 10.1016/j.engappai.2019.103372.

22. Thakur K., Ali M., Jiang N., Qiu M. Impact of Cyber-Attacks on Critical Infrastructure. *IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), High Performance and Smart Computing (HPSC) and Intelligent Data and Security (IDS)*. New York, 2016. DOI: 10.1109/ BigDataSecurity-HPSC-IDS.2016.22.

23. Kimani K., Oduol V., Langat K. Cyber Security Challenges for IoT-based Smart Grid Networks. *International Journal of Critical Infrastructure Protection*, 2019, no. 25, p. 18. DOI: 10.10167j.ijcip.2019.01.001.

24. Tariq N., Asim M., Khan F. Securing SCADA-based Critical Infrastructures: Challenges and Open Issues. *Procedia Computer Science*, 2019, no. 155, pp. 612–617. DOI: 10.1016/j.procs.2019.08.086.

25. Lam P., Ma R. Potential pitfalls in the development of smart cities and mitigation measures: An exploratory study. *Cities*, 2018, no. 91, pp. 146–156. DOI: 10.1016/j.cities.2018.11.014.

26. Townsend A. Smart cities: Big data, civic hackers, and the quest for a new utopia. New York, WW Norton & Company, 2013. 400 p.

27. Doku R., Rawat D. Big Data in Cybersecurity for Smart City Applications. *Smart Cities Cybersecurity and Privacy*; edited by D. Rawat. 2019, pp. 103–112. DOI: 10.1016/B978-0-12-815032-0.00008-1.

28. Ali M., Azad M., Centeno M., Hao F., van Moorsel A. Consumer-facing technology fraud: Economics, attack methods and q potential solutions. *Future Generation Computer Systems*, 2019, no. 100, pp. 408–427. DOI: 10.1016/j.future.2019.03.041.

29. Nian L., Lee D., Chuen K. Introduction to Bitcoin. *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data*; edited by D. Lee. Elsevier, 2015, pp. 6–30.

30. Cryptocurrency anti-money laundering report. 2019. Available at: https://ciphertrace.com/q4-2019-cryptocurrency-anti-money-laundering-report/ (accessed 25.07.2020).

31. Falliere N., Murchu L., Chien E. W32.stuxnet. dossier. Available at: https://www.symantec.com/ content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf (accessed 20.02.2021).

32. Chen K. Information asymmetry in initial coin offerings (ICOs): Investigating the effects of multiple channel signals. *Electronic Commerce Research and Applications*, 2019, vol. 36 (4), p. 11. DOI: 10.1016/j.elerap.2019.100858.

33. The number of crimes related to cryptocurrencies has decreased by 57%. Available at: https://coinspot.io/analysis/chislo-prestuplenij-svyazannyh-s-kriptovalyutami-snizilos-na-57/ (accessed 18.08.2021) (In Russian).

34. Crypto Crime Report 2021. Available at: https://go.chainalysis.com/2021-Crypto-Crime-Report.html (accessed 03.04.2021).

35. Gezer A., Warner G., Wilson C., Shrestha P. A flow-based approach for Trickbot banking trojan detection. *Computers & Security*, 2019, no. 84, pp. 179–192.

36. Szopinski T. Factors affecting the adoption of online banking in Poland. *Journal of Business Research*, 2016, no. 69 (11), pp. 4763–4768. DOI: 10.1016/j.jbusres.2016.04.027.

37. Lopez P., Martin H. Hardware Trojans against virtual keyboards on e-banking platforms – A proof of concept. *AEU-International Journal of Electronics and Communications*, 2017, no. 76, pp. 146–151. DOI: 10.1016/j.aeue.2017.04.003.

38. The Global Risks Report, 2022. Available at: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf (accessed 19.01.2022).

39. Cyber Threats for Financial Organizations in 2021. Report of Kaspersky Lab. Available at: https://securelist.ru/cyberthreats-to-financial-organizations-in-2021/99420/ (accessed 08.08.2022) (In Russian).

40. Scammers have no mercy to bank customers. *Kommersant"* [Kommersant], 2021, 9 July. Available at: https://www.kommersant.ru/doc/4897743?tg (accessed 10.08.2021) (In Russian).

41. Buylov M., Dement'eva K., Stepanova Yu. The Internet of Things came for money. Russian banks reflected the largest DDoS attack. *Kommersant"* [Kommersant], 2021, 3 September, p. 7 (In Russian).

42. Reporting review on information security incidents when transferring funds. Available at: https://www.cbr.ru/analytics/ib/review_2q_2021/ (accessed 08.10.2021) (In Russian).

43. Eder-Neuhauser P., Zseby T., Fabini J., Vormayr G. Cyber attack models for smart grid environments. *Sustainable Energy, Grids and Networks*, 2017, 22 p. Available at: http://dx.doi.org/10.1016/j.segan.2017.08.002 (accessed 04.12.2019).

44. Bhardwaj A., Avasthi V., Goundar S. Cyber security attacks on robotic platforms. *Network Security*, 2019, October, pp. 13–19. DOI: 10.1016/S1353-4858(19)30122-9.

45. Papakostas N., Newell A., Hargaden V. A novel paradigm for managing the product development process utilising blockchain technology principles. *CIRP Annals – Manufacturing Technology*, 2019, no. 68, pp. 137–140.

46. Simon J., Omar A. Cybersecurity investments in the supply chain: Coordination and a strategic attacker. *European Journal of Operational Research*, 2020, vol. 282 (1), pp. 161–171. DOI: 10.1016/j.ejor.2019.09.017.

47. Ferrag M., Ahmim A. Security Solutions and Applied Cryptography in Smart Grid Communications. Hershey, PA. IGI Global, 2016. 464 p. DOI: 10.4018/978-1-5225-1829-7.

48. Li X., Liang X., Lu R., Shen X., Lin X., Zhu H. Securing Smart Grid: Cyber Attacks, Countermeasures, and Challenges. *IEEE Communications Magazine*, 2012, vol. 50, no. 8, pp. 38–45. DOI: 10.1109/MCOM.2012.6257525.

49. Kitchin R. Getting Smarter About Smart Cities: Improving Data Privacy and Data Security. Dublin, Ireland, Data Protection Unit, Department of the Taoiseach, 2016. 82 p.

50. McClure S., Scambray J., Kurtz G. Hacking exposed: Network security secrets and solutions. Berkeley, California, Osborne/McGraw-Hill, 2001. 703 p. Available at: https://theswissbay.ch/pdf/Gentoomen%20Library/Security/Hacking%20Exposed-Network%20Security%20-%20Secrets%20%26%20Solutions%2C%202nd%20Ed.pdf (accessed 23.02.2020).

51. Bailey T., Maruyama A., Wallance D. The energy-sector threat: How to address cybersecurity vulnerabilities. *McKinsey Report*, 2020, November, p. 12. Available at: https://www.mckinsey.com/~/media/mckinsey/business%20functions/risk/our%20insights/the%20energy%20sector%20threat%20how%20to%20address%20cybersecurity%20vulnerabilities/the-energy-sector-threat-how-to-address-cybersecurity-vulnerabilities-f.pdf?shouldIndex=false (accessed 11.12.2020).

52. On approval of a list of security threats that are relevant in the processing of biometric personal data, their verification and transmission of information on the degree of compliance with the physical biometric personal information provided by the biometric personal data in the information systems of organizations carrying out identification and / or authentication with the use of biometric personal data of physical persons, with the exception of a unified information system for personal data, including the collection and storage of biometric personal data, their verification and transmission of information about the degree of their compliance with the physical person provided by biometric personal data, as well as relevant in the interaction of state bodies, local governments, individual entrepreneurs, notaries and organizations, with the exception of the organizations of the financial market, with the indicated information systems, taking into account the assessment of possible harm conducted in accordance with the laws of the Russian Federation of personal data, and taking into account the type of accreditation of an organization among the organizations referred to in parts of 18.28 and 18.31 of Article 14.1 of the Federal Law of July 27, 2006 No. 149-FZ "On information, information technologies and information protection": Order of the Ministry of digital development, communications and mass communications of the Russian Federation of 01.09.2021 No. 902. *Official Internet portal of legal information*. Available at: http://publication.pravo.gov.ru/File/GetFile/0001202111030007?type=pdf (accessed 07.01.2022) (In Russian).

53. Mahdavifar S., Ghorbani A. Application of deep learning to cybersecurity: A survey. *Neurocomputing*, 2019, no. 347, pp. 149–176. Available at: https://doi.org/10.1016/j.neucom.2019.02.056 0925-2312 (accessed 05.11.2020).

54. Maestre V. Swarm and Evolutionary Computation. 2017. 15 p. Available at: http://dx.doi.org/10.1016Zj.swevo.2017.07.002 (accessed 25.03.2019).

55. Tirole J. Economics for the Common Good. *Princeton University Press*, 2017. 576 p. Available at: https://gdsnet.org/Tirole2019FrontMatterChapt1.pdf (accessed 04.12.2018).

56. Wang E., Liang Z., Chen C.-M., Kumari S., Khan M. PoRX: A reputation incentive scheme for blockchain consensus of IioT. *Future Generation Computer Systems*, 2020, no. 102, pp. 140–151. DOI: 10.1016/j.future.2019.08.005.

57. Heritage I. Protecting Industry 4.0: challenges and solutions as IT, OT and IP converge. *Network Security*, 2019, October, pp. 6–9. DOI: 10.1016/S1353-4858(19)30120-5.

58. Mansfield-Devine S. Nation-state hacking threat to everyone. *Computer Fraud & Security*, 2018, August, pp. 17–20. DOI:10.1016/S1361-3723(18)30077-0.

59. Communications Fraud Control Association (CFCA). Announces Results of Worldwide Telecom Fraud Survey. 2016. Available at: https://goo.gl/H1VLae (accessed 14.02.2019).

60. Kessem L., Widens T. Its attack scope in Spain, Brings redirection attacks to local banks. July 19, 2017. Available at: https://securityintelligence.com/TrickBot-habla-espanol-trojan-widens-its-attack-scope-in-spain-brings-redirection-attacks-to-local-banks (accessed 07.12.2018).

61. Khattak S., Ramay N., Khan K., Syed A., Khayam S. A taxonomy of botnet behavior, detection, and defense. *IEEE Communications Surveys & Tutorials*, 2014, vol. 16 (2), pp. 898–924.

62. Yan T., Schulte P., Lee D., Chuen K. InsurTech and FinTech: Banking and Insurance Enablement. *Handbook of Blockchain, Digital Finance, and Inclusion*, 2018, vol. 1, pp. 249–281. DOI: 10.1016/B978-0-12-810441-5.00011-7.

63. Sturm L., Williams C., Camelio J., White J., Parker R. Cyber-physical Vulnerabilities in Additive Manufacturing Systems: A Case Study Attack on the STL file with human subjects. *Journal of Manufacturing Systems*, 2017, no. 44, pp. 154–164.

64. Stark M., Kind S., Neumeyer S. Innovations in Digital Modelling for Next Generation Manufacturing System Design. *CIRP Annals Manufacturing Technology*, 2017, no. 66 (1), pp. 169–172.

65. Lee R., Assante M., Conway T. Analysis of the Cyber Attack on the Ukrainian Power Grid. 2016. Available at: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2016/05/20081514/E-ISAC_SANS_Ukraine_DUC_5.pdf (accessed 07.11.2017).

66. Sharma S., Kaushik B. A survey on internet of vehicles: Applications, security issues & solutions. *Vehicular Communications*, 2019, September, pp. 1–44.

67. Manvi S., Tangade S. A survey on authentication schemes in VANETs for secured communication. *Vehicular Communications*, 2017, no. 9, pp. 19–30.

Информация об авторе

Криштаносов Виталий Брониславович – кандидат экономических наук, докторант Белорусского государственного технологического университета (220006, г. Минск, ул. Свердлова, 13а, Республика Беларусь). E-mail: Krishtanosov@mail.ru

Information about the author

Kryshtanosau Vitaly Bronislavovich – PhD (Economics), post-doctoral student. Belarusian State Technological University (13a, Sverdlova str., 220006, Minsk, Republic of Belarus). E-mail: Krishtanosov@mail.ru

Поступила 28.02.2022