Шумилина В.Е., к.э.н., доцент кафедры «Экономическая безопасность, учет и право» ДГТУ, Ростов-на-Дону, Россия; Shumilina.vera@list.ru
Ким А.В., студент 3-го курса кафедры «Экономическая безопасность, учет и право» ДГТУ, Ростов-на-Дону, Россия; sabertopwaifu64@gmail.com

СОВРЕМЕННЫЕ СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИИ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Аннотация. В данной статье рассматривается понятие информационной безопасности, способы ее осуществления и реализации. Анализируется сущность информации, для чего она нужна, какие процессы с помощью нее изучаются. Приводятся основные критерии информационной безопасности, гарантирующие надежную защиту для информации, а также рассматриваются популярные и вредоносные программные обеспечения, которые дестабилизируют и разрушают работу информационной системы.

Ключевые слова: защита, информация, информационная безопасность, критерии информационной безопасности, вирус, информационная система, вредоносные программы.

Shumilina V.E., Candidate of Economics, Associate Professor Department of economic security, accounting and law of the DSTU Rostov-on-Don, Russia; Shumilina.vera@list.ru
Kim A.V., 3rd year student of the department "Economic security, accounting and law", Don State Technical University, Rostov-on-Don, Russia; sabertopwaifu64@gmail.com

MODERN INFORMATION SECURITY AND INFORMATION SECURITY

Annotation. This article examines the concept of information security, how it is implemented and enforced. It analyses the essence of information, what it is for, what processes are studied with its help. The basic criteria of information security, which guarantee reliable protection for information, are given, and popular and malicious software, which destabilize and destroy the work of the information system, are discussed.

Keywords: protection, information, information security, information security criteria, virus, information system, malware.

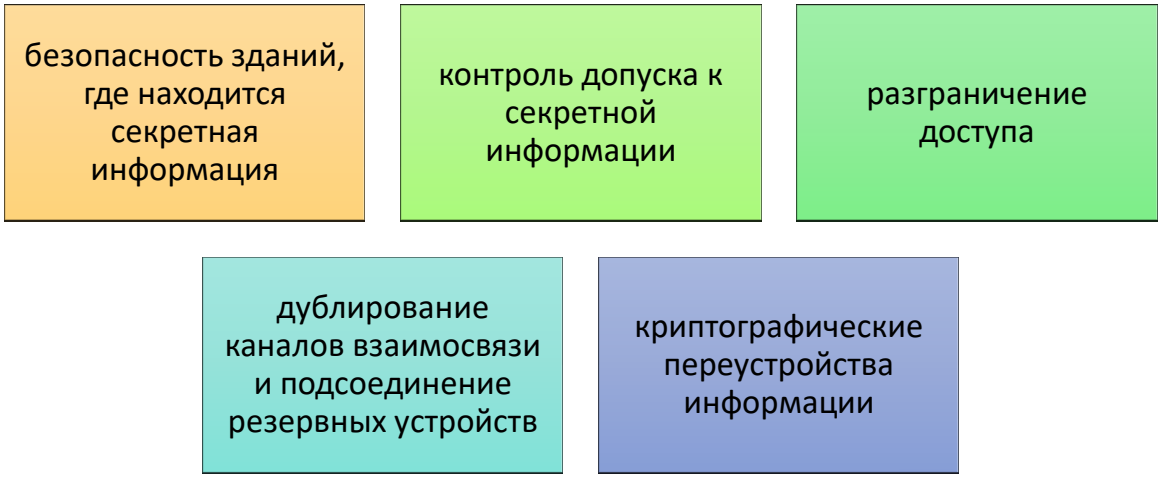
В наше время информация все больше превращается в продукт, который может играть важную роль для человека. Она конвертировалась в способ заработка. Из-за этого все чаще стали возникать отрасли производства, которые основываются исключительно на получении и продаже информации. Данные события породили новые способы хранения и обработки данных, где ключевое место занимает информационная безопасность, обеспечивающая секретность важной информации. Примером таких «хранилищ» могут являться банковские или юридические системы безопасного документооборота. Их основополагающая задача состоит в защите данных в их информационных системах.

Актуальность данного вопроса объясняется и тем фактом, что происходит массовая цифровизация общества, следствием чего является необходимость создания дополнительной защиты файлов и другой хранимой компьютерами информации. С целью описания ряда методов и средств, которые специально предназначены для защиты данных и противодействию хакерам, стал использоваться термин компьютерная безопасность.

Экономическая защита информации становится неотъемлемой задачей, к которой можно отнести следующие действия:

Чтобы избежать утечки информации, разрабатываются и внедряются специальные механизмы на всех этапах деятельности человека.Защищать от дефектов и внешних воздействий необходимо и приборы, на которых находится засекреченная важная информация, а также каналы связи. Дефекты могут быть обусловлены неисправностью оснащения либо подделкой, либо разглашением. Повреждения могут быть вызваны поломкой оборудования, подделкой или разглашением секретной информации.Внешние воздействия появляются как вследствие стихийных несчастий, так и в результате сбоев оборудования либо кражи.

Для сохранения данных применяют разнообразные методы защиты:



Проблема защиты информации и защиты информации в информационных системах требует скорейшего и эффективного решения с целью того, чтобы поспособствовать изолированию функционирующих информационных систем от несанкционированных управляющих воздействий и доступа посторонних лиц или программ к данным с целью хищения.

Информация является основным понятием научных направлений и изучает процессы:

- передачи;

- хранения;

- переработки различной информации.

Информация является основой для нашего быта, неотъемлемой его частью. Именно поэтому она нуждается в защите и охране. В России существует Федеральный закон "Об информации, информационных технологиях и о защите информации", который устанавливает основные права и обязанности, касающиеся информации и информационной безопасности. Согласно данному законодательству информационная безопасность – это защищенность информации от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации.

Основная цель информационной безопасности - защита данных системы, гарантия точности и целостности данных, а также уменьшить разрушения при условиях, если информация станет измененной или совсем разрушенной. Из-за этого к информационной безопасности выдвигаются требования, которые она должна выполнять качественно:

Доступность - способность за определенное время приобрести необходимую информационную услугу

Целостность - ее безопасность от разрушения и несанкционированного изменения

Конфиденциальность - защита от несанкционированного прочтения

Именно эти критерии должны вместе обеспечивать надежность информационной безопасности.

Для того, чтобы разобраться, как именно защитить свою информацию, необходимо разобраться, что такое «угрозы безопасности информационных систем» - это настоящие или потенциально возможные воздействия или события, готовые изменить хранящиеся в информационной системе данные, способствовать уничтожению их или применять в каких-либо других целях, не предусмотренных регламентом предварительно. Именно поэтому необходимо заранее предусматривать угрозы, которые могут возникнуть с информацией. Это позволит разработать способ защиты от таких угроз.

Для обеспечения полной безопасности угрозы необходимо классифицировать, поскольку вся хранимая и обрабатываемая информация находится под влиянием постоянных и чрезвычайных рисков. Это приводит нас к тому, что сложно формализовать проблему описания полного

множества угроз. Классификация помогает рассматривать каждую угрозу не отдельно, а в определенном перечне.

Для классификации угроз был принят подход, предложенный Стивом Кентом. Она не теряет своей актуальности и на сегодняшний день. Данная классификация составляет базовую основу для описания угроз защиты. Рассмотрим виды умышленных угроз безопасности информации, их делят на:

- Пассивные угрозы. Они таргетированы в основном на несанкционированное применение информационных ресурсов, не нарушая и не дестабилизируя при этом деятельность самой системы. К примеру, получение доступа к базам данных, прослушивание каналов связи и т.д.

- Активные угрозы. Являются более опасными, поскольку их основной задачей является нарушение целостности работы системы. Они обладают целью несоблюдения стандартной деятельности информационных ресурсов посредством направленного влияния на ее элементы. К активным угрозам можно отнести:

- вывод из строя компьютера или его операционной системы;
- изменение сведений;
- разрушение программного обеспечения компьютеров;
- несоблюдение работы линий связи и т.д.

Активизировать такие угрозы могут взломщики, вредоносные программы, хакеры и т.д.

Кроме того, умышленные угрозы делятся на внутренние, которые возникают внутри управляемой организации, и внешние.Внутренние угрозы зачастую формируются общественной напряженностью и тяжелым нравственным климатом.Внешние угрозы устанавливаются умышленными поступками конкурентов, экономическими условиями и иными факторами (например, стихийными бедствиями).

В наше время стало популярным использовать метод промышленного шпионажа, чтобы выкрасть информацию. Данная угроза наносит вред владельцу коммерческой тайны незаконные сбор, присвоение и предоставление данных, которые образуют коммерческую тайну, лицом, не являющийся уполномоченным на это ее владельцем.

К главным угрозам безопасности информации и нормального функционирования информационной системы принадлежат:

Потеря секретных данных — это неконтролируемый выход секретных данных за пределы информационных систем или круга лиц, которым она была доверена согласно службе или начала быть известна в ходе работы. Эта утечка может быть следствием:

• разглашение секретной информации;

• ухода информации по различным, главным образом техническим, каналам;

• неразрешенного доступа к секретной информации различными путями.

Разглашение секретной информации ее владельцем или обладателем есть умышленные или неосторожные действия должностных лиц и пользователей, которым соответствующие сведения в установленном

порядке были доверены по службе или по работе, приведшие к ознакомлению с ним лиц, не допущенных к этим сведениям.

Неразрешенный доступ — это противоправное преднамеренное овладение конфиденциальной информацией лицом, не имеющим права доступа к охраняемым сведениям. К способам такого доступа можно отнести:

Большое количество методов утечки секретной информации имеют все шансы послужить причиной к значительному вещественному и нравственному ущербу как для компании, где действует информационная система, так и для ее пользователей.

К примеру, к причинам и обстоятельствам, которые формируют посылы с целью утечки коммерческих тайн, могут являться:

- непонимание или непроинформированность сотрудника как правильно работать с информацией, носящей штамп «коммерческая тайна»;

- применение бракованных, дефектных промышленных средств обработки

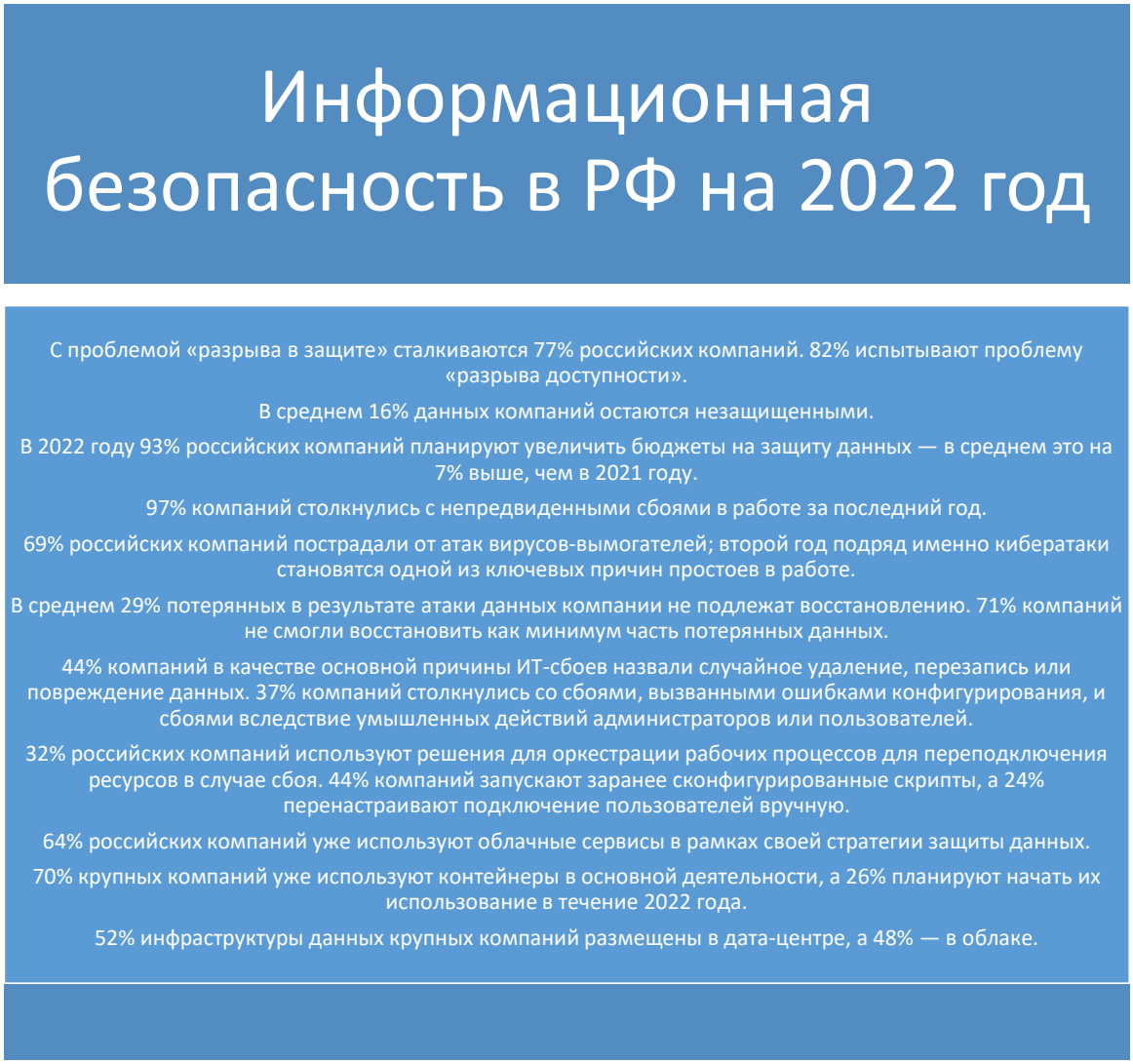
секретных данных;

- отсутствие контроля за соблюдением регламента по вопросу пользования информацией, а также недостаточное количество проведенных мероприятий по организационно-технической составляющей кампании;

- большая текучка кадров. Особенно касается тех сотрудников, которые обладают секретной коммерческой информацией;

- организационные недоработки, вследствие которых виновниками утечки информации считаются люди — работники информационной системы.

Согласно исследованиям и последующим отчетам VeeamDataProtectionTrendsReport 2022 относительно сложившейся ситуации с информационной безопасность в России:



Вышеперечисленные технические пути, которые позволяют получить несанкционированный доступ, возможно обезопаситьпри грамотно разработанной и исследованной на практике системе предоставления защиты. Однако возникают существенные проблемы, которые возникают при создании собственной защиты от компьютерных вирусов.Ключевая сложность заключается в том, что хакеры используют уникальные способы атаки и обхода системы, которые создаются исключительно под выбранную цель. Именно эта проблема не дает возможности разработать единую систему защиты. Взломщики способнынайти уязвимости в защите информационных данных любой сети.

Вредоносные программы имеют собственную классификацию:

Логические бомбы - это версия программы компьютера, распространяющаяся по глобальным сетям, вследствие которой эта программа способна выполняться несколькими путями в зависимости от конкретных условий. При проверке в реальных условиях логическая бомба не проявляется, но при определенном событии данная программа работает по алгоритму. Логические бомбы используются также с целью хищений, способны менять и удалять данные.

Есть два основных типа логических бомб. Первый — когда она интегрирована в вирусный комплекс, например, с трояном и кейлогером. Пользователь сначала скачивает троян, который устанавливает кейлогер и «логическую бомбу». Как только жертва заходит на нужный сайт, где требуется ввести личные данные (логин, пароль, номер карты и пр.), логическая бомба запускает кейлогер. Тот в свою очередь считывает нажатия клавиш и отправляет информацию заказчику.

Второй популярный тип логических бомб — встроенный в официальную программу код, который запускается по заложенному разработчиком сценарию. Из недавних примеров — нашумевшее дело с программистом-подрядчиком Siemens Дэвидом Тинли (DavidTinley),

которого осудили за мошенничество с «логической бомбой». Программист разрабатывал сложноустроенные таблицы Excel, с помощью которых компания решала часть своих CRM-задач. Таблицы в определенный момент начинали работать с ошибками, и Siemens ничего не оставалось делать, как обращаться за платным сервисом к Тинли. В итоге программиста обвинили в умышленном саботаже.

Источники заражения — те же, что и у обычных вирусов: email-вложения, зараженные сайты, кейгены для «крякнутых» утилит и пр. Могут быть встроены в официальное ПО, активизируясь при заданных условиях или при наступлении определенной даты.

Троянский конь — это любая программа, которая способна выполнять разрушающую функцию и срабатывающая при наступлении определенных действий со стороны пользователя. Данный вирус, с виду, является полезным софтом для вашего устройства. Но в конечном случае троян заражает ваш компьютер, компрометирует информацию в нем. Данная программа позволяет злоумышленнику легко совершать следующие действия:

- пользование, владение и перемещение ваших личных данных;

- закрытые доступа вам к вашим личным данным;

- полная дестабилизация программного обеспечения и многое другое.

Типы троянский коней бывают следующие:

Экдоры.

Это один из самых простых, но потенциально наиболее опасных типов троянских программ. Такие программы могут загружать в систему всевозможные вредоносные программы, исполняя роль шлюза, а также повышать уязвимость компьютера для атак.

Эксплойты.

Это программы, содержащие данные или код, позволяющие использовать уязвимость в приложении на компьютере.

Руткиты.

Предназначены для сокрытия определенных объектов или действий в системе. Их основная цель – предотвратить обнаружение вредоносных программ и, как результат, увеличить их время работы на зараженном компьютере.

Дропперы/Загрузчики.

Одной из самых известных троянских программ-дропперов является вредоносная программа Emotet, которая, в отличие от бэкдора, сама по себе не может выполнять никакого кода на компьютере. Дропперы похожи на трояны-загрузчики, но загрузчикам нужен сетевой ресурс для загрузки вредоносных программ из сети, а дропперы содержат другие вредоносные компоненты в своем программном пакете.

Банковские трояны

Встречаются наиболее часто. Распространение онлайн-банкинга и невнимательность некоторых пользователей делают банковские троянские программы перспективным способом для присвоения злоумышленниками чужих денег. Цель таких программ – получить учетные данные для доступа к банковским счетам. Для этого используется фишинг: предполагаемые жертвы перенаправляются на контролируемую злоумышленниками страницу для ввода учетных данных.

Трояны, выполняющие DDoS-атаки.

Распределенные атаки типа «отказ в обслуживании» (DDoS) продолжают будоражить интернет. В этих атаках к серверу или сети

обращается огромное количество запросов, как правило, это делается с использованием ботнетов. Например, в середине июня 2020 года компания Amazon отразила рекордную по интенсивности атаку на свои серверы. В течение более трех дней на веб-сервисы Amazon обрушилось огромное количество запросов, скорость составляла 2,3 терабайта в секунду.

Трояны, имитирующие антивирус.

Они особенно коварны. Вместо защиты устройства они являются источником серьезных проблем. Эти троянские программы имитируют обнаружение вирусов, тем самым вызывая панику у ничего не подозревающих пользователей и убеждая их приобрести эффективную защиту за определенную плату. Однако вместо полезного инструмента антивирусной проверки у пользователя возникают новые проблемы: его платежные данные оказываются переданы создателям троянской программы для дальнейшего несанкционированного использования.

Похитители игровых аккаунтов.

Данная проблема может затронуть тех людей, которые предпочитают проводить свое свободное время за играми. Этот тип программ похищает учетные записи онлайн-игроков.

Трояны, атакующие приложения для обмена мгновенными сообщениями.

Эти троянские программы похищают учетные данные приложений для обмена мгновенными сообщениями, таких как ICQ, MSN Messenger, AOL InstantMessenger, YahooPager, Skype и прочих.

Трояны-вымогатели.

Этот тип троянских программ может изменять данные на компьютере, вызывая сбои в его работе или блокируя доступ к определенным данным.

Злоумышленники обещают восстановить работоспособность компьютера или разблокировать данные только после получения требуемого выкупа.

Трояны-шпионы.

Троянские программы-шпионы могут следить за работой пользователя на компьютере: отслеживать вводимые с клавиатуры данные, делать снимки экрана и получать список запущенных приложений.

Пользователь, запустивший данную программу, не только может потерять всю информацию, но и лишиться возможности нормально пользоваться своим компьютером из-за сбоя информационной системы. Троянский конь функционирует, как правило, в рамках полномочий одного пользователя, однако в интересах иного пользователя или вообще постороннего человека, личность которого определить порой невозможно.

Более опасные воздействия троянский конь способен осуществлять, в случае если запустивший его пользователь владеет расширенным комплектом преимуществ. В данном случае правонарушитель, собравший и внедривший троянского коня, и сам этими привилегиями не владеющий, способен осуществлять неразрешенные функции чужими руками.

Вирус — программа, которая может заражать другие программы, модифицируя их с помощью добавления своих, возможно измененных копий. По статистике считается, что основными методами проникновения вирусов является принесенные из дома носители и программного обеспечение, распространяемое по глобальным сетям.

Вирус имеет две главные особенности:

способностью к саморазмножению

способностью к вмешательству в вычислительный процесс (т. е. к получению возможности управления)

Наличие данных особенностей считается аналогом паразитирования в живой природе, характерное биологическим вирусам. За последнее время вопрос борьбы с вирусами стала крайне актуальной, по этой причине весьма многие занимаются ею. Применяются разнообразные организационные меры, новейшие антивирусные программы, проводится пропаганда всех этих мер.

Червь — программа, которая распространяется посредством сети и не и не оставляет своей копии на магнитном носителе. Червь применяет механизмы поддержки сети для установления узла, который может быть заражен. Далее предается с помощью тех же механизмов свое тело или его часть на этот узел и или активизируется, или ожидает для этого оптимальных обстоятельств. Среда, которая подходит для распространения червя считается сеть, пользователи которой доверяют друг другу, а механизмы защиты отсутствуют. Лучший метод защитыот червя — выполнение мер предосторожности против неразрешенного доступа к сети. Существует довольно большое количество разновидностей сетевых червей, которые могут попасться любому пользователю:

- Почтовые черви (Mail-Worm);
- IM черви (IM-Worm);
- P2P черви (P2P-Worm);
- Черви в IRC-каналах (IRC-Worm);

- Сетевые черви (Net-Worm).

Рассматривая вопрос таких вредоносных червей в общем, можно выделить две общие их классификации:

-Интернет черви - черви, использующие для распространения протоколы Интернет. Преимущественно этот тип червей распространяется с использованием неправильной обработки некоторыми приложениями базовых пакетов стека протоколов TCP/IP;

- LAN-черви - черви, распространяющиеся по протоколам локальных сетей.

Именно поэтому, на протяжении длительного промежутка времени организации внедряют меры для обеспечения информационной безопасности, а вот безопасность ОТ является несколько новой территорией. С ростом степени проникновения технологий промышленного Интернета вещей и последующей конвергенции IT/OT производства утратили «воздушный зазор», который защищал их системы ОТ от хакеров и вредоносных программ. В результате злоумышленники все чаще начинают нацеливаться на системы ОТ для кражи конфиденциальной информации, прерывания операции или совершения актов кибертерроризма в отношении критической инфраструктуры. Отчасти это происходит потому, что существующие вредоносные программы эффективно работают против устаревших систем, развернутых в сетях ОТ, которые, вероятно, не были исправлены или обновлены, учитывая отсутствие дополнительных ресурсов на доработку.

Ряд вызовов сыграли свою роль в эволюции кибератак, которые влияли на системы ОТ на протяжении многих лет. Среди них:

Таким образом, ознакомившись с вредоносными программами, можно прийти к выводу, что необходимо строгое выполнение правил управления системой защиты, а соблюдение принципа минимума привилегий дает возможность исключить такие нарушения.

Список источников

1. Информационная безопасность компьютерных систем и сетей/Шаньгин В. Ф. - М.: ИД «Форум»: Инфра-М, 2018 - 416 с.
2. Защита компьютерной информации/Анин Б. Ю. - СПб.:"BHV-Санкт-Петербург" - 2019, 384 с.

3. Основы информационной безопасности/ Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. - М.:Телеком, 2017. 544 с.
4. Варлатая, С. К. Аппаратно-программные средства и методы защиты информации. / С. К. Варлатая, М.В.Шаханова // Владивосток: Изд-во ДВГТУ, 2017. - 318 с.
5. Шумилина, В. Е. Основные проблемы защиты конфиденциальной информации и пути их решения / В. Е. Шумилина, Ю. И. Коптева, С. А. Тевосян // : Современные проблемы экономической безопасности, учета и права в Российской Федерации. Том 3, 11 января 2018 года – 31 2019 года, 2019. – С. 9. – DOI 10.26526/conferencearticle_5c5060d2f3afe7.25271992. – EDN YWPACT.
6. Шумилина, В. Е. Информационная безопасность как фактор обеспечения экономической безопасности / В. Е. Шумилина, К. Н. Абдуллаева, Ю. А. Топор // Актуальные вопросы обеспечения экономической безопасности в Российской Федерации в условиях цифровой экономики. – Мельбурн : AUS PUBLISHERS, 2018. – С. 1-7. – EDN XOAQHB.
7. Шумилина, В. Е. Информационная безопасность как составляющая экономической безопасности предприятия / В. Е. Шумилина, Е. В. Тетунашвили // Управление безопасностью бизнеса в современных условиях. – Москва : AUSPUBLISHERS, 2021. – С. 119-129. – EDN FESZVK.

References

1. Information security of computer systems and networks / Shangin V. F. - M .: Forum Publishing House: Infra-M, 2018 - 416 p.

2. Protection of computer information / Anin B. Yu. - St. Petersburg: "BHV-St. Petersburg" - 2019, 384 p.

3. Fundamentals of information security / E. B. Belov, V. P. Los, R. V. Meshcheryakov, A. A. Shelupanov. - M.: Telecom, 2017. 544 p.

4. Varlataya, S. K. Hardware and software tools and methods of information protection. / S. K. Varlataya, M. V. Shakhanova // Vladivostok: Publishing House of the Far Eastern State Technical University, 2017. - 318 p.

5. Shumilina, V. E. The main problems of protecting confidential information and ways to solve them / V. E. Shumilina, Yu. I. Kopteva, S. A. Tevosyan //: Modern problems of economic security, accounting and law in the Russian Federation. Volume 3, January 11, 2018 - January 31, 2019, 2019. - P. 9. - DOI 10.26526/conferencearticle_5c5060d2f3afe7.25271992. – EDN YWPACT.

6. Shumilina, V. E. Information security as a factor in ensuring economic security / V. E. Shumilina, K. N. Abdullaeva, Yu. A. Topor // Actual issues of ensuring economic security in the Russian Federation in a digital economy. - Melbourne : AUS PUBLISHERS, 2018. - P. 1-7. – EDN XOAQHB.

7. Shumilina, V. E. Information security as a component of the economic security of an enterprise / V. E. Shumilina, E. V. Tetunashvili // Management of business security in modern conditions. - Moscow: AUSPUBLISHERS, 2021. - P. 119-129. – EDN FESZVK.