Обзорная статья

УДК 004.056.5+007

ББК 32.972.5

К 59

DOI: 10.53598/2410-3225-2021-3-286-88-97

**Кибербезопасность и информационная безопасность:
сходства и отличия**
(Рецензирована)

Наталья Шумафовна Козлова¹, Виталий Анатольевич Довгаль²

¹ Майкопский государственный технологический университет, Майкоп, Россия, natali20052001@bk.ru

² Майкопский государственный технологический университет, Адыгейский государственный университет, Майкоп, Россия, urmia@mail.ru

Аннотация. Проводится анализ понятий «кибербезопасность» и «информационная безопасность», объясняются различия между ними, описывается их эволюция, рассматриваются важные области совпадения, приводятся различные теоретические обоснования – концепции и возможные способы использования. Оценивая современное состояние указанных понятий и сопоставляя их с мировыми тенденциями, определяются основные направления необходимых изменений в рассматриваемых терминах.

Ключевые слова: кибер-безопасность, киберриски, киберугрозы, защита информации, информационная безопасность, информационные системы, цифровые технологии, информация, угрозы, специалисты безопасности

Review article

Cybersecurity and information security: similarities and differences

Natalya Sh. Kozlova¹, Vitaliy A. Dovgal²

¹ Maikop State University of Technology, Maikop, Russia, natali20052001@bk.ru

² Maikop State University of Technology, Adyghe State University, Maikop, Russia, urmia@mail.ru

Abstract. The concepts of “cybersecurity” and “information security” are analyzed, the differences between them are explained, their evolution is described, important areas of overlap are considered, and various theoretical justifications – concepts and possible uses – are given. Assessing the current state of these concepts and matching them with world trends, the main directions of the necessary changes are determined in the terms considered.

Keywords: cyber security, cyber risks, cyber threats, information protection, information security information systems, digital technologies, information, threats, security specialists

Введение

Внедрение цифровых технологий в современную жизнь оказалось стремительным и колоссальным по своим последствиям. Риск для промышленных коммуникационных сетей, особенно тех, которые поддерживают критически важные инфраструктуры (местные, региональные или национальные), в последние годы неуклонно возрастает, поэтому происходит увеличение исследований в области кибербезопасности. В своих результатах некоторые исследователи очень часто взаимозаменяют понятия «кибер-

безопасность» и «информационная безопасность», что вызывает недовольство других профессионалов в области безопасности. В статье приведены важные различия между кибербезопасностью и информационной безопасностью и подробно описано, как эти термины связаны с безопасностью информации, приведены аргументы и примеры их различий и сходства.

Цель исследования заключается в изучении и анализе терминов кибербезопасности и информационной безопасности, а также обосновании сходства и различий, что и обуславливает актуальность статьи. В ходе исследования применялись методы теоретического анализа, синтеза и аналогии.

Ключевые выводы: в статье выявлена необходимость дальнейшего подробного анализа и понимания атак и уязвимостей, благодаря исследованиям, основанным на более глубоком изучении методов угроз и все более сложных режимов атак, таких как сложные постоянные угрозы, программы-вымогатели и атаки на встроенные системы, именно эти аргументы обеспечивают основу для дальнейших исследований.

1. Анализ влияния кибербезопасности в функционировании коммерческой компании

В исследованиях, связанных с обеспечением защиты используемых данных, понятия «кибербезопасность» и «информационная безопасность» часто используются как синонимы. При практически ежедневном внедрении новых технологий и связанного с этим появления огромного количества терминов неудивительно, что ведутся споры о единстве и различии этих терминов обеспечения защиты данных.

Стремительное развитие сетевых и информационных технологий, наблюдающееся на протяжении последнего десятилетия, способствует появлению значимых изменений во всех областях общественной жизни и отраслях. Усиление роли технологий неизбежно ведет к возникновению рисков, связанных с обеспечением цифровой безопасности информации, и побуждает к необходимым своевременным корректировкам ее защиты. Следовательно, система информационной безопасности должна непрерывно подстраиваться под новые условия, чтобы сохранять достаточный уровень защищенности как цифровой информации, так и информации, хранящейся на традиционных носителях.

Помимо стандартных преобразований, связанных с непосредственным совершенствованием технологий, система безопасности должна быстро реагировать на внешние изменения, вызванные вынужденными мерами. Однако многие не были полностью готовы к трансформации формата работы, вызванной эпидемиологическими ограничениями, что спровоцировало появление дополнительных угроз информационной безопасности (утечка персональных данных, несанкционированный доступ посторонних субъектов, нарушение с защитой персональных данных).

В наши дни сфера кибербезопасности развивается быстро, динамично и постоянно, поэтому системе защиты коммерческой компании необходимо совершенствоваться постоянно [1]. Крупные и малые организации подвергаются атакам каждый день, от простых фишинговых писем до сложных, подробных операций, организованных преступными группировками, и для каждой исправленной уязвимости всплывает новая, готовая к эксплуатации. Кибербезопасность не должна стоить огромных денег или требовать много времени для своего внедрения. Независимо от размера коммерческой компании повышение кибербезопасности помогает защитить как собственные данные, так и данные клиентов, что обычно способствует улучшению деловых отношений и открывает новые возможности в ведении бизнеса. Кибербезопасность становится важным компонентом успеха в бизнесе и важнейшей защитой от угроз информационной эпохи.

Инциденты, связанные со взломом, фишингом и вредоносным программным обеспечением (ПО), в настоящее время становятся причиной номер один нарушений безопасности. Кроме того, на попытки взлома оказывают влияние человеческие ошибки. В борьбе с киберпреступниками и предотвращении нарушений безопасности критически важными являются образование и осведомленность.

2. Сопутствующие работы по теме исследования

В рамках исследования было рассмотрено более пятидесяти источников, из которых следует выделить труды М.В. Арсентьева, В.Я. Ищейнова, К.В. Мирошниченко, В.В. Герасимова, в которых зафиксированы подходы к определению информационной безопасности, что может позволить сгруппировать варианты толкования и перейти к исследованию применения новых технологий для защиты информации [2–5].

В учебном пособии [4] приводится следующая трактовка рассматриваемых понятий: «Информационная безопасность – состояние системы, при котором она, с одной стороны, способна противостоять дестабилизирующему воздействию внешних и внутренних информационных угроз, а с другой – ее функционирование не создает информационных угроз для элементов самой системы и внешней среды».

В работе [5] информационная безопасность зафиксирована как «защита информации и поддерживающей ее инфраструктуры с помощью совокупности программных, аппаратно-программных средств и методов, а также организационных мер, с целью недопущения причинения вреда владельцам этой информации или поддерживающей ее инфраструктуре». Предположим, что защита чего-либо – это процесс, а не состояние, следовательно, можно утверждать, что толкование, приведенное в работе [5], более конкретное по сравнению с предыдущим.

В учебном пособии [6] наблюдается схожее раскрытие сущности рассматриваемого понятия: «Информационная безопасность – защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий». Основное отличие – понимание безопасности как состояния среды, а не процесса приобретения, сохранения и контроля безопасности.

В работе [7] отсутствует оформленное определение нужного термина, однако фигурирует цель, на основе которой представляется возможным выделить значения. Информационная безопасность – состояние экономического субъекта, позволяющее ему стабильно развиваться и сохранять целостность.

В доктрине информационной безопасности Российской Федерации, утвержденной Указом Президента РФ от 5 декабря 2016 года № 646, информационная безопасность определена как «состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз» [8].

Кибербезопасность и информационная безопасность настолько тесно связаны, что их часто считают синонимами. Но между ними есть несколько важных различий.

Кибербезопасность определяется NIST (Национальный институт стандартов и технологий) как «способность защищать или защищать использование киберпространства от кибератак». Хотя есть и другие определения – у CISA (Сертифицированный аудитор информационных систем) есть свое определение, как и у ISO (Международная организация по стандартизации), – большинство из них похоже.

Проще говоря, кибербезопасность связана с атаками изнутри или за пределами организации. Это структура защиты всего, что уязвимо для взлома, атак или несанкционированного доступа, что в основном состоит из компьютеров, устройств, сетей, серверов и программ.

Кибербезопасность также относится исключительно к защите данных, исходящих в цифровой форме – она характерна для цифровых файлов, что является ключевым

отличием от информационной безопасности. Поэтому, когда мы говорим о кибербезопасности, мы автоматически обсуждаем цифровую информацию, системы и сети.

3. Проблемы, возникающие в сфере кибербезопасности

Кибербезопасность – это область информационных технологий, ориентированная на защиту систем, включающих в себя электронные записи, устройства для отслеживания информации, оборудование и программное обеспечение, используемое для оказания услуг и управления ими. Кибербезопасность направлена на предотвращение атак путем защиты систем от несанкционированного доступа, использования и раскрытия данных. Основная цель – обеспечить доступность, конфиденциальность и целостность критически важных данных, которые в случае компрометации могут поставить под угрозу жизнь.

Кибератаки могут принимать разные формы – от программ-вымогателей до кражи личной информации. Воздействие атаки может варьироваться в зависимости от размера объекта. Несколько проблем являются общими для всех отраслей промышленности и производства: защита конфиденциальной информации персональных данных, уязвимости устаревших систем, проблемы ИТ и нарушения безопасности.

Информационная безопасность (или “InfoSec”) – это еще один способ сказать «безопасность данных», подразумевая конфиденциальность, целостность и доступность данных (*англ.* CIA). Большинство современных бизнес-данных хранятся в электронном виде на серверах, настольных компьютерах, ноутбуках или в Интернете, но десять лет назад, до того, как вся конфиденциальная информация была перенесена в Интернет, она хранилась в архиве и кабинете.

Информационная безопасность связана с обеспечением безопасности данных в любой форме и является немного более широким понятием, чем кибербезопасность. Поэтому можно считать, что эксперт по информационной безопасности не является специалистом в области кибербезопасности.

Кибербезопасность – это защита данных в электронной форме (например, компьютеров, серверов, сетей, мобильных устройств и т.д.) от компрометации или атак. Частично это определение критических данных, их местонахождения, подверженности рискам и технологии, которую необходимо внедрить для их защиты. Как в кибербезопасности, так и в информационной безопасности есть компонент физической безопасности.

Склад, полный конфиденциальных бумажных документов, нуждается в обеспечении физической защиты. Перевод данных в цифровую форму требует использования более совершенных инструментов защиты этих данных. Не имея возможности поставить физический замок на настольный компьютер, его можно повесить на дверь серверной комнаты. Другими словами, если данные хранятся физически или в цифровом виде, необходимо быть уверенным, что у них есть все необходимые средства контроля физического доступа, чтобы предотвратить доступ посторонних лиц.

Бизнес, связанный с информационной безопасностью, имеет основную задачу защитить данные коммерческой компании от несанкционированного доступа любого рода. Бизнес, связанный с кибербезопасностью, имеет основную задачу обеспечения защиты данных компании от несанкционированного электронного доступа. Но в обоих случаях значение данных имеет первостепенное значение.

Оба специалиста должны знать, какие данные наиболее важны для организации, чтобы сосредоточиться на правильном управлении киберрисками и контроле над этими данными. В некоторых сценариях специалист по информационной безопасности может помочь специалисту по кибербезопасности определить приоритетность защиты данных, а затем специалист по кибербезопасности определит наилучший курс действий

для защиты данных. Но с изменением ландшафта безопасности за последнее десятилетие все не всегда так однозначно.

За последнее десятилетие мы стали свидетелями слияния кибербезопасности и информационной безопасности, поскольку эти ранее разрозненные позиции объединились. Проблема в том, что у большинства команд нет в штате специалиста по информационной безопасности, поэтому обязанности специалиста по кибербезопасности резко расширились. Специалисты по кибербезопасности традиционно понимают, какие технологии, брандмауэры и системы защиты от вторжений необходимы, но не обязательно были связаны с бизнесом по оценке данных.

Поскольку эта тема становится все более важной для бизнеса, роль экспертов по управлению рисками кибербезопасностью меняется для должной защиты данных. Деловые партнеры и инвесторы все больше осознают важность этой темы, и компании заинтересованы в регулярной и эффективной защите данных и управлении как физическими рисками, так и киберрисками.

Кибербезопасность – это особый тип информационной безопасности, относящийся к способам, которыми организации защищают цифровую информацию, такую как сети, программы, устройства, серверы и другие цифровые активы.

Хотя это лишь один из аспектов информационной безопасности (наряду с физической безопасностью), ему уделяется наибольшее внимание, поскольку киберугрозы гораздо более вероятны, чем физические.

Вредоносное ПО, преступный взлом и внутренние ошибки являются основными причинами утечки данных, поэтому имеет смысл уделять приоритетное внимание защите, которая снижает эти риски.

Это не означает, что кибербезопасность и физическая безопасность полностью разделены. Возьмем, например, угрозу кражи устройств. В этом случае необходимы меры физической безопасности, препятствующие попаданию устройств в руки злоумышленников. В первую очередь это будет осуществляться в форме политик, инструктирующих сотрудников о том, как обращаться со своими устройствами, такими как ноутбуки, вне помещений.

Однако они должны быть дополнены мерами кибербезопасности, которые защитят организацию в случае кражи устройства.

Такие меры могут включать парольную защиту устройства и баз данных, шифрование конфиденциальной информации и реализацию аварийного отключения для удаленной очистки украденных ноутбуков.

Из-за эволюции этой позиции легко понять, почему многие люди одновременно обсуждают кибербезопасность и информационную безопасность. Вопросы, на которые пытаются ответить информационная безопасность и кибербезопасность, по сути, одинаковы.

Независимо от того, обеспечивается кибербезопасность или информационная безопасность в целом, необходимо знать о трех столпах безопасности данных. Модель описывает методы защиты конфиденциальной информации и включает:

1. Люди: сотрудники ежедневно обрабатывают конфиденциальную информацию, поэтому важно, чтобы организации информировали их о рисках и о том, как оставаться в безопасности.
2. Процессы: организации должны документировать шаги, которые сотрудники должны предпринять, чтобы оставаться в безопасности. Это должно включать определение ролей и ответственности за действия по защите данных.
3. Технологии: существует бесчисленное множество технических средств защиты, которые организации могут использовать для борьбы с угрозами, например, антивирусное программное обеспечение, контроль доступа и шифрование данных.

Хотя в Интернете по-прежнему ведутся оживленные дискуссии о том, означают ли кибербезопасность и информационная безопасность одно и то же, имеет смысл рассматривать кибербезопасность как форму информационной безопасности. Надо рассматривать информационную безопасность как зонтик, под которым стоит кибербезопасность и другие темы безопасности, такие как криптография и мобильные вычисления. Однако провести четкое различие может быть непросто, учитывая их взаимное расположение в описной иерархии и влияние.

Есть и другие различия в обсуждении кибербезопасности и информационной безопасности. В то время, как кибербезопасность связана с защитой информации в киберпространстве, информационная безопасность означает защиту данных в киберпространстве и за его пределами. Другими словами, Интернет или оконечное устройство могут быть только частью общей картины. Оба включают защиту киберпространства от взломов, которые могут включать программы-вымогатели, шпионское ПО, вредоносное ПО и другие типы вредоносного программного обеспечения, которые могут вызывать разного рода хаос. Однако профессионалы в области кибербезопасности имеют более узкую направленность.

Специалисты по кибербезопасности принимают активное участие в защите серверов, конечных точек, баз данных и сетей, обнаруживая дыры и неправильные конфигурации, которые создают уязвимости. Другими словами, они несут ответственность за предотвращение нарушений. Самые талантливые думают, как хакеры и, возможно, даже были таковыми в прошлом. Конечно, специалисты по информационной безопасности также озабочены предотвращением потери данных. Они работают над этим вместе со своими кибер-коллегами, но могут играть более широкую роль в определении приоритетов, в первую очередь наиболее конфиденциальных данных и составлении плана восстановления после взлома. В таблице 1 приведены сравнительные характеристики специалистов в этих двух направлениях.

Таблица 1

Сравнительные характеристики специалистов
Table 1. Comparative characteristics of specialists

Компьютерная безопасность	Информационная безопасность
Сосредоточена исключительно на онлайн-угрозах	Рассматривает ландшафт безопасности издалека
Учится думать, как хакер	Занимается защитой данных от любых угроз
Развивает глубокое понимание вредоносного ПО	Наблюдает за несанкционированным доступом / изменением / нарушением
Действует как первая линия защиты	Создает планы восстановления после нарушения

Также полезно подумать о разнице между данными и информацией на более фундаментальном уровне. Данные могут быть любыми, например, серией чисел, но не все данные равны. Что представляют собой эти данные и насколько они конфиденциальны, находятся в ведении профессионалов в области информационной безопасности? Если, например, ряд цифр был номером кредитной карты клиента, то группы информационной безопасности обязаны убедиться, что они соответствуют государственным постановлениям. Опять же, они тесно сотрудничают со своими кибер-коллегами, чтобы обеспечить безопасность наиболее важных данных. Но они несут ответственность за гораздо более значительную долю общей безопасности в организации.

В таблице 2 представлены данные признаков отличия между информационной безопасностью и кибербезопасностью.

Таблица 2

Признаки отличий информационной безопасности и кибербезопасности

Table 2. Differences of information security and cybersecurity

Кибербезопасность	Информационная безопасность
Представляет собой практику защиты данных извне ресурса в Интернете	Представляет собой защиту информации от неавторизованного пользователя, доступа и изменения или удаления данных для обеспечения конфиденциальности
Предназначена для защиты киберпространства от кибератак	Занимается защитой данных от любых форм угроз
Предназначена для защиты всего периметра в киберсфере	Предназначена для защиты информации независимо от области
Устраняет опасность для киберпространства	Занимается защитой данных от любых форм угроз
Предотвращает киберпреступления, кибермошенничество и применяется правоохранительными органами	Борется против несанкционированного доступа, нарушений целостности и раскрытия информации
Оказывает помощь специалистам при постоянной угрозе взлома данных	В первую очередь обеспечивает приоритет ресурсов в борьбе с угрозами информации
Занимается проблемами угроз, возникающими в киберпространстве	Связана с информационными активами и целостностью, конфиденциальностью

Центр кибернетической и информационной безопасности определяет информационную безопасность как процесс защиты информации, а также информационных систем от несанкционированного доступа, раскрытия, нарушения, уничтожения, модификации или использования, и все это для обеспечения конфиденциальности, целостности и доступности. Эти три термина определены следующим образом:

1. Конфиденциальность – относится к сохранению санкционированных ограничений на доступ и раскрытие, включая средства защиты личной информации, а также конфиденциальной информации [9].

2. Целостность – относится к защите от несанкционированного уничтожения или модификации информации, включая обеспечение ее подлинности и невозможности отказа от авторства.

3. Доступность – относится к обеспечению надежного и своевременного доступа к информации, а также ее использования.

Можно выделить пять важнейших отличий понятий «кибербезопасность» и «информационная безопасность»:

1. Определение. Кибербезопасность – это практика защиты данных, связанных с ними технологий и источников хранения от угроз. С другой стороны, информационная безопасность означает защиту информации от несанкционированного доступа, который может привести к нежелательному изменению или удалению данных.

По сути, кибербезопасность – это киберсфера и связанные с ней данные. Информационная безопасность, напротив, в первую очередь ориентирована на информацию, что гарантирует конфиденциальность, целостность и доступность.

2. Домен. Кибербезопасность означает защиту всего и вся, что присутствует в киберсфере, например, данных, информации или устройств и технологий, связанных с вышеупомянутым. Информационная безопасность, с другой стороны, касается защиты обеих форм информации – цифровой и аналоговой – независимо от области.

Защита профилей в социальных сетях и личной информации в киберсфере связана с кибербезопасностью. Информационная безопасность, напротив, имеет дело

конкретно с информационными активами, доступностью и конфиденциальностью целостности.

3. Процесс – в то время как кибербезопасность в первую очередь связана с защитой использования киберпространства и предотвращением кибератак, информационная безопасность просто защищает информацию от любой формы угрозы и предотвращает такой угрожающий сценарий.

4. Профессионалы, занимающиеся информационной безопасностью, составляют основу безопасности данных и отдают приоритет ресурсам, прежде чем бороться с угрозами. Специалисты по кибербезопасности имеют дело именно с постоянными угрозами повышенной сложности.

5. Защита. Кибербезопасность устраняет все опасности, скрывающиеся в киберпространстве. Информационная безопасность, напротив, имеет дело только со всеми формами угроз информации.

Кибербезопасность конкретно касается киберпреступлений, кибермошенничества и правоохранительных органов. Изменение и нарушение раскрытия информации, а также несанкционированный доступ – две наиболее важные проблемы, с которыми сталкивается информационная безопасность.

4. Синергия кибербезопасности и информационной безопасности

Ранее были показаны в основном теоретические различия между кибербезопасностью и информационной безопасностью. С практической точки зрения кибербезопасность и информационная безопасность обычно рассматриваются как синонимы, что связано с их частично совпадающим характером с точки зрения процесса, направленности и целей.

Единственный способ защитить себя от злоумышленников, которые пытаются использовать атаки для разрушения, – это опередить игру и предвидеть их следующий ход. Именно это является целью передовых исследований кибербезопасности и информационной безопасности. Поскольку частота, интенсивность и масштабы атак и кибератак постоянно растут, это сейчас является более важным, чем когда-либо прежде [10].

Таким образом, можно сказать, что кибербезопасность охватывает все аспекты безопасности, относящиеся к киберсфере, а информационная безопасность – это безопасность информации независимо от области применения. Можно сделать вывод, что информационная безопасность есть надмножество кибербезопасности, поэтому бесконечные дебаты о кибербезопасности и информационной безопасности могут быть неправильным подходом к двум вещам, которые так дополняют друг друга и защищают данные от кражи, доступа, изменения или удаления. Основное отличие, на наш взгляд, – ширина их направленности.

Заключение

И кибербезопасность, и информационная безопасность являются важными аспектами процветания технологий в XXI веке. Следовательно, любой профессионал, стремящийся добиться успеха в мире безопасности данных, должен хорошо понимать эти два термина. Чтобы узнать больше и лучше понять безопасность данных, необходимо ознакомиться с руководствами по информационной безопасности и этическому взлому [11].

Специалисты по безопасности должны быть на шаг впереди тех, кто использует технологии с неправильными намерениями и целями. Именно они знают, как это может случиться и как этого можно избежать, предотвратить или свести к минимуму. В условиях непрерывного развития технологий ИТ-специалистам по безопасности необходи-

мо быть в курсе всех последних событий в области технологий, чтобы иметь возможность решать и, когда и где это возможно, предотвращать такие сценарии.

По мере того, как мир становится все более взаимосвязанным, исследования в области кибербезопасности и информационной безопасности будут оставаться одним из самых эффективных и незаменимых инструментов в глобальной борьбе с злоумышленниками, желающими вызвать хаос и разрушение.

Список литературы

1. Козлова Д.Р., Козлова Н.Ш. Информационная безопасность в виртуальной среде // Наука и творчество: вклад молодежи: материалы Всерос. молодеж. науч.-практ. конф. студентов, аспирантов и молодых ученых. Махачкала, 2020. С. 48–50.
2. Арсентьев М.В. К вопросу о понятии «Информационной безопасности» // Информационное общество. 1997. № 4. С. 48–50.
3. Герасимов В.В., Минина Л.С., Васильева А.В. Информационные технологии производственных систем: учеб. пособие. Новосибирск: НГАСУ, 2019. 74 с.
4. Ищейнов В.Я. Информационная безопасность и защита информации: учеб. пособие. Москва: Директ-Медиа, 2020. 271 с.
5. Статев В.Ю., Тиньков В.А. Информационная безопасность распределенных информационных систем // Информационное общество. 1997. № 1. С. 68–71.
6. Ковалев Д.В. Информационная безопасность: учеб. пособие. Ростов-на-Дону: ЮФУ, 2016. 74 с.
7. Карзаева Н.Н. Основы экономической безопасности: учеб. пособие. Москва: ИНФРА-М, 2017. 275 с.
8. Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента РФ от 05.12.2016 № 646 // КонсультантПлюс. Москва, 2021.
9. Стандарты категорий безопасности информации и информационных систем / L.E. Donald, J.B. Phillip, L.B. Arden, E.D. Никуленко. 2017. URL: <http://www.masters.donntu.edu.ua/2011/fknt/nikulenکو/library/translate.htm> (дата обращения: 01.07.2021).
10. Довгаль В.А., Довгаль Д.В. Анализ проблем обеспечения информационной безопасности беспроводных сенсорных сетей и методов обеспечения безопасности Интернета вещей // Вестник Адыгейского государственного университета. Сер.: Естественно-математические и технические науки. 2021. Вып. 1 (276). С. 75–83. URL: <http://vestnik.adygnet.ru>
11. Довгаль В.А., Довгаль Д.В. Сценарии кибер-атак на умные города и их последствия // Дистанционные образовательные технологии: материалы IV Всерос. науч.-практ. конф. с междунар. участием. Посвящается 75-летию ГПА / отв. ред. В.Н. Таран. Симферополь, 2019. С. 427–433.

References

1. Kozlova D.R., Kozlova N.Sh. Information security in a virtual environment // Science and creativity: the contribution of youth: proceedings of the Russian Youth scient. and pract. conf. of students, graduate students and young scientists. Makhachkala, 2020. P. 48–50.
2. Arsenyev M.V. On the problem of the concept of “Information security” // Information Society. 1997. No. 4. P. 48–50.
3. Gerasimov V.V., Minina L.S., Vasilyeva A.V. Information technologies of production systems: a manual. Novosibirsk: NGASU, 2019. 74 p.
4. Ishcheynov V.Ya. Information security and information protection: a manual. Moscow: Direct-Media, 2020. 271 p.
5. Statyev V.Yu., Tinkov V.A. Information security of distributed information systems // Information Society. 1997. No. 1. P. 68–71.

6. Kovalev D.V. Information security: a manual. Rostov-on-Don: SFedU, 2016. 74 p.
7. Karzaeva N.N. Fundamentals of economic security: a manual. Moscow: INFRA-M, 2017. 275 p.
8. On the approval of the Doctrine of information security of the Russian Federation: Decree of the President of the Russian Federation of 05.12.2016 No. 646 // ConsultantPlus. Moscow, 2021.
9. Standards of categories of security of information and information systems / L.E. Donald, J.B. Phillip, L.B. Arden, E.D. Nikulenko. 2017. URL: <http://www.masters.donntu.edu.ua/2011/fknt/nikulenko/library/translate.htm> (access date: 01.07.2021).
10. Dovgal V.A., Dovgal D.V. Analysis of the problems of ensuring information security of wireless sensor networks and methods of ensuring the security of the Internet of Things // The Bulletin of the Adyghe State University. Ser.: Natural-Mathematical and Technical Sciences. 2021. Iss. 1 (276). P. 75–83. URL: <http://vestnik.adygnet.ru>
11. Dovgal V.A., Dovgal D.V. Scenarios of cyber attacks on smart cities and their consequences // Remote educational technologies: proceedings of the 4th Russian scient. and pract. conf. with international participation. Dedicated to the 75th anniversary of the GPA / ed. by V.N. Taran. Simferopol, 2019. P. 427–433.

Авторы заявляют об отсутствии конфликта интересов.

The authors declare no conflicts of interests.

Статья поступила в редакцию 19.07.2021; одобрена после рецензирования 21.08.2021; принята к публикации 23.08.2021.

The article was submitted 19.07.2021; approved after reviewing 21.08.2021; accepted for publication 23.08.2021.

© Н.Ш. Козлова, В.А. Довгаль, 2021