УДК 330.341

В. Б. Криштаносов
Белорусский государственный технологический университет

МЕТОДОЛОГИЯ ОЦЕНКИ И УПРАВЛЕНИЯ ЦИФРОВЫМИ РИСКАМИ

Выявлены основные подходы к оценке рисков, связанных с внедрением современных технологий, приведен анализ подходов к управлению рисками как на уровне предприятия, так и государства в целом, дана характеристика и выделена специфика качественных и количественных методов оценки цифровых угроз. Обоснована необходимость разработки международных стандартов управления цифровыми рисками. Приведены методы оценки OCTAVE, STRIDE и CIA. Предложена классификация экономических затрат, связанных с кибератаками, выделены факторы, влияющие на возникновение (усиление) новых цифровых рисков. Даны оценки современным стратегиям, разработанным для снижения рисков и эффективного реагирования на инциденты, связанные с рисками. Выявлены наиболее распространенные киберугрозы в динамике их распространения.

Ключевые слова: методология оценки рисков, управление рисками, риски цифровизации, киберпреступления, OCTAVE, STRIDE и CIA.

Для цитирования: Криштаносов В. Б. Методология оценки и управления цифровыми рисками // Труды БГТУ. Сер. 5, Экономика и управление. 2021. № 2 (250). С. 15–36.

V. B. Kryshtanosau
Belarusian State Technological University

METHODOLOGY FOR ASSESSMENT AND MANAGEMENT OF DIGITAL RISKS

There were identified the main approaches to assessing the risks associated with the implementation of modern technologies, were given analysis of approaches to risk management both at the level of the enterprise and the state and a characteristic and highlighted the specifics of qualitative and quantitative methods for assessing digital threats. It has been substantiated the necessity of developing international standards for digital risk management. There were given methods for risk evaluating: OCTAVE, STRIDE and CIA. There were carried out classification of the economic costs associated with cyber attacks, and the factors influencing the emergence (strengthening) of new digital risks were highlighted. There were given assessments to the modern strategies developed to reduce risks and effectively respond to incidents associated with risks. There have been identified the most common cyber threats in the dynamics of their spread.

Key words: risk assessment methodology, risk management, digitalization risks, cybercrime, OCTAVE, STRIDE and CIA.

For citation: Kryshtanosau V. B. Methodology for assessment and management of digital risks. *Proceedings of BSTU, issue 5, Economics and Management*, 2021, no. 2 (250), pp. 15–36 (In Russian).

Введение. В условиях высокой динамики внедрения цифровых технологий в традиционных отраслях, а также формирования новых цифровых сегментов осуществляется интенсивная трансформация технологических, управленческих и бизнес-подходов в современной экономике. В данном контексте значительно вырастают риски, связанные не только со стабильным развитием макро- и микроэкономических систем в цифровой экосистеме, но и их уязвимостью в условиях роста кибератак, угроз национальной безопасности в сфере критической инфраструктуры и пр. В этой связи представляется важным выделить риски, связанные с цифровизацией экономики, классифицировать их по степени вероятности и потенциалу возможного ущерба как на уровне предприятия, так и страны в целом, а также рассмотреть наиболее эффективные механизмы управления цифровыми рисками.

Разработка эффективных механизмов прогнозирования потенциальных угроз цифровизации различных сфер экономики является важнейшей задачей, позволяющей в дальнейшем оптимизировать финансовые, людские и технологические ресурсы предприятия / страны / интеграционной группировки / международного сообщества для управления рисками с целью нивелирования возможного ущерба киберугроз и восстановления стабильного развития экономических систем на различных уровнях в максимально короткие сроки.

Концепция риска претерпела ряд трансформаций[1] и в настоящее время отражает ряд контекстов, включая предпринимательский,

социальный, экономический, безопасности, инвестиционный, военный, политический и т. д. [1].

На международном уровне принят стандарт ISO 31000, который определяет риск как влияние неопределенности на цели и выражается в виде сочетания последствий события (включая изменение обстоятельств) и связанной с этим вероятности возникновения [2]. Согласно классическому определению Британского института стандартов, риск рассчитывается как «комбинация вероятности или частоты возникновения определенной опасности и величины последствий этого события» [3].

Международный совет по управлению рисками (IRGC) выделяет риски системного характера, которые обычно охватывают более одной страны, более одного сектора экономики и могут оказывать влияние на природные, технологические и социальные системы [4]. Эти риски могут быть относительно редкими по вероятности наступления, но иметь глубокие последствия для безопасности, экономической и социальной стабильности. В этой связи, как показано в табл. 1, IRGC определяет три категории возникающих рисков, связанных с технологиями:

– неопределенного воздействия;

– системного воздействия;

– неожиданного воздействия.

Руан [1] рассматривает риски управления на уровне предприятия (Enterprise Risk Management – ERM) как в микроэкономическом, так и макроэкономическом разрезах, выделяя следующие их разновидности: стратегический, кредитный, операционный, регуляторный, рыночный и системный.

Ряд исследователей [5] различают на уровне управления предприятием эндогенные и экзогенные риски. К эндогенным рискам относятся:

1) риски, которые связаны с организационной сетью, в том числе любые неопределенности, возникающие в результате взаимодействия между организациями в рамках бизнес-экосистемы;

2) риски, связанные с бизнес-процессами, такими как сбои во внутренних операциях (продукт / услуга, процесс / контроль), материальный поток, финансовый поток и информационный поток, а также риски, связанные с принятием решений;

3) риски, связанные с цепочкой поставок, в том числе риски со стороны предложения / спроса, такие как банкротство поставщика, сбои распределенных или транспортных поставщиков, и т. д.;

4) риски, связанные с безопасностью, в том числе злонамеренные угрозы (преднамеренные и непреднамеренные, такие как кража, саботаж, промышленный шпионаж, кибератака и т. д.), а также сбои в инфраструктуре, включая ИТ, и финансовые риски.

Экзогенные риски классифицируются:

– на риски, связанные с окружающей средой в целом, которые возникают в результате взаимодействия бизнес-экосистемы с окружающей средой;

– стихийные бедствия, такие как эпидемические заболевания, ураганы, наводнения, торнадо и т. д.;

– социально-экономические риски, такие как политические риски (эмбарго, война, терроризм и т. д.), экономические риски (рецессия, колебания валютных курсов, высокие банковские интересы и нехватка средств и т. д.) и политические риски (регулирующие, правовые и бюрократические);

– инфраструктурные риски, в том числе глобальные сбои инфраструктуры, такие как Интернет, электрические сети и т. д.

Основная часть. Интенсификация внедрения цифровых технологий в экономические системы привела к необходимости исследовать влияние инноваций на трансформацию экономики в разрезе возможных рисков.

Таблица 1

Категории рисков, связанных с технологиями

Категория	Описание	Особенность
А	Неопределенные воздействия: неопределенность, связанная с развитием науки и технологических инноваций	Отсутствие знаний и опыта о последствиях, которые могут возникнуть в результате внедрения новой технологии
Б	Системные воздействия: технологические системы с множественными взаимодействиями и системными зависимостями	Сложность и взаимосвязанность системы: потеря запаса прочности в развивающихся и взаимодействующих (сложных) системах
В	Неожиданные воздействия: установленные технологии в меняющихся средах или контекстах	Неожиданности от известных факторов риска: непредвиденные или изменившиеся обстоятельства

Всемирный банк в своем докладе «Цифровые дивиденды. Доклад о мировом развитии» выделил следующие риски цифровизации [6]:

1) киберпреступность (в том числе кража личных данных);

2) дискриминация (использование финансовыми учреждениями ошибочной цифровой информации для составления цифрового портрета клиента или алгоритмических расчетов с целью определения размеров страховых взносов или процентных ставок);

3) сохранение устаревшей информации (не позволяющее защититься от информации нежелательного характера);

4) снижение доверия к цифровым технологиям;

5) возможность массовой безработицы;

6) рост «цифрового разрыва» (разрыв в цифровом образовании в условиях доступа к цифровым услугам и продуктам и, как следствие, разрыв в уровне благосостояния) между гражданами и бизнесом внутри стран, а также между странами.

С учетом растущего внимания к преступлениям в сфере ИТ сформировано понятие «киберпреступление». Киберпреступность можно определить как компьютерные и информационно-технологические правонарушения, которые включают несанкционированный доступ к пользовательским данным, изменение или нарушение электронных коммуникаций с использованием пользовательских данных для личной выгоды или получения финансовой выгоды [7]. Киберпреступления имеют как краткосрочные[2], так и долгосрочные[3] последствия [8, 9]. По мнению правоохранительных органов Великобритании, современная киберпреступность является одной из самых серьезных угроз экономическому благополучию страны [10].

Термин «киберриск» Национальный институт стандартов и технологий (США) (NIST) определяет как «риск, возникающий из-за потери конфиденциальности, целостности или доступности информации или информационных систем и отражающий потенциальные неблагоприятные воздействия на деятельность организации (например, миссию, функции, имидж или репутацию), активы организации, отдельных лиц, другие организации и страну» [11].

Ключевые компоненты киберриска, согласно NIST, включают:

– угрозы – это любые обстоятельства или события, которые могут оказать неблагоприятное воздействие на деятельность и активы организации, отдельных лиц, другие организации или нацию через информационную систему через несанкционированный доступ, уничтожение, разглашение или изменение информации и / или отказ в обслуживании (DoS);

– уязвимости – это слабость информационной системы, процедур безопасности системы, внутреннего контроля или реализации, которые могут быть использованы источником угрозы;

– вероятность возникновения – это взвешенный фактор риска, основанный на анализе вероятности того, что данная угроза способна использовать данную уязвимость (или набор уязвимостей).

На микроэкономическом уровне киберриски являются важной составляющей стратегического риска предприятия, кредитного риска, а также регуляторного риска[4] [1]. Кибератаки на частный сектор становятся все более важным риском в анализе корпоративного кредитования [12]. Более того, рейтинги кибербезопасности компаний учитываются при оценке инвестиций [13].

На макроэкономическом уровне киберриск может явно влиять на рынки и представлять системный риск, генерируя вероятность разрушения системы или рынка.

В данном контексте актуальной представляется проблематика управления рисками как на уровне государства, так и отрасли или предприятия. В соответствии с определением Совета Общества по анализу рисков (SRA), анализ рисков – это отдельная наука, охватывающая оценку рисков, восприятие, коммуникацию, управление, руководство и политику в контексте рисков, вызывающих озабоченность отдельных лиц, организаций государственного и частного секторов и общества на местном, региональном, национальном или глобальном уровне, это применение принципов управления для идентификации, оценки, управления и передачи риска [14]. Управление рисками включает в себя совокупность действующих лиц, правил, соглашений, процессов и механизмов, связанных с тем, как собирается, анализируется и распространяется соответствующая информация о рисках и принимаются управленческие решения. Управление рисками лежит в основе глобальной финансовой системы, работы ее международных рынков капитала, транснациональных, региональных и местных игроков, а также основных продуктов и услуг [15].

Международный совет по управлению рисками (IRGC) разработал интегрированную аналитическую основу для управления рисками, которая обеспечивает руководство для формирования комплексных стратегий оценки и управления рисками, в том числе на глобальном уровне [16]. Данная структура разделена на три

основных этапа: предварительная оценка, окончательная оценка и управление.

Рамезани и Камаринья-Матос [5] отмечают необходимость компаниям, управляющим крупными, глобальными, конкурентными и сложными цепочками, использовать подходы для проактивного и реактивного противодействия различным угрозам. В этой связи предложен механизм трехэтапного управления рисками: подготовка, реагирование и восстановление.

1. Этап подготовки предполагает комплекс упреждающих мер и действий по выявлению и устранению источника возможных сбоев или снижению (смягчению) их негативного воздействия. Кроме того, вводят другие важные стратегии для этой фазы, такие как: качество, эффективность, минимизация затрат, возможности хеджирования рисков, резервное копирование систем и процессов, систематическое планирование на случай непредвиденных обстоятельств, модернизация информационных технологий и заменимость в цепочке поставок.

2. Этап реагирования предполагает действия, осуществляемые за минимальный период времени после атаки с целью защиты имущества сообщества или бизнес-экосистемы, а также подготовку к началу этапа восстановления.

3. Этап восстановления относится к действиям, направленным на возвращение системы в доаварийное или рабочее состояние за счет изменения бизнес-процессов, изучение опыта и использование новых возможностей.

Качественный скачок в управлении рисками обусловлен инновациями в технологиях, стимулируемыми беспрецедентным развитием объема и качества цифровых данных, которые доступны для глобальных финансовых учреждений. Генерирование цифровых данных становится бесконечным, они регистрируются в реальном времени. Управление рисками характеризуется новыми методами прикладной аналитики и в большей степени зависит от машинного обучения / ИИ [16].

В условиях цифровизации актуальным является обеспечение кибербезопасности как на макро-, так и на микроуровнях. Кибербезопасность, согласно определению Бойсона [17], – это «совокупность комбинированных технологий, процессов и практик, которые применяются для защиты данных и сетей от атак, повреждения или несанкционированного доступа». Большинство организаций используют одно или несколько приложений безопасности, таких как брандмауэры, антивирусное программное обеспечение или системы обнаружения вторжений [18].

Эволюция кибербезопасности в отношении процессов обнаружения вредоносного поведения, ориентированных на защиту информации в критически важных инфраструктурах и пользователях, характеризуется изменением глубины, системности и инструментария: от выявления и удаления вредоносного кода (в 2000 г.) до обеспечения конфиденциальности пользователей, использования технологий блокчейн, аналитики поведения пользователей, учета требований Общего регламента по защите данных ЕС (GDPR) [19].

С целью выявления наиболее эффективных механизмов снижения подверженности компании киберрискам используется анализ сценариев для оценки средств управления в случае наиболее разрушительных киберпотерь в отношении наиболее ценных цифровых активов. Деятельность по управлению киберрисками может включать:

– построение моделей угроз и уязвимостей, направленных на их выявление и классификацию в разрезе приоритетности, принятие мер по выборочному снижению рисков с наивысшим приоритетом в условиях ограниченности ресурсов организации. Данный инструмент обеспечивает аналитиков систематическим анализом профиля вероятного злоумышленника, наиболее вероятных векторов атаки и уязвимых активов. Процесс снижения рисков связан с принятием экономических решений для стратегического инвестирования ограниченных ресурсов, чтобы преобразовать неприемлемые риски в приемлемые;

– разработку и внедрение моделей с учетом зрелости инфраструктуры, которые позволяют интегрировать различные стратегии, возможности и компоненты управления с целью повышения возможностей безопасности организации;

– осуществление киберстрахования, которое позволяет перенести риск и сократить убытки, вызванные кибернарушениями, а также дополняет существующий набор инструментов безопасности для управления киберриском после соответствующего инвестирования. Страхование передает риск компенсируемого убытка страховщику и является стратегией [20], основанной на устойчивости[5];

– создание нормативной базы, которая устанавливает требования к киберриску, регламентируя систему внутреннего контроля и ее мониторинга, обеспечивая тем самым целостность и правильность регулируемых активов (в том числе финансовых данных);

– внедрение международных стандартов, таких как ISO/IEC 27000, которые содержат руководство по организации Системы управления информационной безопасностью (ISMS).

Первым этапом в методологии управления рисками является его оценка, цель которой – определение степени риска и контрмеры, которые могут быть реализованы [21]. Результаты оценки риска могут быть использованы для

определения переносимости или приемлемости рисков [22].

Общепринятая методология оценки риска разработана для решения проблем безопасности и предполагает оценку потерь в расчете на вероятность наступления события[6] [23].

Вместе с тем в научной литературе при оценке безопасности выделяют два основных подхода: качественный и количественный. Количественная оценка риска – это использование измеримых, объективных данных для определения стоимости активов, вероятности потерь и связанного с ними риска (рисков) [1]. Количественные методы варьируют от ранжирования рисков, корреляций рисков, сравнительного анализа и анализа сценариев до генерации прогнозных точечных оценок, а затем до генерации прогнозных распределений (вероятностных моделей)[7].

Качественные подходы к риску, как правило, применяются к тем рискам, которые трудно определить количественно. Качественные подходы заменяют количественные значения, присваивая субъективно определенное значение, например высокое, среднее или низкое. Сравнительный анализ использования количественных и качественных подходов оценки рисков приведен в табл. 2.

Исследовательский центр McKinsey для выявления и определения наиболее важных рисков рекомендует использовать матричную сетку рисков, где потенциальное воздействие события на всю компанию расположено по вертикальной оси, а уровень уверенности лиц, принимающих решения в отношении воздействия, расположен по горизонтальной оси[8] [25]. Таким образом, потенциальные риски ранжируются по отношению друг к другу, а не по абсолютной шкале.

Вместе с тем в условиях цифровизации в современной экономике все большее распространение приобретают комплексные подходы оценки рисков, адаптированные к новым условиям и рискам.

В условиях киберугроз оценка риска представляет собой процесс выявления, оценки и определения приоритетов рисков информационной безопасности. Оценка риска требует тщательного анализа информации об угрозах и уязвимости, чтобы определить степень, в которой обстоятельства или события могут оказать неблагоприятное воздействие на организацию, и вероятность того, что такие обстоятельства или события произойдут.

Разработку методов оценки рисков кибербезопасности осуществляют как международные организации, так и специализированные национальные агентства[9]. Среди наиболее распространенных является серия ISO 27000X, предполагающая непрерывный процесс структурированных последовательностей действий для организаций всех форм и размеров.

Таблица 2

Сравнительный анализ количественных и качественных подходов оценки рисков [1]

Преимущества	Недостатки
Качественные	
1) относительная быстрота и легкость; 2) предоставляет обширную информацию, помимо финансового воздействия и вероятности, например, выявляет уязвимости; 3) показывает скорость возникновения и нефинансовое воздействие (здоровье, безопасность и репутация); 4) легкость восприятия оценок рисков сотрудниками, которые не могут быть обучены сложным методам количественной оценки	1) предоставляет ограниченную дифференциацию между уровнями риска (т. е. очень высокий, высокий, средний и низкий); 2) вероятностные события, относящиеся к одному и тому же уровню риска, могут представлять существенно разную величину риска; 3) невозможность численного агрегирования или рассмотрения взаимодействия и корреляции рисков
Количественные	
1) позволяет выполнить числовое агрегирование с учетом взаимодействия рисков при использовании показателя «подверженности риску», такого как денежный поток; 2) снижает стоимость урегулирования, позволяет осуществлять анализ преимуществ при выборе вариантов реагирования на риски; 3) обеспечивает возможность распределения капитала на основе рисков для бизнеса с оптимальной доходностью; 4) позволяет рассчитать требования к капиталу для поддержания платежеспособности в условиях кризиса	1) может потребовать длительного времени и значительных средств, особенно на первых этапах разработки модели; 2) необходимость выбора единицы измерения, что может привести к игнорированию качественного воздействия; 3) вводные данные и гипотезы могут быть неточными

Некоторые из самых известных методов оценки разработаны Национальным институтом стандартов и технологий США (NIST) [26] и включают платформы 800-53 и Cyber Security Framework (CSF)[10]. Важно отметить, что CSF широко используется во всем мире и NIST продвигает ее в качестве «модели международного сотрудничества по укреплению критически важной инфраструктуры кибербезопасности». NIST 800-53 первоначально разработана с целью содействия компаниям в выполнении Федеральных стандартов информации США (Federal Information Standards – FIPS)[11].

Национальный инфраструктурный консультативный совет США (NIAC) разработал Общую систему оценки уязвимостей (Common Vulnerability Scoring System – CVSS), предназначенную для осуществления открытых и универсально стандартных оценок серьезности уязвимостей программного обеспечения[12].

Кроме того, на уровне компаний осуществляется использование более широкого и простого метода оценки рисков в отношении критически важных для эксплуатации, активов и уязвимостей OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation)[13].

Компания Microsoft разработала собственный метод оценки рисков STRIDE, который классифицирует угрозы безопасности по шести категориям: подмена, фальсификация, отказ, раскрытие информации, отказ в обслуживании, повышение привилегий[14] [27].

Конфиденциальность, целостность и доступность, также известные как триада CIA, являются целевой моделью безопасности, которую используют в качестве общей методологии идентификации угроз[15] [28]. При этом потеря конфиденциальности, целостности и доступности, как показано в табл. 3, может иметь низкий, средний или высокий уровень воздействия на систему.

В рамках инициативы Всемирного экономического форума «Партнерство для киберустойчивости» [29] разработана структура статистической модели для количественной оценки финансового воздействия киберугроз, которая использует вероятность для оценки потерь от кибератак в течение заданного периода времени[16].

Таблица 3

Оценка рисков по методологии CIA

Уровень воздействия	Определение	Применение
Низкий	Можно ожидать, что потеря конфиденциальности, целостности или доступности окажет ограниченное неблагоприятное воздействие на деятельность организации, активы организации или отдельных лиц	Ограниченный неблагоприятный эффект означает, что, например, потеря конфиденциальности, целостности или доступности: 1) может вызвать ухудшение функциональных возможностей организации до такой степени и такой продолжительности, на которые организация способна выполнять свои основные функции, но эффективность функции заметно сокращается; 2) приводит к незначительному повреждению активов организации; 3) вызывает незначительные финансовые потери; 4) приводит к незначительному ущербу для физических лиц
Средний	Можно ожидать, что потеря конфиденциальности, целостности или доступности окажет серьезное неблагоприятное воздействие на деятельность организации, активы организации или отдельных лиц	Серьезный неблагоприятный эффект означает, что, например, потеря конфиденциальности, целостности или доступности: 1) может вызвать значительное ухудшение возможностей осуществления деятельности до такой степени и продолжительности, в течение которых организация способна выполнять свои основные функции, но эффективность функций значительно сокращается; 2) приводит к значительному повреждению активов организации; 3) вызывает значительные финансовые потери; 4) приводит к значительному ущербу для людей, который не связан с потерей жизни или серьезными опасными для жизни травмами

Окончание табл. 3

Уровень воздействия	Определение	Применение
Высокий	Можно ожидать, что потеря конфиденциальности, целостности или доступности окажет серьезное или катастрофическое неблагоприятное воздействие на деятельность организации, активы организации или отдельных лиц	Серьезный или катастрофический неблагоприятный эффект означает, что, например, потеря конфиденциальности, целостности или доступности: 1) может вызвать серьезное ухудшение или потерю способности организации до такой степени и продолжительности, что организация не в состоянии выполнить одну или несколько основных функций; 2) приводит к серьезному ущербу активов организации; 3) вызывает крупные финансовые потери; 4) приводит к серьезному или катастрофическому ущербу для людей, в том числе к смерти или серьезным опасным для жизни травмам

С экономической точки зрения при оценке киберрисков осуществляется оценка стоимости безопасности или ее отсутствия. В данном контексте важно отметить проблематику оценки потерь от киберинцидентов, которая обусловлена сложностью определения стоимости нематериальных цифровых активов. Следует также учитывать такой показатель, как потеря рыночной стоимости фирмы из-за сообщений о нарушениях безопасности [30].

Экономическая классификация затрат, связанных с киберинциндентами, приведена в табл. 4 и включает прямые затраты (или собственные убытки), косвенные затраты (или убытки от третьих лиц), краткосрочные затраты (или переменные затраты), долгосрочные затраты (или постоянные затраты), материальные затраты, нематериальные затраты, ожидаемые затраты, ответные затраты.

Микроэкономические потери в результате киберинциндентов также могут быть определены количественно с использованием категорий убытков, включая прямые убытки, расходы на расследование инцидента и реагирование на него, репутационный ущерб, юридическую ответственность, выплату штрафов, негативное влияние на цену акций.

Таблица 4

Категории затрат на киберинциденты (составлено автором на основе [31])

Категория потерь	Описание
Прямые затраты (или собственные убытки)	Убытки, которые напрямую влияют на организацию. Распространенные сценарии собственных потерь включают: 1) злонамеренное уничтожение данных; 2) атаки отказа в обслуживании (DoS); 3) вирусы, вредоносное ПО, шпионское ПО и т. д.; 4) случайное повреждение данных; 5) человеческие ошибки; 6) скачки электроэнергии / стихийные бедствия; 7) отказ ИТ-систем; 8) угрозы кибервымогательства
Косвенные затраты (или убытки от третьих лиц)	Убытки, косвенно влияющие на организацию. Распространенные сценарии сторонних потерь включают: 1) репутационные потери; 2) потерю доверия сотрудников; 3) возможные судебные иски, как гражданские, так и уголовные; 4) потерю конфиденциальных данных
Краткосрочные затраты (или переменные затраты)	Краткосрочные расходы, понесенные только в период, когда произошел инцидент, могут включать: 1) снижение производительности труда и производительности сотрудников из-за взломанных информационных ресурсов, затрат на рабочую силу и материалов, необходимых для обнаружения, сдерживания, ремонта и восстановления взломанных ресурсов; 2) затраты, связанные с поиском, сбором доказательств и судебным преследованием злоумышленника; 3) расходы на предоставление информации клиентам и общественности, связанные со СМИ

Окончание табл. 4

Категория потерь	Описание
Долгосрочные затраты (или постоянные затраты)	Долгосрочные затраты, понесенные после устранения непосредственных последствий инцидента, могут включать: 1) затраты, связанные с потерей клиентов; 2) невозможность привлечь новых клиентов из-за предполагаемой низкой безопасности; 3) потерю доверия клиентов и деловых партнеров; 4) возможные будущие юридические обязательства, возникающие в результате нарушения; 5) стоимость доступа конкурента к конфиденциальной или служебной информации; 6) повышенную стоимость страхования или более высокую стоимость капитала на рынках заемных средств и акций из-за предполагаемого увеличения бизнес-риска
Материальные затраты	Материальные затраты могут включать: 1) возможные упущенные продажи, потерю активов; 2) дополнительные затраты на страхование
Нематериальные затраты	Нематериальные затраты могут включать: 1) репутационный ущерб; 2) потерю доверия клиентов
Ожидаемые затраты	Увеличение затрат на безопасность в ожидании будущих рисков. Ожидаемые затраты могут быть фиксированными
Ответные затраты	Затраты на безопасность, понесенные в ответ на уже произошедшие отказы информационной безопасности. Затраты носят переменный характер

Следует выделить факторы, способствующие возникновению (или усилению) новых рисков, в том числе инновации, потеря запаса прочности, изменение восприимчивости к риску, конфликты интересов, социальная динамика, технический прогресс, коммуникации, информационная асимметрия, неправильные стимулы, преступные мотивы и поступки [4].

Инновационные технологии могут оказывать кардинальное влияние на производственные модели, подходы, концепции и бизнес [32]. В докладе о системных рисках, разработанном ОЭСР в 2003 г., отмечаются три аспекта новых технологий, которые влияют на риск: взаимосвязанность; скорость и распространенность технологических изменений; фундаментальные изменения в среде, которые они могут вызвать [33].

Согласно Рабочему соглашению по управлению возникающими рисками, связанными с технологией, Европейского комитета по стандартизации (CEN) (CWA 16649: 2013), определены в том числе следующие факторы, генерирующие технологические риски в промышленных организациях:

1) новые технологии;

2) новые материалы;

3) новые производственные процессы и новые производственные сети;

4) новые политики;

5) неопределенности в измерениях и характеристиках и пр. [34].

Ряд исследований в области производственных процессов дополнительно выделяют такие факторы риска, как автоматизация и интерфейсы «человек – машина» и «человек – ICT» [35].

Руан классифицирует следующие факторы киберриска: технологические факторы (связаны с использованием технологий), нетехнологические факторы (обусловлены процессами, социально-экономическими, геополитическими факторами), внутренние факторы (основаны на характере бизнеса, отрасли, операциях, товарах и услугах и пр.), контрольные факторы (отражают эффективность контроля предприятия в отношении кибератак и являются предметом инвестиций, когда речь идет о снижении рисков) (табл. 5).

Отмечается, что для измерения киберрисков целесообразным является создание банка данных киберрисков с целью идентификации ключевых факторов киберрисков, связанных с профилем организации. На подверженность компании кибернетическому риску влияет широкий спектр динамических технологических и нетехнологических факторов профилирования, внутренних уязвимостей и внешних угроз. В частности, мотивы злоумышленников во многом определяются нетехнологическими факторами [36].

В контексте потенциальных рисков значительное внимание со стороны как ученых, так и практиков уделено стратегиям, разработанным для снижения рисков и эффективного реагирования на инциденты, связанные с рисками [5].

Таблица 5

Количественный метод оценки микроэкономических потерь (составлено автором на основе [31])

Категория потерь	Метод оценки потерь
Прямые убытки (финансовые убытки, материальный ущерб, смерть и телесные повреждения)	Убыток, основанный на оценке атакованных цифровых ценностей, прямые убытки по расходам и т. д.
Расследование инцидента и реагирование	Стоимость оплаты группы судебно-медицинских экспертов и внешних консультантов за расследование инцидента и реагирование на него, включая технические инструменты и приложения, необходимые для приобретения и установки
Репутационный ущерб (применяется после обнародования инцидента)	Расчетные экономические потери коррелируют с размером аудитории СМИ, в которых публикуется информация об инциденте, и через рейтинговые агентства
Юридическая ответственность	Ответственность, как это определено в законах, нормативных актах, контрактах и соглашениях
Нормативные штрафы	Нормативные штрафы, например 5% от выручки
Влияние на цену акций	По неявной рыночной стоимости (оценки) и явной рыночной стоимости (наблюдаемой)

Ряд исследований рекомендуют переход от управления рисками к управлению устойчивостью [37]. Это обосновывается тем фактом, что данный подход охватывает кризисные и посткризисные фазы. В этом смысле управление устойчивостью близко к тому, что обычно понимается как кризисное управление или цикл кризисного управления.

В научной литературе выделяют три аспекта концепции устойчивости системы:

– способность системы восстанавливаться после сбоя и / или атаки;

– способность системы поддерживать желаемое состояние (т. е. возвращаться к новому состоянию равновесия или принятому состоянию);

– способность системы противостоять атаке с постепенной адаптацией и трансформацией.

В последнее время концепция устойчивости системы эволюционирует, чтобы представлять адаптивную и даже трансформирующую способность, концентрируясь на нелинейной сложности и многомерной устойчивости систем (мультиравновесия). Это означает выход за рамки традиционной устойчивости, перетаргетирование на ее улучшение и привнесение новой перспективы устойчивости, формирование сложной адаптивной системы.

С экономической точки зрения при принятии управленческих решений по защите от киберугроз представляется целесообразным учитывать такие факторы, как:

1) оценка прочности элементов управления для цифровых активов;

2) измерение экономической эффективности средств управления цифровыми активами;

3) определение предела киберриска субъекта;

4) измерение стоимости снижения риска;

5) измерение рентабельности инвестиций в киберриск.

В настоящее время, как показал проведенный анализ, среди наиболее распространенных и опасных инструментов кибератак выделяют следующие:

А. 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 [17] [38].

При этом, как показал ряд исследований, выделяют следующие тенденции распространения вредоносных программ [39]:

– существенно возрастает сложность вредоносных программ;

– цели атаки смещаются в сторону сложного шпионажа;

– векторы доступа становятся комплексными и зависимыми от наличия эксплойтов нулевого дня;

– в ближайшем будущем кибератаки станут более распространенными и разрушительными;

– таргетированному шпионскому вредоносному программному обеспечению не хватает модулей для киберфизических атак и специальных протоколов интеллектуальных сетей, однако такие функции будут реализованы в будущем.

Одним из самых распространенных инструментов кибератак являются программы-вымогатели[18]. Исследования показывают, что с 2014 по 2017 г. было выявлено 327 семейств вымогателей, в результате которых было совершено 184 млн атак [40]. Цифровая бизнес-платформа Statista оценивает количество атак программ-вымогателей в 2020 г. в размере 304 млн, при этом рост по сравнению с 2019 г. составил более 60% [41].

В 2018 г. 40% средних и крупных британских компаний подвергались в среднем пяти атакам программ-вымогателей, при этом суммарные выплаты каждой организации превысили 320 тыс. фунтов стерлингов в год [42]. Важно отметить, что около 90% предприятий, потерявших данные, были вынуждены прекратить деятельность в течение следующих двух лет после атаки.

Как показало исследование «Лаборатории Касперского», секторально наиболее подверженными отраслями данного вида кибератак являются образование, информационно-коммуникационные технологии (ИКТ), медиа и развлечения, финансовые услуги (рис. 1). Больницы и иные медицинские учреждения становятся мишенями программ-вымогателей, так как для них доступ к файлам с данными пациентов является критическим. Медицинские учреждения, как правило, не располагают ни финансовыми, ни людскими ресурсами, необходимыми для организации и поддержания надлежащей киберзащиты [43]. В мае 2017 г. программа-вымогатель (WannaCry) заразила более 300 тыс. компьютеров, в том числе ряд высокопроизводительных систем, включая Национальную службу здравоохранения Великобритании (NHS) [40].

Согласно отчету Chainalysis 2021, программы-вымогатели представляют собой серьезную растущую проблему кибербезопасности как для государственного, так и для частного секторов [44].

Известные выплаты злоумышленникам-вымогателям с 2019 по 2020 г. выросли на 337%, достигнув суммы более 400 млн долл. США. Отмечается, что приведенные данные – это нижние оценки, реальные показатели выше. При этом средний размер выкупа значительно вырос с 12 тыс. долл. США в криптовалюте в четвертом квартале 2019 г. до 54 тыс. долл. США в первом квартале 2021 г. Данная тенденция объясняется повышением эффективности атак более крупных организаций с помощью незаконного приобретения инструментов для взлома, украденных данных и других цифровых активов. По мнению экспертов Chainalysis, самое большое количество атак с использованием программ-вымогателей осуществляется киберпреступниками из СНГ.

Б. Целевые кибератаки[18] (Advanced Persistent Threats – APT) предполагают скрытое внедрение в ИКТ-сектор организации, как правило, с целью кражи данных и промышленного шпионажа. Целевые атаки иногда остаются необнаруженными в течение месяцев или даже лет[19] [45]. Согласно исследованию Symantec [46], программа Stuxnet заразила около 100 тыс. систем в 115 странах; программа Duqu, предназначенная для промышленных систем управления, собирала конфиденциальную информацию, по крайней мере, в восьми странах[20] [47, 48].

В. DDoS-атаки имеют целью отключение компьютерных систем или сетей[21] [49]. По мнению Европейского полицейского управления (Европол) [50], инструментарий DDoS становится все более связанным с организованной преступностью. Ведущий поставщик решений для сетевой защиты – компания Corero Networks [8] подтвердила, что сетевые атаки, такие как распределенный отказ в обслуживании (DDoS), в год увеличиваются на 40%, достигнув в 2018 г. величины более чем 400 тыс. атак в месяц.

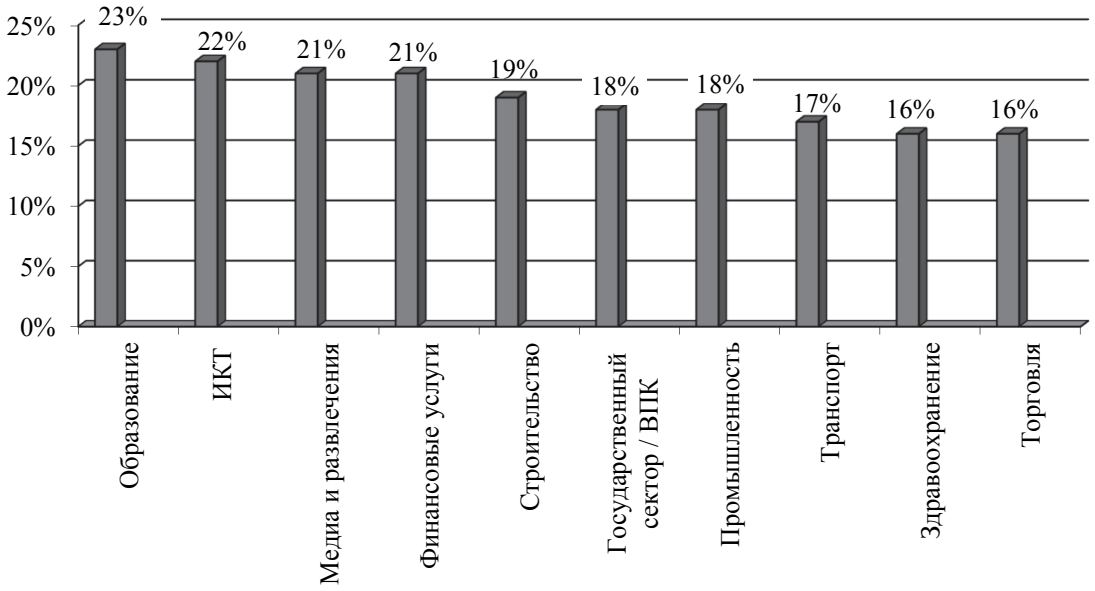

Рис. 1. Доля атакованных программами-вымогателями предприятий по секторам [43]

Важно отметить расширение использования кибератак, спонсируемых государствами и организованными преступными группировками [31]. Злоумышленники / хакеры имеют доступ к сложным инструментам, конфиденциальной информации и учетным данным (некоторые из них получены незаконным путем), финансовые ресурсы и иммунитет от государственного преследования, возможно, даже степень анонимности или защиты личности [51]. К основным направлениям данного вида угроз следует отнести следующие:

1) атака критической иностранной инфраструктуры [52];

2) целевые кибератаки для кражи военных секретов или разведывательных данных;

3) коммерческий кибершпионаж и саботаж для получения коммерческих секретов, конкурентного преимущества по сравнению с конкурирующими компаниями[23];

4) атака с целью получения доступа к личной компрометирующей и финансовой информации;

5) хакерские атаки или DDoS-атаки во имя «социальной справедливости» и / или «возмездия» в отношении отдельных организаций[24];

6) инсайдерские угрозы, создаваемые недовольными сотрудниками, включают использование доступа к внутренней системе и учетным данным или «социальную инженерию» для получения конфиденциальной информации;

7) деятельность одиночных хакеров по взлому военной инфраструктуры или инфраструктуры национальной безопасности;

8) кража финансовых активов в интересах конкретных государств[25].

При этом, по данным «Лаборатории Касперского», наибольшее количество кибератак на компьютеры пользователей с ноября 2019 г. по октябрь 2020 г. происходило из США (49,8%), Нидерландов (13,36%), Франции (7,2%).

Анализ современных тенденций развития киберпреступлений и противодействия им позволяет отметить тот факт, что в условиях глобальной цифровизации формируется новая индустрия «Киберпреступление как услуга» (CaaS) [7, 53]. При этом отдельно выделяются направления аутсорсинга предложения по таким услугам, как программа-вымогатель (Ransomware-as-a-Service – RaaS) и аренда бот-сетей для создания инфраструктуры DDoS-атак. Также выделяют следующие составляющие цифровизации криминальных услуг [54]:

– обслуживание криминальной инфраструктуры, предполагающее предоставление серверов, необходимых для совершения киберпреступлений[26] [55];

– оказание услуг, включающих проектирование, создание и распространение вредоносных программ [56];

– предоставление сервисов взлома, начиная с учетных записей электронной почты или социальных сетей, запуск DDoS-атак [55];

– продажа личных, финансовых данных, информации об уязвимостях программ или приложений[27];

– оказание услуг по отмыванию денег[28];

– в период пандемии в Интернете расширились продажи наркотиков, оружия и поддельных ценных бумаг, кроме того, отмечается взрывной рост фишинговых ресурсов[29] [57];

– переход на дистанционную работу повысил нагрузку на корпоративную безопасность за счет растущего числа атак на веб-приложения[30] [43];

– расширение использования технологий биометрии для противодействия киберпреступлениям;

– увеличение количества атак на IoT, включая такие устройства, как веб-камеры, умные часы, телевизоры и пр.[31];

– масштабная цифровизация предприятий привела к необходимости комплексной защиты критической и промышленной инфраструктуры: медицинских учреждений, производств, финансового сектора, транспортных систем, телекоммуникаций, энергетики, систем водоснабжения и т. д., так как данные предприятия оказались в большей степени подвержены киберугрозам [43]. В настоящее время отмечается специализация ряда профессиональных группировок на целевых атаках предприятий в таких секторах, как энергетика, машиностроение и промышленность. Более того, фиксируются кибератаки, нацеленные на автоматизированные системы управления технологическим процессом, промышленные сети, IoT и критическую инфраструктуру в целом.

Следует отметить рост ущерба для экономики от глобальной киберпреступности за 2014–2017 гг. с 445 до 608 млрд долл. США (см. табл. 6). Данные табл. 6 свидетельствуют о прямой корреляции объема регионального ВВП с размером потерь, связанных с киберпреступностью.

Согласно данным отчета, опубликованного Symantec, в 2017 г. от киберпреступности пострадали 978 млн человек в 20 странах мира [59] на сумму 172 млрд долл. США (в среднем 142 долл. США на жертву. Кроме того, эти киберпреступления не только приносят финансовые потери, но также оказывают психологическое и социальное влияние на благополучие жертв [60].

Данные отчета по прогнозированию угроз и оценки идентичности (ITAP) университета Техаса [61, 62] свидетельствуют о том, что в 2019 г. кражи цифровых активов увеличились на 25% по сравнению с 2018 г.

Таблица 6

Региональное распределение киберпреступлений в 2017 г. [58]

Регион	Объем ущерба от киберпреступлений, млрд долл. США	Потеря от киберпреступлений, % от ВВП
Северная Америка	140–175	0,69–0,87
Европа и Центральная Азия	160–180	0,79–0,89
Восточная Азия и Тихоокеанский регион	120–200	0,53–0,89
Южная Азия	7–15	0,24–0,52
Латинская Америка	15–30	0,28–0,57
Африка к югу от Сахары	1–3	0,07–0,20
Ближний Восток и Северная Африка	2–5	0,06–0,16
Итого	445–608	0,59–0,80

Согласно отчету WEF, менее чем за 10 лет кибербезопасность стала одной из наиболее важных системных проблем для мировой экономики. Коллективные глобальные расходы достигли 145 млрд долл. США в год и, по прогнозам, превысят 1 трлн. долл. США в период между 2017 и 2021 гг. [63]. При этом, несмотря на рекордные расходы на кибербезопасность, по данным ряда исследований, 53% из 3000 опрошенных компаний были плохо подготовлены к противодействию кибератакам [64, 65]. По оценкам ЕС, издержки от киберпреступлений для мировой экономики к 2020 г. превысили 5,5 трлн. евро (двухкратный рост за период с 2015 г.), более 12% всех европейских компаний уже были атакованы киберпреступниками [66]. Исследование, которое проводил Институт Ponemon, подтвердило, что средняя утечка данных обошлась компаниям в 3,8 млн долл. США [67].

Анализ актуальных проблем и рисков цифровизации экономики показывает необходимость международного регулирования данной сферы с акцентом на сферу борьбы с киберпреступлениями:

1) для стандартизации сбора данных об инцидентах необходимо разработать Международную классификацию киберинцидентов (International Classification of Cyber Incidents – ICCI) в сочетании с Международной классификацией цифровых активов (International Digital Asset Classification – IDAC);

2) для борьбы со сложными угрозами глобального уровня важно развивать международное сотрудничество и обмен экспертизой;

3) необходимо улучшить обмен информацией и опытом между частным и государственным секторами на национальном и международном уровнях.

В Республике Беларусь уполномоченным правоохранительным органом по борьбе с киберпреступностью является Главное управление МВД по противодействию киберпреступности («Управление К»). По данным данного учреждения, в 2020 г. в Беларуси зарегистрировано свыше 25,5 тыс. киберпреступлений с нарастающей динамикой (рис. 2), к уголовной ответственности привлечены 1592 человека. Пострадавшими от данного вида преступлений в Беларуси в 2020 г. стали около 100 тыс. человек[32].

За 2018–2020 гг. предприятиям причинен ущерб на сумму более 2 млн руб., при этом за четыре месяца 2021 г. сумма причиненного киберпреступниками ущерба составила более 290 тыс. руб.[33].

Основными видами киберпреступлений, по данным правоохранительных органов[34], являлись шифрование коммерческой информации, подмена реквизитов при переводе средств, фишинговые письма.

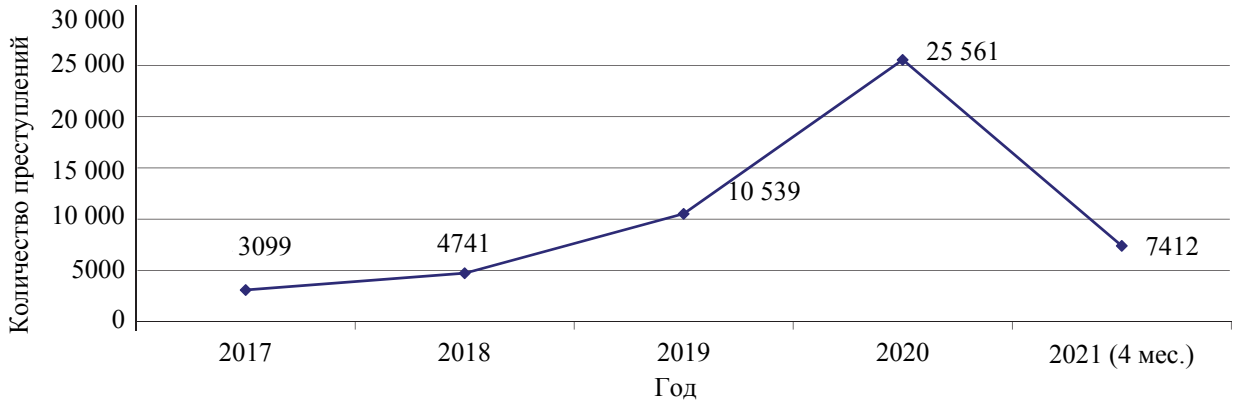

Рис. 2. Количество киберпреступлений в Республике Беларусь за 2017–2021 гг.

Заключение. Таким образом, следует отметить, что концепция риска претерпела ряд трансформаций и в настоящее время может рассматриваться через призму бизнес, социальных, экономических, инвестиционных, военных и политических угроз.

Среди рисков цифровизации, в первую очередь, выделяют: киберпреступность, рост «цифрового разрыва» и массовую безработицу. При этом если на микроуровне киберриски являются важной составляющей стратегического риска предприятия, кредитного и регуляторного рисков, то на макроуровне киберриск может оказывать влияние на рынки и представлять системный риск, генерируя вероятность разрушения системы или рынка. Риски системного характера охватывают более одной страны, более одного сектора экономики и могут оказывать влияние на природные, технологические и социальные системы.

Управление рисками включает в себя совокупность действующих лиц, правил, соглашений, процессов и механизмов, связанных с тем, как собирается, анализируется и распространяется соответствующая информация о рисках и принимаются управленческие решения. Современной концепцией также является отказ от управления рисками в пользу управления устойчивостью организаций / систем. Данная концепция устойчивости системы эволюционирует, чтобы представлять адаптивную и даже трансформирующую способность, концентрируясь на нелинейной сложности и многомерной устойчивости систем (мультиравновесия).

Среди наиболее распространенных и опасных инструментов кибератак выделяют вредоносные программы; целевые кибератаки (APT), предполагающие скрытое внедрение в ИКТ-сектор организации, как правило, с целью кражи данных и промышленного шпионажа; DDoS-атаки, имеющие целью отключение компьютерных систем или сетей. В условиях глобальной цифровизации формируется новая индустрия «Киберпреступление как услуга» (CaaS).

Объектами кибератак становятся, как правило, элементы критической инфраструктуры страны, государственные учреждения, банковские и финансовые организации, медицинские учреждения, образовательные институты, сфера ИКТ, медиа и развлечения.

Комплексное решение проблем киберугроз требует наднационального регулирования, которое может включать стандартизацию сбора данных об инцидентах, развитие международного сотрудничества и обмен экспертизой, обмен информацией и опытом между частным и государственным секторами на национальном и международном уровнях.

---

[1]Концепция риска возникла в математике в XVII в. для расчета комбинации вероятности и величины потенциальных прибылей и убытков в азартных играх. В XVIII в. риск как нейтральная концепция рассчитывался применительно к страхованию морских перевозок. Изучение рисков в экономике возникло в XIX в.

[2]Краткосрочные последствия имеют место, когда значительные ежедневные финансовые и другие потери затрагивают операционную деятельность предприятий и правительств.

[3]Утрата репутации может быть отнесена к долгосрочным последствиям. Например, в 2018 г. утечка данных, затронувшая 50 млн пользователей Facebook, вызвала потерю доверия инвесторов к Facebook и потерю около 43 млрд долл. капитализации.

[4]Согласно оценкам, из-за успешной атаки 60% предприятий малого и среднего бизнеса прекращают свою деятельность в течение 6-месячного периода. Конкурентные преимущества или коммерческие секреты часто являются основными целями кибератак. Каждый пятый бизнес, пострадавший от вымогателей, вынужден закрыться.

[5]Развивая данный подход, Фишер, Халибозек, Вальтерс [24] предложили два альтернативных решения, которые должны дополнять друг друга: инвестиции в методы предотвращения потерь и страхование.

[6]При оценке рисков, как правило, используется формула: $R = T \cdot D$, где T – вероятность наличия опасности, а D – оценка потерь в случае повреждения системы.

[7]Как правило, количественные подходы следуют базовой формуле, которая идентифицирует активы, угрозы для этих активов, назначает вероятность возникновения угрозы и затем умножает эту вероятность на оценку активов. Сумма этой формулы обеспечивает базовый расчет, который учитывает вероятность потери и ее стоимость в случае ее возникновения. Многие современные количественные подходы стали сложными актуарными моделями с применением исторических данных о происшествиях для определения вероятности наступления события.

[8]Высокое размещение на вертикальной оси означает, что существование компании окажется под угрозой, если возникнет этот риск, или компания упустит прибыль. Низкое расположение по вертикальной оси означает, что воздействие или возможность будут ограниченными или изолированными.

[9]Наиболее широко признанными являются структуры Международной организации по стандартизации (International Organisation for Standardisation – ISO) и Международной электротехнической комиссии (International Electrotechnical Commission – IEC), совместно ISO / IEC, а также Национального института

стандартов и технологий США (National Institute of Standards and Technology – NIST). Так, серия ISO 27000X предоставляет руководство по наилучшей практике для всей системы управления информационной безопасностью. Структура поощряет организации оценивать свои ИТ-риски, а затем вводить соответствующие средства контроля в соответствии с их конкретными потребностями. Данный подход включает в себя непрерывную обратную связь и мероприятия по улучшению, чтобы противостоять текущему ландшафту угроз или принимать во внимание инциденты безопасности.

[10]Первая версия NIST Cyber Security Framework (CSF) была выпущена в 2014 г. в соответствии с Законом США об усилении кибербезопасности и была разработана для улучшения критической инфраструктуры кибербезопасности. Платформа была создана в качестве живого документа и включает информацию, полученную от новых угроз и рисков, и предлагает решения путем регулярных обновлений.

[11]В эту структуру включены стратегии по приведению в соответствие Федерального закона об управлении информационной безопасностью 2002 г. (Federal Information Security Management Act – FISMA) с международным стандартом безопасности ISO / IEC 27001.

[12]NIAC был создан как глобальная структура для раскрытия информации об уязвимостях в сфере безопасности и помогает ИТ-менеджерам преобразовать множество данных об уязвимостях в практические приоритеты. CVSS была принята во всем мире и используется поставщиками бюллетеней по уязвимостям, поставщиками программных приложений, организациями пользователей, компаниями по сканированию и управлению уязвимостями, фирмами по обеспечению безопасности и управлению рисками, а также исследовательскими институтами.

[13]OCTAVE был разработан в 2001 г. в Университете Карнеги – Меллона (CMU) для Министерства обороны США. OCTAVE используется для определения уровней риска и для планирования против кибератак. Его структура предназначена для минимизации подверженности организаций угрозам, а также для прогнозирования вероятных результатов атак и устранения тех, которые были успешными. Структура разбита на три определенных этапа: создание профилей угроз на основе активов, выявление уязвимостей инфраструктуры, разработка стратегии и планов безопасности.

[14]*Подмена*: когда человек или программа успешно маскируется под другого, подделывая данные, чтобы получить незаконное преимущество. *Фальсификация*: акт преднамеренного изменения данных по несанкционированным каналам. *Отказ*: когда приложение или система не применяют элементы управления для надлежащего отслеживания и регистрации действий пользователя, что позволяет злонамеренно манипулировать или подделывать идентификацию новых действий. *Раскрытие информации*: атака, такая как нарушение конфиденциальности или утечка данных, которая приводит к тому, что информационная система раскрывает конфиденциальную информацию, которая не должна раскрываться. *Отказ в обслуживании*: кибератака, при которой злоумышленник пытается сделать компьютер или сетевой ресурс недоступным для своих предполагаемых пользователей путем временного или неограниченного прерывания работы хоста, подключенного к Интернету. *Повышение привилегий* (Elevation of privilege – EoP): предоставление разрешения авторизации злоумышленника сверх первоначально предоставленного.

[15]Потеря конфиденциальности – несанкционированное разглашение информации. Потеря целостности – это несанкционированное изменение или уничтожение информации. Потеря доступности – это нарушение доступа или использования информации или информационной системы.

[16]Концепция Cyber VaR основана на понятии VaR – статистическом методе, широко применяемом в индустрии финансовых услуг для выражения уровня финансового риска банка (или финансового риска, связанного с конкретным инвестиционным портфелем) в течение определенного периода времени. Cyber VaR рассматривает три основных фактора киберрисков для организации: уязвимость, активы и профиль его потенциальных злоумышленников.

[17]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).

[18]Вредоносное программное обеспечение, которое после загрузки в систему-жертву шифрует жесткий диск и выдает предупреждение о том, что если выкуп не будет выплачен в течение 24–48 ч, все данные станут невосстановимыми. Затем программное обеспечение сообщает жертве о необходимости, как правило, отправки преступнику от 250 до 1000 долл. США в течение отведенного периода, обычно через биткоины. Когда выкуп будет выплачен, преступник отправит жертве буквенно-цифровую последовательность, чтобы разблокировать вредоносное ПО. Жертвы обычно заражаются, нажимая на фишинговое сообщение или загружая вымогателей с зараженного или вредоносного веб-сайта. Относительно короткий срок, позволенный заплатить выкуп, состоит в том, чтобы отговорить жертв найти альтернативные методы расшифровки системы. Многие жертвы считают, что им нужно больше времени, чтобы понять, как использовать бит-монеты. В некоторых случаях жертвы договаривались с преступниками о снижении оплаты.

[19]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.

[20]Программа Stuxnet предназначалась для программируемых логических контроллеров, чувствительных промышленных систем, была активна в течение по крайней мере 3 лет до ее обнаружения.

[21]С точки зрения шпионажа троян Regin, как полагают, использовался для глобальных систематических атак как минимум с 2008 г. Другие примеры включают Flame, Mahdi и Gauss.

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

[23]Правительство США в 2019 г. запретило продажу продуктов Huawei своим клиентам, так как считает, что КНР установило «скрытые программы» в устройствах. Продукты израильской компании Checkpoint также были запрещены для продажи правительственным клиентам США, поскольку Checkpoint не позволяла проводить проверку своего программного обеспечения.

[24]Хакерские коллективные группы, такие как Lulzsec или Anonymous, нацелены на веб-сайты или критически важную инфраструктуру, вызывая перебои в обслуживании и простои с соответствующими финансовыми и репутационными издержками.

[25]Эксперты по кибербезопасности выяснили, что в 2019–2020 гг. хакеры КНДР украли в биткоинах и остальных криптовалютах около 316 млн долл. Об этом сообщило агентство Kyodo, сославшись на отчет Комитета при Совбезе ООН по контролю за соблюдением санкций в отношении Пхеньяна. Исследователи выяснили, что хакеры взламывали не только криптовалютные биржи, но и сайты инвестиционных компаний и фондов. Даже частные трейдеры периодически становились жертвами корейских киберпреступников.

[26]Вместо того, чтобы рисковать совершением незаконных действий на своих компьютерах, правонарушители предпочитают либо подключаться к выделенному серверу или прокси-серверу, либо обращаться к услугам хостинга, чтобы избежать обнаружения правоохранительных органов. Хостинг-провайдеры играют решающую роль в криминальной онлайн-экономике, и услуги «непробиваемого» хостинга являются одним из самых востребованных товаров.

[27]Одним из самых известных онлайн-форумов по кардингу был DarkMarket, на котором могли удовлетворяться спрос и предложение незаконных материалов, таких как личные и финансовые данные.

[28]Услуга аналогична той, как это происходит в реальном мире, где большинству традиционных преступников нужен канал для легитимизации их преступных доходов. Киберпреступники также нуждаются в выходе из цифровой финансовой системы. Типичные провайдеры, такие как денежные «мулы», играют заметную роль в соединении онлайн- и оффлайн-миров.

[29]По данным Positive Technologies, во втором квартале 2020 г. число кибератак выросло на 59% по сравнению с аналогичным периодом 2019 г. По данным компании «Ростелеком», за первые полгода 2020 г. объем киберпреступлений в отношении организаций увеличился на 40% по сравнению с аналогичным периодом 2019 г. По данным МВД России, в первом полугодии 2020 г. число киберпреступлений выросло на 91,7% на фоне снижения традиционной преступности.

[30]Среднее ежедневное число атак методом брутфорса – автоматизированного перебора паролей – на базы данных в апреле 2020 г. увеличилось на 23% по сравнению с январем того же года и фишинга на тему пандемии коронавируса (с конца февраля 2020 г. количество фишинговых атак по электронной почте выросло более чем на 600%).

[31]Рост атак на домашние сети, умные устройства и роутеры в первом полугодии 2020 г. отмечают в компании Trend Micro.

[32]Необходима надежная защита от киберпреступности. URL: https://www.sb.by/articles/informatsiya-bezopasnosti3445.html.

[33]Как защититься от киберпреступников. URL: https://www.sb.by/articles/zaslon-dlya-kiberataki3.html.

[34]Главное управление по противодействию киберпреступности КМ МВД РБ предупреждает. URL: https://www.mrik.gov.by/glavnoe-upravlenie-po-protivodejstviyu-kiberprestupnosti-km-mvd-rb-preduprezhdaet.

Список литературы

1. Ruan K. Cyber Risk Management: A New Era of Enterprise Risk Management. Digital Asset Valuation and Cyber Risk Measurement Principles of Cybernomics. Cambridge: Elsevier Inc., 2019. P. 49–73. URL: https://doi.org/10.1016/B978-0-12-812158-0.00003-X (date of access: 10.10.2020).

2. International Organization for Standardization (ISO). Risk Management – Principles and Guidelines: ISO 31000: 2009. URL: https://www.iso.org/iso-31000-risk-management.html (date of access: 11.04.2020).

3. Quality vocabulary. Availability, reliability, and maintainability terms. Guide to concepts and related definitions: BS 4778-3.1: 1991. London: British Standards Institution, 1991. 32 p.

4. International Risk Governance Council (IRGC). The Emergence of Risks. Contributing Factors. Geneva, 2010. URL: www.irgc.org (date of access: 10.02.2020).

5. Ramezani J., Camarinha-Matos L. Approaches for resilience and antifragility in collaborative business ecosystems // Technological Forecasting & Social Change. 2020. No. 151. P. 26. URL: https://doi.org/10.1016/j.techfore.2019.119846 (date of access: 15.04.2020).

6. Цифровые дивиденды. Доклад о мировом развитии 2016. Обзор. Вашингтон: Группа Всемирного банка, 2016. 58 с. URL: https://openknowledge.worldbank.org/bitstream/handle/10986/23347/210671RuSum.pdf (дата обращения: 05.02.2020).

7. Consumer-facing technology fraud: Economics, attack methods and potential solutions / M. Ali [et al.] // Future Generation Computer Systems. 2019. No. 100. P. 408–427. URL: https://doi.org/10.1016/j.future.2019.03.041 (date of access: 14.01.2020).

8. Sharafaldin I., Lashkari A., Ghorbani A. An evaluation framework for network security visualizations // Computers & Security. 2019. No. 84. P. 30–92. URL: https://doi.org/10.1016/j.cose.2019.03.005 (date of access: 24.12.2020).

9. Choo K-Kr. The cyber threat landscape: challenges and future research directions // Computers & Security. 2011. No. 30 (8). P. 719–731.

10. Hunton P. Data attack of the cybercriminal: Investigating the digital currency of cybercrime // Computer Law & Security Review. 2012. No. 28. P. 201–207. URL: https://10.1016/j.clsr.2012.01.007 (date of access: 03.03.2020).

11. NIST. Guide for Conducting Risk Assessments. Special Publication 800-30 Rev 1: US Department of Commerce. Washington, DC, 2012. 95 p. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecial publication800-30r1.pdf (date of access: 01.03.2020).

12. Volz D. Cyber attacks loom as growing corporation credit risk. Moody's, 2015. URL: http://www.reuters.com/article/us-cybersecurity-moody-s-idUSKBN0TC2CP20151123 (date of access: 02.04.2020).

13. KKR adds cyber risk score to its assessment of companies. Bloomberg, 2014. URL: http://www.bloomberg.com/news/articles/2014-04-11/kkr-adds-cyber-risk-score-to-its-assessment-of-companies (date of access: 02.04.2020).

14. Society for Risk Analysis (SRA). 2020. URL: https://www.sra.org/risk-analysis-introduction/ (date of access: 23.05.2020).

15. Scardovi C. Digital Transformation in Financial Services. London: Springer International Publishing AG, 2017. 236 p. URL: https://doi:10.1007/978-3-319-66945-8 (date of access: 14.02.2021).

16. Towards an Integrative Approach. International Risk Governance Council (IRGC). White Paper on Risk Governance. Geneva, 2005. URL: www.irgc.org (date of access: 04.06.2020).

17. Boyson S. Cyber supply chain risk management: Revolutionizing the strategic control of critical it systems // Technovation. 2014. No. 34 (7). P. 342–353.

18. A cloud-edge based data security architecture for sharing and analysing cyber threat information / D. Chadwick [et al.] // Future Generation Computer Systems. 2020. No. 102. P. 710–722.

19. Andrade R., Yoo S. Cognitive security: A comprehensive study of cognitive science in cybersecurity // Journal of Information Security and Applications. 2019. No. 48. P. 13. URL: https://doi.org/10.1016/jjisa.2019.06.008 (date of access: 08.01.2020).

20. Tomlin B. On the value of mitigation and contingency strategies for managing supply chain disruption risks // Management Science. 2006. No. 52 (5). P. 639–657. URL: https://doi.org/10.1287/mnsc.1060.0515 (date of access: 03.01.2019).

21. Ruan K. Principles of Cybernomics. Digital Asset Valuation and Cyber Risk Measurement. Cambridge: Elsevier Inc., 2019. P. 141–158. URL: https://doi.org/10.1016/B978-0-12-812158-0.00009-0 (date of access: 23.11.2020).

22. Gerber M., von Solms R. Management of risk in the information age // Computer Security. 2005. No. 24. P. 16–30.

23. Lacon M., Marron S. Risk Assessment and Monitoring in Intelligent Data-Centric Systems. Security and Resilience in Intelligent Data-Centric Systems and Communication Networks. Cambridge: Elsevier Inc., 2018. P. 29–52. URL: https://doi.org/10.1016/B978-0-12-811373-8.00002-1 (date of access: 16.04.2019).

24. Fischer R., Halibozek E., Walters D. Risk Analysis, Security Surveys and Insurance. Introduction to Security. Cambridge: Elsevier Inc., 2019. P. 137–168. URL: https://doi.org/10.1016/B978-0-12-805310-2.00007-X (date of access: 13.08.2020).

25. Nauck F., Usher O., Weiss L. The disaster you could have stopped: Preparing for extraordinary risks. McKinsey&Company, 2020. 9 p. URL: https://www.mckinsey.com/business-functions/risk/our-insights/the-disaster-you-could-have-stopped-preparing-for-extraordinary-risks?cid=other-eml-nsl-mip-mck&hlkid=061d027268294196b455863b2fa7bbd6&hctky=11708326&hdpid=89044107-4811-4e7a-a384-9ca7c398bac6 (date of access: 13.03.2020).

26. Security and Privacy Controls for Federal Information Systems and Organizations. NIST Special Publication 800-53. National Institute of Standards and Technology. URL: https://nvlpubs.nist.gov/nistpubs/Special Publications/NIST.SP.800-53r4.pdf (date of access: 13.03.2020).

27. Introduction to Threat Modeling. Microsoft. URL: https://download.microsoft.com/download/9/3/5/935520EC-D9E2-413E-BEA7-0B865A79B18C/Introduction_to_Threat_Modeling.ppsx (date of access: 10.01.2020).

28. What is the CIA Triad? URL: https://www.forcepoint.com/cyber-edu/cia-triad (date of access: 11.05.2020).

29. Risk and Responsibility in a Hyperconnected World: Pathways to Global Cyber Resilience. WEF (World Economic Forum). Cologny, Switzerland, 2012. URL: https://www3.weforum.org/docs/WEF_IT_PathwaysToGlobalCyberResilience_Report_2012.pdf (date of access: 09.02.2019).

30. Cavusoglu H., Mishra B., Raghunathan S. The effect of Internet security breach announcements on market value of breached firms and Internet security developers // Int. J. Electron. Commerce. 2004. No. 9 (1). P. 69–104.

31. Ruan K. Cyber Risk Measurement in the Hyperconnected World. Digital Asset Valuation and Cyber Risk Measurement Principles of Cybernomics. Cambridge: Elsevier Inc., 2019. P. 75–86. URL: https://doi.org/10.1016/B978-0-12-812158-0.00004-1 (date of access: 11.09.2020).

32. Intelligent manufacturing in the context of Industry 4.0: A review / R. Zhong [et al.] // Engineering. 2017. No. 3 (5). P. 616–630.

33. Organization for Economic Co-Operation and Development (OECD). Emerging Systemic Risks in the 21st Century: An Agenda for Action. Paris, 2003. URL: http://www.oecd.org/ (date of access: 14.08.2019).

34. Managing emerging technology-related risks. Standard Recommendation: CWA 16649: 2013. URL: https://shop.standards.ie/preview/98705249998.pdf?sku=877230_SAIG_NSAI_ NSAI_2084853 (date of access: 28.01.2019).

35. Ellwood P., Reynolds J., Duckworth M. Green Jobs and Occupational Safety and Health: Foresight on New and Emerging Risks Associated with New Technologies by 2020. EU-OSHA (European Agency for Safety and Health at Work). Luxembourg, 2014. URL: http://osha.europa.eu (date of access: 23.07.2019).

36. Huq N. TrendLabs Research. Follow the Data: Dissecting Data Breaches and Debunking Myths: Trend Micro Analysis of Privacy Rights Clearinghouse 2005–2015 Data Breach Records. Tokyo, Japan: Trend Micro, 2015. P. 51. URL: https://documents.trendmicro.com/assets/wp/wp-follow-the-data.pdf (date of access: 04.05.2021).

37. Pursiainen C. Critical infrastructure resilience: A Nordic model in the making? // International Journal of Disaster Risk Reduction. 2018. No. 27. P. 632–641. URL: http://dx.doi.org/10.1016/j.ijdrr.2017.08.006 (date of access: 06.07.2019).

38. Mahdavifar S., Ghorbani A. Application of deep learning to cybersecurity: A survey // Neurocomputing. 2019. No. 347. P. 31–176. URL: https://doi.org/10.1016/j.neucom.2019.02.056 0925-2312 (date of access: 05.11.2020).

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

40. Malecki F. StorageCraft. Best practices for preventing and recovering from a ransomware attack // Computer Fraud & Security. 2019. March. P. 8–10.

41. Annual number of ransomware attacks worldwide from 2014 to 2020. Statista, 2020. URL: https://www.statista.com/statistics/494947/ransomware-attacks-per-year-worldwide/ (date of access: 14.06.2020).

42. Ransomware is Costing UK Companies £346 Million Per Annum to their Bottom Line 27th March. 2017. URL: https://www.sentinelone.com/press/ransomware-costing-uk-companies-346-million-per-annum/ (date of access: 18.11.2020).

43. Касперский Е. Цифровой преступный мир самоизолировался, но не ушел на каникулы // Harvard Business Review. Россия. 2021. 5 февр. URL: https://hbr-russia.ru/innovatsii/tekhnologii/854790 (дата обращения: 01.04.2020).

44. Ransomware 2021. Critical Mid-Year Update. Chainalysis. 2021. May. 38 p. URL: https://go.chainalysis.com/rs/503-FAP-074/images/Ransomware-2021-update.pdf (date of access: 03.06.2020).

45. Luh R., Janicke H., Schrittwieser S. AIDIS: Detecting and classifying anomalous behavior in ubiquitous kernel processes // Computers & Security. 2019. No. 84. P. 31–147.

46. 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: 01.01.2020).

47. Chien E., O'Murchu L., Falliere N. W32. duqu: the precursor to the next Stuxnet // Proceedings of the fifth USENIX workshop on large-scale exploits and emergent threats (LEET). 2012. URL: https://www.usenix.org/conference/leet12/workshop-program/presentation/chien (date of access: 25.08.2021).

48. The DUQU 2.0 Technical Details Version: 2.1 (11 June 2015). URL: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07205202/The_Mystery_of_Duqu_2_0_a_sophisticated_cyberespionage_actor_returns.pdf (date of access: 24.01.2020).

49. 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).

50. Europol. The Internet Organized Crime Threat Assessment (iOCTA). 2015. URL: http://www.europol.europa.eu (date of access: 11.10.2019).

51. Kurtz J. Noncivilian Government Context. Hacking Wireless Access Points Cracking, Tracking, and Signal Jacking. 2017. P. 109–128. URL: http://dx.doi.org/10.1016/B978-0-12-805315-7.00008-5 (date of access: 08.07.2019).

52. Urquhart L., McAuley D. Avoiding the Internet of insecure industrial things // Computer Law & Security Review. 2018. No. 34. P. 32–466.

53. Zhang T. A comparative study on sanction system of cyber aider from perspectives of German and Chinese criminal law // Computer Law & Security Review: The International Journal of Technology Law and Practice. 2017. No. 33 (1). P. 98–102. DOI: 10.1016/j.clsr.2016.11.017.

54. Ransomware threat success factors, taxonomy, and countermeasures: a survey and research direction / B. Al-Rimy [et al.] // Computers & Security. 2018. P. 49. URL: https://doi.org/10.1016/j.cose.2018.01.001 (date of access: 25.05.2019).

55. Goncharov M. Russian Underground 101. Trend Micro Incorporated. Research Paper. 2012. 29 p. URL: https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf?_ga=2.259319754.1186463633.1634981178-1453004565.1634981175 (date of access: 03.11.2019).

56. PandaLabs Q1 Report: Trojans Account for 80% of Malware Infections, Set New Record. Panda Security. 2013. URL: http://www.pandasecurity.com/mediacenter/press-releases/pandalabs-q1-report-trojans-account-for-80-of-malware-infections-set-new-record/ (date of access: 06.02.2020).

57. Степанова Ю. Криминал перешел в Интернет // Коммерсантъ. 2020. 23 окт. URL: https://www.kommersant.ru/doc/4544119?tg (дата обращения: 23.10.2020).

58. Economic Impact of Cybercrime – No Slowing Down Report, McAfee. 2018. URL: https://goo.gl/QLjj8H (date of access: 15.10.2020).

59. 2017 Norton Cyber Security Insights Report Global Results. 2018. URL: https://goo.gl/nF88NN (date of access: 16.10.2020).

60. Cybercrime victimization and subjective well-being: An examination of the buffering effect hypothesis among adolescents and young adults / M. Kaakinen [et al.] // Cyberpsychology Behavior Social Network. 2017. No. 21 (2). P. 129–137. URL: https://DOI:10.1089/cyber.2016.0728 (date of access: 03.10.2019).

61. Srimoolanathan A. Protecting privacy: are today's national laws a boon or bane? // Biometric Technology Today. 2019. November/December. P. 8–11.

62. Identity Threat and Assessment Prediction (ITAP) 2019'. University of Texas at Austin Center for Identity. URL: https://identity.utexas.edu/research-projects/identity-threat-and-assessment-prediction-itap (date of access: 23.02.2020).

63. Future Series: Cybersecurity, emerging technology and systemic risk. Insight Report November 2020. World Economic Forum. URL: http://www3.weforum.org/docs/WEF_Future_Series_Cybersecurity_emerging_technology_and_systemic_risk_2020.pdf (date of access: 15.04.2021).

64. Cyber Security: Export Strategy'. Department for International Trade. 2018. 20 p. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/693989/CCS151_CCS0118810124-1_Cyber_Security_Export_Strategy_Brochure_Web_Accessible.pdf (date of access: 26.03.2020).

65. Q2 Cyber Security Market Report 2017 published by Cyber Security Ventures. URL: https://cybersecurityventures.com/cybersecurity-market-report/ (date of access: 15.12.2020).

66. The EU's Cybersecurity Strategy in the Digital Decade. European Comission. 2020. URL: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade (date of access: 03.04.2021).

67. Threat Forecasting. Leveraging Big Data for Predictive Analysis / J. Pirc [et al.]. Cambridge: Elsevier, 2016. P. 1–15. URL: http://dx.doi.org/10.1016/B978-0-12-800006-9.00001-X (date of access: 13.12.2019).

References

1. Ruan K. Cyber Risk Management: A New Era of Enterprise Risk Management. Digital Asset Valuation and Cyber Risk Measurement Principles of Cybernomics. Cambridge, Elsevier Inc., 2019, pp. 49–73. Available at: https://doi.org/10.1016/B978-0-12-812158-0.00003-X (accessed 10.10.2020).

2. International Organization for Standardization (ISO). Risk Management – Principles and Guidelines: ISO 31000: 2009. Available at: https://www.iso.org/iso-31000-risk-management.html (accessed 11.04.2020).

3. Quality vocabulary. Availability, reliability, and maintainability terms. Guide to concepts and related definitions: BS 4778-3.1: 1991. London: British Standards Institution, 1991. 32 p.

4. International Risk Governance Council (IRGC). The Emergence of Risks. Contributing Factors. Geneva, 2010. Available at: www.irgc.org (accessed 10.02.2020).

5. Ramezani J., Camarinha-Matos L. Approaches for resilience and antifragility in collaborative business ecosystems. *Technological Forecasting & Social Change*, 2020, no. 151, p. 26. Available at: https://doi.org/10.1016/j.techfore.2019.119846 (accessed 15.04.2020).

6. *Tsifrovyye dividenty. Doklad o mirovom razvitii 2016. Obzor* [Digital dividends. Word Development Report 2016. Overview]. Washington DC, World Bank Group, 2016. 58 p. Available at: https://openknowledge.worldbank.org/bitstream/handle/10986/23347/210671RuSum.pdf (accessed 05.02.2020).

7. Ali M., Azad M., Centeno M., Hao F., van Moorsel A. Consumer-facing technology fraud: Economics, attack methods and potential solutions. *Future Generation Computer Systems*, 2019, no. 100, pp. 408–427. Available at: https://doi.org/10.1016/j.future.2019.03.041 (accessed 14.01.2020).

8. Sharafaldin I., Lashkari A., Ghorbani A. An evaluation framework for network security visualizations. *Computers & Security*, 2019, no. 84, pp. 30–92. Available at: https://doi.org/10.1016/j.cose.2019.03.005 (accessed 24.12.2020).

9. Choo K-Kr. The cyber threat landscape: challenges and future research directions. *Computers & Security*, 2011, no. 30 (8), pp. 719–731.

10. Hunton P. Data attack of the cybercriminal: Investigating the digital currency of cybercrime. *Computer Law & Security Review*, 2012, no. 28, pp. 201–207. Available at: https://10.1016/j.clsr.2012.01.007 (accessed 03.03.2020).

11. NIST. Guide for Conducting Risk Assessments. Special Publication 800-30 Rev 1: US Department of Commerce. Washington, DC, 2012. 95 p. Available at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf (accessed 01.03.2020).

12. Volz D. Cyber attacks loom as growing corporation credit risk. Moody's, 2015. Available at: http://www.reuters.com/article/us-cybersecurity-moody-s-idUSKBN0TC2CP20151123 (accessed 02.04.2020).

13. KKR adds cyber risk score to its assessment of companies. Bloomberg, 2014. Available at: http://www.bloomberg.com/news/articles/2014-04-11/kkr-adds-cyber-risk-score-to-its-assessment-of-companies (accessed 02.04.2020).

14. Society for Risk Analysis (SRA). 2020. Available at: https://www.sra.org/risk-analysis-introduction/ (accessed 23.05.2020).

15. Scardovi C. Digital Transformation in Financial Services. London, Springer International Publishing AG, 2017. 236 p. Available at: https://doi:10.1007/978-3-319-66945-8 (accessed 14.02.2021).

16. Towards an Integrative Approach. International Risk Governance Council (IRGC). White Paper on Risk Governance. Geneva, 2005. Available at: www.irgc.org (accessed 04.06.2020).

17. Boyson S. Cyber supply chain risk management: Revolutionizing the strategic control of critical it systems. *Technovation*, 2014, no. 34 (7), pp. 342–353.

18. Chadwick D., Fan W., Costantino G., de Lemos R., Di Cerbo F., Herwono I., Manea M., Mori P., Sajjad A., Wang X.-S. A cloud-edge based data security architecture for sharing and analysing cyber threat information. *Future Generation Computer Systems*, 2020, no. 102, pp. 710–722.

19. Andrade R., Yoo S. Cognitive security: A comprehensive study of cognitive science in cybersecurity. *Journal of Information Security and Applications*, 2019, no. 48, p. 13. Available at: https://doi.org/10.1016/jjisa.2019.06.008 (accessed 08.01.2020).

20. Tomlin B. On the value of mitigation and contingency strategies for managing supply chain disruption risks. *Management Science*, 2006, no. 52 (5), pp. 639–657. Available at: https://doi.org/10.1287/mnsc.1060.0515 (accessed 03.01.2019).

21. Ruan K. Principles of Cybernomics. Digital Asset Valuation and Cyber Risk Measurement. Cambridge, Elsevier Inc., 2019, pp. 141–158. Available at: https://doi.org/10.1016/B978-0-12-812158-0.00009-0 (accessed 23.11.2020).

22. Gerber M., von Solms R. Management of risk in the information age. *Computer Security*, 2005, no. 24, pp. 16–30.

23. Lacon M., Marron S. Risk Assessment and Monitoring in Intelligent Data-Centric Systems. Security and Resilience in Intelligent Data-Centric Systems and Communication Networks. Cambridge, Elsevier Inc., 2018, pp. 29–52. Available at: https://doi.org/10.1016/B978-0-12-811373-8.00002-1 (accessed 16.04.2019).

24. Fischer R., Halibozek E., Walters D. Risk Analysis, Security Surveys and Insurance. Introduction to Security. Cambridge, Elsevier Inc., 2019, pp. 137–168. Available at: https://doi.org/10.1016/B978-0-12-805310-2.00007-X (accessed 13.08.2020).

25. Nauck F., Usher O., Weiss L. The disaster you could have stopped: Preparing for extraordinary risks. McKinsey&Company, 2020. 9 p. Available at: https://www.mckinsey.com/business-functions/risk/our-insights/the-disaster-you-could-have-stopped-preparing-for-extraordinary-risks?cid=other-eml-nsl-mip-mck&hlkid=061d027268294196b455863b2fa7bbd6&hctky=11708326&hdpid=89044107-4811-4e7a-a384-9ca7c398bac6 (accessed 13.03.2020).

26. Security and Privacy Controls for Federal Information Systems and Organizations. NIST Special Publication 800-53. National Institute of Standards and Technology. Available at: https://nvlpubs.nist.gov/nistpubs/Special Publications/NIST.SP.800-53r4.pdf (accessed 13.03.2020).

27. Introduction to Threat Modeling. Microsoft. Available at: https://download.microsoft.com/download/9/3/5/935520EC-D9E2-413E-BEA7-0B865A79B18C/Introduction_to_Threat_Modeling.ppsx (accessed 10.01.2020).

28. What is the CIA Triad? Available at: https://www.forcepoint.com/cyber-edu/cia-triad (accessed 11.05.2020).

29. Risk and Responsibility in a Hyperconnected World: Pathways to Global Cyber Resilience. WEF (World Economic Forum). Cologny, Switzerland, 2012. Available at: https://www3.weforum.org/docs/WEF_IT_PathwaysToGlobalCyberResilience_Report_2012.pdf (accessed 09.02.2019).

30. Cavusoglu H., Mishra B., Raghunathan S. The effect of Internet security breach announcements on market value of breached firms and Internet security developers. *Int. J. Electron. Commerce*, 2004, no. 9 (1), pp. 69–104.

31. Ruan K. Cyber Risk Measurement in the Hyperconnected World. Digital Asset Valuation and Cyber Risk Measurement Principles of Cybernomics. Cambridge, Elsevier Inc., 2019, pp. 75–86. Available at: https://doi.org/10.1016/B978-0-12-812158-0.00004-1 (accessed 11.09.2020).

32. Zhong R., Xu X., Klotz E., Newman S. Intelligent manufacturing in the context of Industry 4.0: A review. *Engineering*, 2017, no. 3 (5), pp. 616–630.

33. Organization for Economic Co-Operation and Development (OECD). Emerging Systemic Risks in the 21st Century: An Agenda for Action. Paris, 2003. Available at: http://www.oecd.org/ (accessed 14.08.2019).

34. Managing emerging technology-related risks. Standard Recommendation: CWA 16649: 2013. Available at: https://shop.standards.ie/preview/98705249998.pdf?sku=877230_SAIG_NSAI_ NSAI_2084853 (accessed 28.01.2019).

35. Ellwood P., Reynolds J., Duckworth M. Green Jobs and Occupational Safety and Health: Foresight on New and Emerging Risks Associated with New Technologies by 2020. EU-OSHA (European Agency for Safety and Health at Work). Luxembourg, 2014. Available at: http://osha.europa.eu (accessed 23.07.2019).

36. Huq N. TrendLabs Research. Follow the Data: Dissecting Data Breaches and Debunking Myths: Trend Micro Analysis of Privacy Rights Clearinghouse 2005–2015 Data Breach Records. Tokyo, Japan, Trend Micro, 2015, p. 51. Available at: https://documents.trendmicro.com/assets/wp/wp-follow-the-data.pdf (accessed 04.05.2021).

37. Pursiainen C. Critical infrastructure resilience: A Nordic model in the making? *International Journal of Disaster Risk Reduction*, 2018, no. 27, pp. 632–641. Available at: http://dx.doi.org/10.1016/j.ijdrr.2017.08.006 (accessed 06.07.2019).

38. Mahdavifar S., Ghorbani A. Application of deep learning to cybersecurity: A survey. *Neurocomputing*, 2019, no. 347, pp. 31–176. Available at: https://doi.org/10.1016/j.neucom.2019.02.056 0925-2312 (accessed 05.11.2020).

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

40. Malecki F. StorageCraft. Best practices for preventing and recovering from a ransomware attack. *Computer Fraud & Security*, 2019, March, pp. 8–10.

41. Annual number of ransomware attacks worldwide from 2014 to 2020. Statista, 2020. Available at: https://www.statista.com/statistics/494947/ransomware-attacks-per-year-worldwide/ (accessed 14.06.2020).

42. Ransomware is Costing UK Companies £346 Million Per Annum to their Bottom Line 27th March. 2017. Available at: https://www.sentinelone.com/press/ransomware-costing-uk-companies-346-million-per-annum/ (accessed 18.11.2020).

43. Kaspersky E. The digital underworld isolated itself, but did not go on vacation. *Harvard Business Review*. Russia, 2021, February 5. Available at: https://hbr-russia.ru/innovatsii/tekhnologii/854790 (accessed 01.04.2020).

44. Ransomware 2021. Critical Mid-Year Update. Chainalysis. 2021, May, 38 p. Available at: https://go.chainalysis.com/rs/503-FAP-074/images/Ransomware-2021-update.pdf (accessed 03.06.2020).

45. Luh R., Janicke H., Schrittwieser S. AIDIS: Detecting and classifying anomalous behavior in ubiquitous kernel processes. *Computers & Security*, 2019, no. 84, pp. 31–147.

46. 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 01.01.2020).

47. Chien E., O'Murchu L., Falliere N. W32. duqu: the precursor to the next Stuxnet. *Proceedings of the fifth USENIX workshop on large-scale exploits and emergent threats (LEET)*, 2012. Available at: https://www.usenix.org/conference/leet12/workshop-program/presentation/chien (accessed 25.08.2021).

48. The DUQU 2.0 Technical Details Version: 2.1 (11 June 2015). Available at: https://media.kaspersky-contenthub.com/wp-content/uploads/sites/43/2018/03/07205202/The_Mystery_of_Duqu_2_0_a_sophisticated_cyberespionage_actor_returns.pdf (accessed 24.01.2020).

49. 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).

50. Europol. The Internet Organized Crime Threat Assessment (iOCTA). 2015. Available at: http://www.europol.europa.eu (accessed 11.10.2019).

51. Kurtz J. Noncivilian Government Context. Hacking Wireless Access Points Cracking, Tracking, and Signal Jacking. 2017, pp. 109–128. Available at: http://dx.doi.org/10.1016/B978-0-12-805315-7.00008-5 (accessed 08.07.2019).

52. Urquhart L., McAuley D. Avoiding the internet of insecure industrial things. *Computer Law & Security Review*, 2018, no. 34, pp. 32–466.

53. Zhang T. A comparative study on sanction system of cyber aider from perspectives of German and Chinese criminal law. *Computer Law & Security Review: The International Journal of Technology Law and Practice*, 2017, no. 33 (1), pp. 98–102. DOI: 10.1016/j.clsr.2016.11.017.

54. Al-Rimy B., Maarof M., Zainuddin S., Shaid M. Ransomware threat success factors, taxonomy, and countermeasures: a survey and research direction. *Computers & Security*, 2018, p. 49. Available at: https://doi.org/10.1016/j.cose.2018.01.001 (accessed 25.05.2019).

55. Goncharov M. Russian Underground 101. Trend Micro Incorporated. Research Paper. 2012. 29 p. Available at: https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf?_ga=2.259319754.1186463633.1634981178-1453004565.1634981175 (accessed 03.11.2019).

56. PandaLabs Q1 Report: Trojans Account for 80% of Malware Infections, Set New Record. Panda Security. 2013. Available at: http://www.pandasecurity.com/mediacenter/press-releases/pandalabs-q1-report-trojans-account-for-80-of-malware-infections-set-new-record/ (accessed 06.02.2020).

57. Stepanova Yu. Crime moved to the Internet. *Kommersant*, 2020, 23 October. Available at: https://www.kommersant.ru/doc/4544119?tg (accessed 23.10.2020).

58. Economic Impact of Cybercrime – No Slowing Down Report, McAfee. 2018. Available at: https://goo.gl/QLjj8H (accessed 15.10.2020).

59. 2017 Norton Cyber Security Insights Report Global Results. 2018. Available at: https://goo.gl/nF88NN (accessed 16.10.2020).

60. Kaakinen M., Keipi T., Rasanen P., Oksanen A. Cybercrime victimization and subjective well-being: An examination of the buffering effect hypothesis among adolescents and young adults. *Cyberpsychology Behavior Social Network*, 2017, no. 21 (2), pp. 129–137. Available at: https://DOI:10.1089/cyber.2016.0728 (accessed 03.10.2019).

61. Srimoolanathan A. Protecting privacy: are today's national laws a boon or bane? *Biometric Technology Today*, 2019, November/December, pp. 8–11.

62. Identity Threat and Assessment Prediction (ITAP) 2019'. University of Texas at Austin Center for Identity. Available at: https://identity.utexas.edu/research-projects/identity-threat-and-assessment-prediction-itap (accessed 23.02.2020).

63. Future Series: Cybersecurity, emerging technology and systemic risk. Insight Report November 2020. World Economic Forum. Available at: http://www3.weforum.org/docs/WEF_Future_Series_Cybersecurity_emerging_technology_and_systemic_risk_2020.pdf (accessed 15.04.2021).

64. Cyber Security: Export Strategy'. Department for International Trade. 2018. 20 p. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/693989/CCS151_CCS0118810124-1_Cyber_Security_Export_Strategy_Brochure_Web_Accessible.pdf (accessed 26.03.2020).

65. Q2 Cyber Security Market Report 2017 published by Cyber Security Ventures. Available at: https://cybersecurityventures.com/cybersecurity-market-report/ (accessed 15.12.2020).

66. The EU's Cybersecurity Strategy in the Digital Decade. European Commission. 2020. Available at: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade (accessed 03.04.2021).

67. Pirc J., DeSanto D., Davison I., Gragido W. Threat Forecasting. Leveraging Big Data for Predictive Analysis. Cambridge, Elsevier, 2016, pp. 1–15. Available at: http://dx.doi.org/10.1016/B978-0-12-800006-9.00001-X (accessed 13.12.2019).

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 20.09.2021