Кибербезопасность в условиях цифровой трансформации

В. А. Артамонов, доктор технических наук, профессор, академик МАИТ
E-mail: artamonov@itzashita.ru
220012, ул. Сурганова, 6, г. Минск, Республика Беларусь
Е. В. Артамонова, кандидат технических наук, член МАИТ
E-mail: admin@itzashita.ru
220012, ул. Сурганова, 6, г. Минск, Республика Беларусь

Аннотация. В статье рассматриваются вопросы кибербезопасности в условиях процесса цифровой трансформации экономики и развития общественных отношений. Дано понятийное определение кибербезопасности и киберпространства в соответствии с международной практикой стандартизации процессов информационных технологий. Согласно стандарта ISO/IEC 27032, определено положение кибербезопасности относительно других сфер информационной безопасности. С позиций риск-ориентированного подхода рассмотрены актуальные аспекты кибербезопасности, с опорой на лучшие практики международных стандартов в области защищённости в условиях киберугроз как внешних, так и внутренних. Опираясь на глобальные статистические исследования, выявлены актуальные угрозы цифровой трансформации, которые она привносит в процесс кибербезопасности. Приведено ранжирование этих угроз по степени их значимости. Даны практические советы и рекомендации по противостоянию этим угрозам и снижению рисков от потерь реализации наиболее опасных кибератак.
Ключевые слова: информационно-коммуникационные технологии (ИКТ), безопасность ИКТ, кибербезопасность, политика безопасности, киберпространство, киберугрозы, риски, уязвимости, активы, владельцы, нарушители, оценки, цифровая трансформация, руководящие указания.
Для цитирования: Артамонов, В. А. Кибербезопасность в условиях цифровой трансформации /В. А. Артамонов, Е. В. Артамонова //Цифровая трансформация. – 2021. – № 4 (17). – С. 42–51.

The Cybersecurity in Conditions of the Digital Transformation

V. A. Artamonov, Doctor of Technical Sciences, Professor, the full member of IAIT, UN
E-mail: artamonov@itzashita.ru
220012, st. Surganova, 6, Minsk, Republic of Belarus
E. V. Artamonova, PhD (Tech.), member of IAIT, Belarus, UN
E-mail: admin@itzashita.ru
220012, st. Surganova, 6, Minsk, Republic of Belarus

Abstract. The paper deals with the issues of cybersecurity in the conditions of digital transformation and the development of society. The authors define cybersecurity and cyberspace by following international practice and IT standardization. According to the ISO/IEC 27032 standard, the cybersecurity position concerning other security domains is defined. Based on the best practices of IT international standards, the authors have considered the current aspects of cybersecurity threats, both external and internal. Considering the results of global statistical research, the authors have identified the current threats to digital transformation in organizations. The paper deals with guidelines to reducing the risks from losses of dangerous cyberattacks.
Key words: Information and communication technologies (ICT), ICT safety, cybersecurity, security policy, cyberspace, cybersecurity threats, risks, vulnerabilities, assets, owners, intruders, assessments, digital transformation, guidelines.
For citation: Artamonov V. A., Artamonova. The Cybersecurity in Conditions of the Digital Transformation *Cifrovaja transformacija* [Digital transformation], 2021, 4 (17), pp. 42–51(in Russian).

Вводная часть. Прежде чем перейти к основному вопросу влияния цифровой трансформации (ЦТ) на кибербезопасность (КБ) продуктов и систем информационных технологий, давайте сформулируем понятийную сущность этих процессов.

Среди специалистов сложился ряд направлений толкования определения «кибербезопасность», отражающего различные аспекты военной политики, международного права, критической информационной инфраструктуры (КИИ), информационно-коммуникационных технологий (ИКТ), компьютерных сетей и т.д. [1]. В связи с этим, на рынке информационных технологий (ИТ) часто возникает путаница в понятиях «информационная безопасность» и «кибербезопасность», хотя под «кибербезопасностью» подразумевается, исключительно, совокупность технологий, процессов и практик, предназначенных для защиты сетей, компьютеров, программ и данных от атак, повреждений или несанкционированного доступа. При этом в контексте компьютерных технологий под термином «информационная безопасность» (ИБ) подразумевается кибербезопасность.

Для разрешения данных противоречий компания Gartner дала собственное понятийное толкование кибербезопасности [2], позднее вошедшее в международный стандарт ISO/IEC 27032-2012 [3].

Кибербезопасность (англ. – cybersecurity) — это сочетание людей, политик, процессов и технологий, используемых предприятием для защиты своих киберактивов. Кибербезопасность оптимизирована до уровней, определяемых бизнес-лидерами, с уравновешиванием требуемых ресурсов с удобством использования, управляемостью и степенью компенсации риска. Подмножества кибербезопасности включают ИТ-безопасность, безопасность Интернета вещей (IoT), ИБ и безопасность операционных технологий (ОТ).

Тезаурус кибербезопасности интегрирован с понятиями информационной безопасности, безопасности приложений, сетевой безопасности, безопасности сети Интернет, а также безопасности критической информационной инфраструктуры. По аналогии с классическим определением информационной безопасности, в стандарте, под кибербезопасностью фактически понимают свойство защищенности активов от угроз конфиденциальности, целостности, доступности информации, но в некоторых абстрактных рамках, речь идет о киберпространстве.

Киберпространство (англ. – cyberspace) формулируется как комплексная виртуальная среда (не имеющая физического воплощения), сформированная в результате действий людей, программ и сервисов в сети Интернет или других структур посредством соответствующих ИКТ.

Безопасность приложений определяется в отношении программных приложений, а также информационно-программных ресурсов и процессов, участвующих в их жизненном цикле. Безопасность сетей связана с проектированием, внедрением и использованием сетей ИКТ внутри организации, между организациями, между организациями и пользователями. Безопасность в сети Интернет касается интернет-услуг и соответствующих систем информационно-коммуникационных технологий. Безопасность КИИ характеризует защищенность от соответствующих угроз, в том числе угроз ИБ. Иллюстрация соотношения названных понятий (как ее определили в международном комитете ISO JTC 1) представлена на рис.1.

Характерной особенностью данного стандарта в интерпретации международного комитета ISO JTC 1 является следующее:

Киберпреступность (англ. – cybercrime) вообще является отдельной сущностью и не имеет никакого отношения ни к информационной безопасности, ни к кибербезопасности. Также, как и понятие cybersafety, смысл которого — это безопасное поведение в киберпространстве.

В ряде научных источников определено, что предвестником 4-й промышленной революции (Индустрия 4.0) является цифровая трансформация (ЦТ), также ей дается определение.

Цифровая трансформация — это процесс интеграции цифровых технологий во все аспекты бизнес-деятельности и инфраструктуру общественных отношений, требующий внесения коренных изменений в технологии, культуру, финансовые операционные технологии и принципы создания новых продуктов и услуг [4]. Для максимально эффективного использования новых технологий и их оперативного внедрения во все сферы деятельности человека, предприятия и бизнес должны отказаться от прежних устоев и полностью преобразовать процессы и модели работы. Цифровая трансформация требует смещения акцентов на периферию предприятий и повышение гибкости центров обработки данных (ЦОД), а

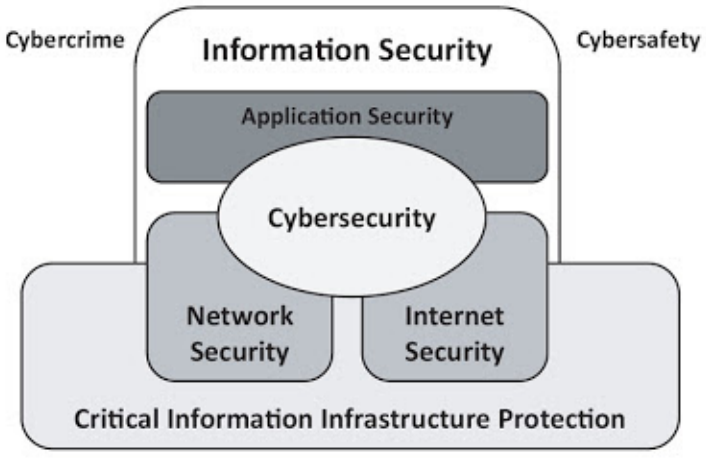

Figure 1 — Relationship between Cybersecurity and other security domains

Рис. 1. Положение кибербезопасности относительно других сфер безопасности
Источник: Международный стандарт ISO/IEC 27032-2012 [3]
Fig.1. The cybersecurity position concerning other security domains
Source: ISO/IEC 27032-2012 [3]

также облачных вычислений, поддерживающих периферию. Этот процесс означает постепенный отказ от устаревших технологий, обслуживание которых может дорого обходиться предприятиям, несет в себе изменение культуры производства (переход к Интернету вещей, IoT), которое, в результате, поддерживает ускорение производственных процессов, обеспечиваемое ЦТ.

Вместе с тем, ЦТ предъявляет совершенно особые вызовы компаниям и выявляет новые киберугрозы для систем ИКТ в результате чего, большинство организаций в этих условиях уже не соответствуют требованиям по кибербезопасности. Далее перейдём к основной части нашей работы, в которой попытаемся дать современную интерпретацию противостояния угрозам КБ в условиях ЦТ.

Концептуальные аспекты кибербезопасности. Как мы уже определили выше, кибербезопасность является сущностью информационно-коммуникационных технологий, глобальной задачей которой является защита активов компаний (владельцев) от угроз и злонамеренных воздействий в киберпространстве со стороны нарушителей как внешних, так и внутренних.

Поэтому, в основу анализа основных составляющих кибербезопасности, целесообразно положить фундаментальные положения стандарта ГОСТ Р ИСО/МЭК 15408-1-2012, более известного под названием «Общие критерии» [5], с учётом основных положений стандарта ISO/IEC 27032-2012.

Положения стандарта ИСО/МЭК 15408 обеспечивают сопоставимость результатов независимых оценок безопасности. В ИСО/МЭК 15408 это достигается предоставлением единого набора требований к функциональным возможностям безопасности продуктов ИТ и к мерам доверия, применяемым к этим продуктам ИТ при оценке безопасности.

Многие киберактивы предприятий представлены в виде информации, которая хранится, обрабатывается и передается средствами ИТ таким образом, чтобы удовлетворить требованиям безопасности владельцев этой информации. Владельцы информации при этом должны предполагать, что доступность, распространение и модификация любой такой информации строго контролируется и активы защищены от угроз контрмерами.

Рис. 2 иллюстрирует высокоуровневые понятия безопасности в контексте риск-ориентированного подхода к оценке кибербезопасности.

Следующим этапом концептуальной основы кибербезопасности является оценка достигнутого уровня кибербезопасности. В процессе оценки достигается определенный уровень уверенности в том, что функциональные возможности безопасности таких продуктов ИТ, а также меры доверия, предпринятые по отношению к таким продуктам, отвечают предъявляемым требованиям. Результаты оценки могут помочь потребителям решить — отвечают ли продукты ИТ их потребностям в безопасности. На рис.3 представлен алгоритм оценки и взаимосвязь составляющих кибербезопасности.

Угрозы и риски кибербезопасности, прив-

Рис.2. Понятия кибербезопасности в контексте риск-ориентированного подхода защиты владельцев активов предприятий
Источник: Стандарт ГОСТ Р ИСО/МЭК 15408-1-2012 [5]
Fig.2. The concept of cybersecurity in the context of risk-based approach to protect assets of business owners
Source: ISO/IEC 15408-1-2012 [5]

Рис.3. Алгоритм оценки и взаимосвязь составляющих кибербезопасности
Источник: Стандарт ГОСТ Р ИСО/МЭК 15408-1-2012 [5]
Fig.3. Algorithm for assessment and the relationship of the cybersecurity components
Source: ISO/IEC 15408-1-2012 [5]

несённые цифровой трансформацией. Известно, что цифровая трансформация оказывает значительное влияние на технологии: от принятия решений на основе данных до внедрения облачных технологий, мобильности и взрывного развития Интернета вещей (IoT), при этом сам процесс ЦТ выходит за рамки простого развертывания новых решений в области ИКТ-технологий. В ходе ЦТ организации должны пересмотреть сложившиеся бизнес-модели и процессы для стимулирования инноваций и улучшения результатов своей деятельности. Именно совместное применение цифровых технологий и информационных процессов дает поводы для переосмысления моделей бизнеса, и это нелегкая задача.

Эффективная трансформация бизнес-процессов требует совместных усилий всех подразделений с участием партнеров, клиентов и других заинтересованных сторон. Императивы цифровой трансформации требуют коренного переосмысления проблем безопасности ИКТ для достижения главной цели — обеспечения кибербезопасности активов предприятий и устойчивости, как ко внешним, так и внутренним угрозам.

Интеграция бизнес-систем, ИТ и ОТ, позволяющих принимать решения на основе потоков данных, создает новые проблемы безопасности, поскольку вновь подключенные системы также могут увеличить ущерб от атак в корпоративных сетях. В дальнейшем, система безопасности должна стать целостной и автоматизированной с самого начала, а не собираться воедино с течением времени из отдельных программно-технических решений.

Чтобы охватить влияние такого глобального процесса, как ЦТ на кибербезопасность систем ИКТ, аналитикам и специалистам по ИБ необходимо опираться на статистику. Именно с этой целью компания Fortinet выпустила отчет о последствиях цифровой трансформации для безопасности в 2018 году [6]. В ходе этого исследования было опрошено 300 руководителей служб безопасности компаний (CISO/CSO) с численностью сотрудников не менее 2500 человек из различных отраслей промышленности по всей Северной Америке, Европе, Азии и Австралии. Цель опроса — собрать данные о ходе цифровой трансформации в этих компаниях, а также выявить проблемные места ЦТ.

Исходя из результатов этих статистических исследований, рассмотрим основные ИТ-тренды, влияющие на базовые бизнес-процессы компаний.

В таблице 1 приведена степень влияния основных ИТ-трендов (в %) на структуру бизнеса.

Из всех опрошенных специалистов, 92% ре-

Таблица1. Влияние ИТ-трендов на бизнес-процессы компании.
Примечание: Выполнена на основе интерпретации инфографики отчёта [6]
Table 1. Influence of IT trends on the company's business processes.
Note: Implications-of-Digital-Transformation-Report [6]

№ п/п	Наименование ИТ-технологий	Оценка влияния ИТ- трендов (в %)		
		Крайне важно	Безразлично	Совершенно не важно
1	Цифровая трансформация	92%	6%	2%
2	Интернет вещей (IoT)	78%	16%	6%
3	Краудлендинг или кредитный краудфандинг	56%	34%	10%
4	Программно – определяемые (маршрутизируемые) глобальные сети	28%	55%	17%
5	Облачные и периферийные вычисления	11%	32%	57%
6	Блокчейн	10%	25%	66%

спондентов оценили процесс ЦТ, как имеющий «довольно большой» или «чрезвычайно большой» эффект для организации.

Второе и третье место в рейтинге влияния на бизнес получили две тенденции, которые часто считаются элементами ЦТ: IoT (78%), искусственный интеллект (AI) и машинное обучение (56%).

Вывод 1: Цифровая трансформация является самым влиятельным трендом для бизнеса в последние 5 лет и на будущее.

Далее перейдём к оценке влияния ЦТ на значимость киберугроз.

В таблице 2 приведены значимости угроз кибербезопасности систем ИКТ, создаваемые ЦТ (в %).

В настоящее время, во многих публикациях и на ИТ-форумах, организационные вопросы и ограничения, которые несут в себе устаревшие технологии, обсуждаются, как самые большие проблемы для ЦТ, что отчасти имеет место в реальной деятельности компаний. Однако специалисты по информационной безопасности, в подавляющем большинстве уверены, что проблемы безопасности являются самыми большими препятствиями для реализации ЦТ. Согласно проведенным исследованиям, 85% опрошенных CISO/CSO (руководителей и специалистов информационной безопасности компаний) оценивают проблемы безопасности, как имеющие «довольно большое» или «чрезвычайно большое» влияние на бизнес-процессы в организациях. Кроме того, второй, наиболее распространенный ответ (56%) связан с соблюдением требований регуляторов.

Руководители служб информационной безопасности особое внимание уделяют двум источникам риска: внешнему и внутреннему.

Таблица 2. Атаки, угрозы и уязвимости ЦТ
Примечание: Выполнена на основе интерпретации инфографики отчёта [6]
Table 2. Attacks, threats and vulnerabilities of the DT
Note: Implications-of-Digital-Transformation-Report [6]

№ п/п	Атаки, угрозы и уязвимости цифровой трансформации (ЦТ)	Значимость угроз (%)	Рекомендации по обнаружению и предотвращению атак, ликвидацию угроз и уязвимостей ЦТ
1	Полиморфные атаки	85%	Внедрение SIEM-систем и систем мониторинга на базе систем ИИ и глубокого машинного обучения Deep learning
2	Угрозы технологии Dev Ops	81%	Перейти на более безопасную технологию Dev Sec Ops
3	Уязвимости «слепых» зон инфраструктуры ИТ-системы	70%	Принять меры для придания прозрачности инфраструктур ИТ-систем, подлежащих ЦТ
4	Рост атакующего потенциала киберпреступников	68%	Широкое внедрение систем автоматизации и интеграции ИБ инфраструктур ИТ-систем, подлежащих ЦТ
5	Широкое использование протокола SSL	57%	Для снижения доли фишинговых атак следует перейти на EVSSL
6	Угрозы и уязвимости интернета вещей (IoT)	47%	Использование технологии Блокчейн для управления аутентификацией, обеспечения неделимости информации и работоспособности ИТ-сервисов
7	Расширение пространства реализации угроз	34%	Использование проактивных методов защиты информации
8	Незащищённость клиентских данных	28%	Использование криптографических методов защиты информации
9	Возрастание времени простоя ИТ-системы	23%	Комплексное решение вопросов безопасности для обеспечения непрерывности бизнес-процессов компании

Рост полиморфных атак и угроз, которые постоянно трансформируются или изменяются, чтобы избежать обнаружения, 85% специалистов по ИБ оценивают как «довольно большую» или «чрезвычайно большую» проблему [7]. Также следует обратить внимание (81%) на рост негативного влияния технологии DevOps, который, по мнению опрошенных CISO/CSO, позволяет уязвимостям «проникать» в корпоративную сеть вместе с более ускоренными темпами разработки ПО. Именно эта тенденция начинает усиливаться в последнее время [8]. Обе эти угрозы потенциально могут увеличиться по мере того как поверхность атаки становится более сложной в контексте проходящей в компании ЦТ. Учитывая важность этих угроз для кибербезопасности, дадим расширенное толкование этим опасным технологиям.

Полиморфизм заключается в формировании программного кода вредоносной программы «на лету» уже во время исполнения, при этом сама процедура, формирующая код, также не должна быть постоянной и видоизменяется при каждом новом заражении. Во многих случаях, изменение вредоносного кода достигается путём добавления операторов, которые не изменяют сам алгоритм работы программы (например, оператор NOP). Постоянное видоизменение программного кода вредоносной программы не позволяет создать универсальную сигнатуру для данного образца. Специалисты по кибербезопасности для противодействия этому методу в антивирусном программном обеспечении успешно применяют такие технологии, как эвристический анализ на основе ИИ и эмуляцию.

Немного остановимся на такой популярной в последнее время в ИТ-компаниях технологии, как DevOps.

Методология DevOps означает интеграцию деятельности разработчиков и специалистов по обслуживанию ПО, сетей и оборудования в командах и компаниях. DevOps является предметом особой настороженности специалистов ИБ, так как она принципиально изменила взаимоотношения между разработчиками программного и аппаратного обеспечения, системными администраторами, службами технической поддержки и конечными пользователями.

Еще одна серьезная проблема — это отсутствие полной видимости всех зон и процессов систем ИКТ для специалистов отделов безопасности (70%), учитывая все более сложную вычислительную инфраструктуру, которую представляет ЦТ. Эта проблема также может являться результатом наследия не интегрированных в корпоративную сеть организации, многопозиционных систем и ИТ-продуктов (применявшихся ранее в оборонной промышленности). Для обеспечения безопасности сложных, высокоразвитых распределенных сред, охватывающих удаленные филиалы, корпоративные ЦОД и гибридные облака, службы безопасности должны поддерживать наиболее полную видимость для выявления аномального поведения систем и быстрой нейтрализации угроз.

Цифровая трансформация также создала акцент на защиту конфиденциальности и более высокие требования к ее соблюдению. По мере того, как кибератаки становятся все более изощренными и разрушительными, регулирующие органы устанавливают более строгие правила и руководящие принципы защиты персональной идентификационной информации (англ. – personally identifiable information, PII). В результате, организации должны помнить о комплаенсе (соответствие каким-либо внутренним или внешним требованиям, или нормам, англ. – compliance) и обращаться к лучшим в своем классе сертифицированным продуктам, процессам и специалистам, чтобы обеспечить должный уровень управления рисками. Еще до начала ЦТ, системы информационной безопасности, по умолчанию, на предприятии включали несколько разрозненных хранилищ с локальными службами и развертывались, как правило, в нескольких облачных сервисах с различными инструментами безопасности.

Стратегия ЦТ может привести к еще более сложной среде, с еще большим количеством «облаков/ЦОД» и увеличением количества устройств IoT, многие из которых не были разработаны с учетом требований кибербезопасности.

Особое внимание необходимо уделить инцидентам ИБ на объектах критической информационной инфраструктуры (КИИ), это могут быть, как таргетированные атаки (англ. – advanced persistent threat, APT), так и техногенные катастрофы, физическое похищение активов и др. угрозы. По мере усложнения атак наращиваются и «средства обороны» (т.е. инфраструктура кибербезопасности).

Вывод 2: Самый большой вызов для реализации ЦТ — это безопасность и устойчивость систем к кибератакам и отсутствие прозрачности

инфраструктуры кибербезопасности в ходе ЦТ.

На этом фоне все большую популярность набирают интеллектуальные системы управления кибербезопасностью — SIEM (англ. – Security information and event management), основная задача которых — это мониторинг корпоративных систем и анализ событий безопасности в режиме реального времени, в том числе с широким использованием систем искусственного интеллекта (ИИ) и глубокого машинного обучения (англ. – Deep learning) [9].

Вывод 3: Использование высокоинтеллектуальных систем для управления кибербезопасностью является актуальным трендом времени.

Однако не все организации так далеко продвинулись во внедрении современных методов обеспечения кибербезопасности, упомянутых в [6]. Также нужно учесть, что компания Fortinet проводила свои статистические исследования в основном среди организаций ТОП–уровня, т.е. в так называемых высокоуровневых компаниях. И поэтому о состоянии кибербезопасности в организациях среднего и низкого уровня можно только догадываться. Проекты по интеграции решений безопасности, обеспечению сквозной прозрачности и автоматизации контроля соответствия все еще находятся в стадии реализации в 30–40% организаций и завершены менее чем в одной трети компаний. Однако уже сам факт того, что многие из них находятся в стадии развертывания, указывает, что организации осознают веление времени в части кибербезопасности и начинают двигаться в попытках опережать развивающиеся угрозы.

По средним оценкам специалистов CISO/CSO, около 25% инфраструктуры не защищены от сегодняшних угроз безопасности. По мере расширения поверхности атаки устаревшие архитектуры безопасности часто не могут масштабироваться для удовлетворения новых требований. Даже если точечные решения развернуты для обеспечения некоторой защиты возникающей в результате распространения разрозненных систем, означает, что общий профиль безопасности организации не может быть значительно улучшен.

Уязвимости, которые можно устранить с помощью обновлений программного обеспечения и исправлений, остаются потенциальной проблемой для некоторых организаций. В то время, как почти все организации сообщают, что исправления «в некоторой степени обновлены», и только одна треть указали, что они «чрезвычайно актуальны».

Вывод 4: Значительные составляющие инфраструктуры ИКТ по-прежнему остаются уязвимыми для различного рода кибератак. И в этом проявляется одна из парадигм ЦТ — не все организации одинаково готовы к столь сложному, а порой и длительному процессу преобразований, каковым является цифровая трансформация. Однако прорывное развитие интеллектуальных механизмов управления кибербезопасностью, в том числе на основе ИИ вселяют в нас надежду на минимизацию этой рудиментарной тенденции в обозримой перспективе.

Руководящие указания и заключительные положения. В целях планирования обеспечения кибербезопасности стандарт ISO/IEC 27032-2012 представляет три руководства:

- рекомендации по оценке и отработке рисков от угроз ЦТ;
- рекомендации по соблюдению требований безопасности пользователями;
- рекомендации по обеспечению кибербезопасности для организаций-провайдеров.

Рекомендации по оценке и обработке рисков опираются на ISO/IEC 27005-2010 [10], акцентируя внимание на особенностях кибербезопасности (см. рис.4).

Рекомендации для пользователей составляют совокупность норм поведения, определенных провайдером, а именно:

- понимание политики кибербезопасности контента или приложения;
- понимание рисков кибербезопасности с учётом влияния ЦТ;
- соблюдение политики безопасности персональных данных;
- управление безопасностью личных данных;
- информирование уполномоченных органов о подозрительных явлениях или сообщениях;
- проверка подлинности и понимание политики безопасности торговых площадок (в случае осуществления виртуальных торговых сделок);
- контролирование целостности используемого и разрабатываемого программного обеспечения с учётом угроз DevOps;
- обеспечение безопасности онлайн-публикаций и блогов;
- соблюдение корпоративной политики информационной безопасности в киберпространстве;
- незамедлительное информирование

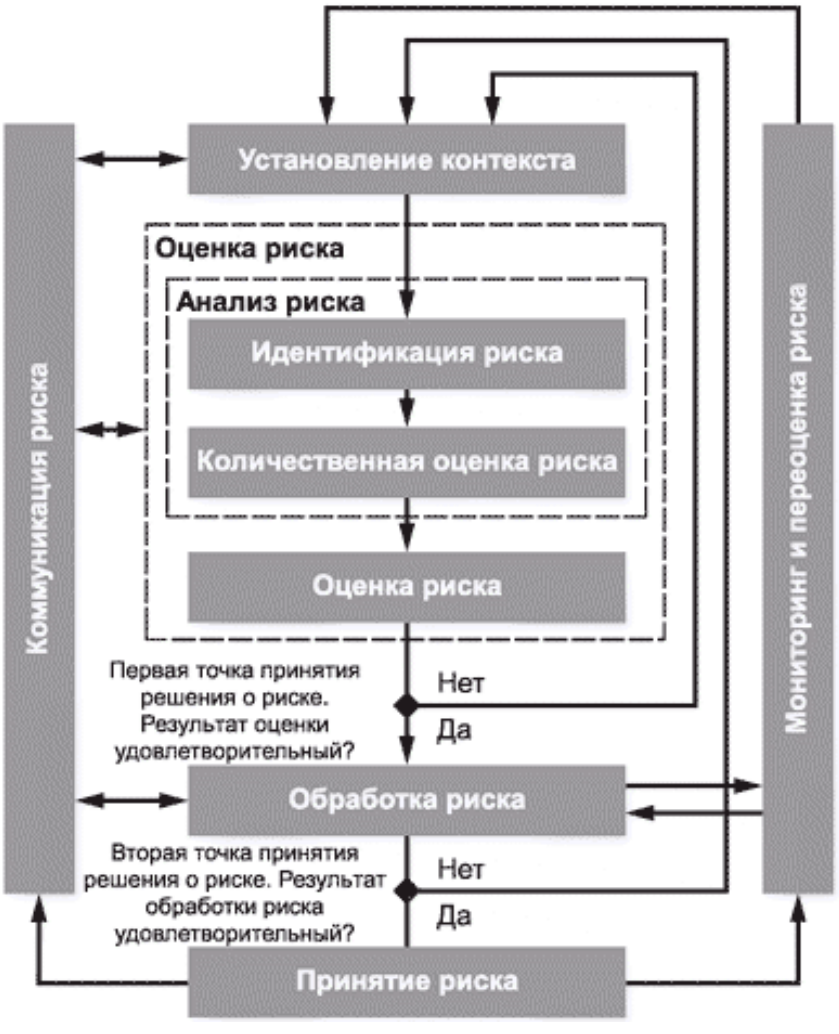

Рис.4. Алгоритм управления рисками кибербезопасности
Fig.4. Cybersecurity Risk Management Algorithm

уполномоченных органов о личных нарушениях безопасности.

Руководящие указания организациям предлагают широкий комплекс мероприятий по управлению кибербезопасностью организацией, а именно:

- внедрение и сертификация системы менеджмента информационной безопасности;
- предоставление безопасных продуктов и систем ИКТ, прошедших соответствующую оценку;
- тестирование, мониторинг сетей и реагирование;
- техподдержка;
- поддержание уровня собственной осведомленности относительно новейших разработок;
- повышение осведомленности пользователей;
- контроль соблюдения политики кибербезопасности и т.д.;
- проектирование архитектуры кибербезопасности организации, которая обеспечивает прозрачность и видимость всей ИТ-инфраструктуры и позволяет осуществлять централизованный контроль за ней;
- выработка стратегии, использующей интеграцию для повсеместной автоматизации рабочих процессов и обмена аналитическими данными об угрозах как вне, так и внутри компании.

Что касается собственно обеспечения кибербезопасности, то в качестве приоритета выделена координация взаимодействия между организациями, формирующими киберпространство, самостоятельные действия которых не обеспечивают эффективную защиту от киберугроз.

Список литературы

1. Dan Craigen, Nadia Diakun-Thibault, and Randy Purse. Defining Cybersecurity. [Электронный ресурс]. – 2021. – Режим доступа: https://www. researchgate.net/publication/267631801_Defining_Cybersecurity/link/54550d9f0cf26d5090a6fa6c/download – Дата доступа: 08.06.21
2.Gartner Information Technology (IT) Glossary — A comprehensive dictionary of Information Technology (IT) terms and definitions. Learn the key terminology related to the Information Technology (IT) industry with this glossary/ [Электронный ресурс]. – 2021. – Режим доступа: https://www.Gartner.com/en/information-technology/glossary/cybersecurity – Дата доступа: 08.06.21.
3. BSI BS ISO/IEC 27032-2012 Информационные технологии. Методы обеспечения безопасности. Руководящие указания по кибербезопасности.
4. Артамонов, В. А., Артамонова, Е.В. Цифровая трансформация экономики как предвестник 4-й промышленной революции // Защита информации ИНСАЙД. – 2019. – №3. – С25–33.
5. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.
6. Fortinet 2018. Security Implications of Digital Transformation Report . [Электронный ресурс]. – 2021. Режим доступа: https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/Fortinet-2018-Security-Implications-of-Digital-Transformation-Report. pdf. – Дата доступа: 08.06.21
7. Полиморфизм компьютерного вируса. [Электронный ресурс]. – 2021. – Режим доступа: https://ru.wikipedia.org/wiki – Дата доступа: 08.06.21.
8. Что такое DevOps? / Описание DevOps | Microsoft Azure. [Электронный ресурс]. – 2021. – Режим доступа: https://azure.microsoft.com/ru-ru/overview/what-is-devops/ – Дата доступа: 08.06.21.
9. Котенко И.В. Интеллектуальные механизмы управления кибербезопасностью//Управление рисками и безопасностью. Труды Института системного анализа Российской академии наук (ИСА РАН). Т.41, Москва, URSS, 2019. С.74–103.
10. ГОСТ Р ИСО/МЭК 27005:2018 Информационные технологии – Техники обеспечения безопасности –Управление рисками информационной безопасности.

References

1. Dan Craigen, Nadia Diakun-Thibault, and Randy Purse. Defining Cybersecurity: https://www. researchgate.net/publication/267631801_Defining_Cybersecurity/link/54550d9f0cf26d5090a6fa6c/download.
2Gartner Information Technology (IT) Glossary: A comprehensive dictionary of Information Technology (IT) terms and definitions. Learn the key terminology related to the Information Technology (IT) industry with this glossary: https://www.Gartner.com/en/information-technology/glossary/cybersecurity
3. BSI BS ISO/IEC 27032-2012 Information technology - Security techniques - Guidelines for cybersecurity
4.Artamonov V. A., Artamonova E. V. The Digital transformation of economy is Industry 4.0 beginning. Zaŝita informacii. Inside. [Zaŝita informacii. Inside]. Nauka Publ., 2019. No.3 pp.25 – 33.
5. ISO/IEC 15408-1. Information technology. Security techniques. Evaluation criteria for IT security. Part 1. Introduction and general model.
6.Fortinet 2018. Security Implications of Digital Transformation Report: https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/Fortinet-2018-Security-Implications-of-Digital-Transformation-Report.pdf.
7. Polymorphic viruses, 2021. Available at: https://ru.wikipedia.org/wiki.(accessed 08.06.21) (in Russian).
8. What is DevOps?/ Overview | Microsoft Azure, 2021. Available at: https://azure.microsoft.com/ru-ru/overview/what-is-devops.(accessed 08.06.21) (in Russian).
9. Kotenko I.V. Intellektual'nye mekhanizmy upravleniya kiberbezopasnost'yu / Upravlenie riskami i bezopasnost'yu.// Trudy Instituta sistemnogo analiza Rossijskoj akademii nauk [Proceeding of the Institute for Systems Analysis of the Russian Academy of Science], 2019, N41, pp 74–03 (in Russian)
10. ISO/IEC27005 Information technology – Security techniques – Information security risk management.

Received: 21.06.2021 *Поступила: 21.06.2021*