важности новейших научных разработок в управлении таможенными процессами через разработки и проекты для совершенствования таможенных систем, но и их практическому внедрению и использованию в рамках возможностей таможенных служб. Информационно-техническое обеспечение таможенного управления через предоставление услуг на Едином портале Таможни России (с помощью лицевого счета) должно побуждать участников ВЭД следовать правилам таможни, способствовать сокращению расходов бизнеса и минимизации рисков, связанных с финансами.

ЛИТЕРАТУРА

1. Таможенный кодекс Евразийского экономического союза [Электронный ресурс]: Приложение №1 к Договору о Таможенном кодексе Евразийского экономического союза [офиц. сайт] / Евразийский экономический союз.- Режим доступа: https://eec.eaeunion.org/

2. Афонин П.Н. Информационные таможенные технологии / П.Н. Афонин. – СПб.: Троицкий мост, 2020. – 352 с.

3. Дробот Е.В., Коновалова Е.А. Совершенствование электронного декларирования в таможенных органах Российской Федерации/ Е.В. Дробот // Экономические отношения. 2019. Том 7, №2. -143-158 с.

4. Саенко В.В. Основные направления развития информационно-коммуникационных технологий в таможенных органах Российской Федерации // Вестник Российской таможенной академии. 2020, №2. – 75-80 с.

5. Шаурина О.С., Лесина Т.В., Мигел А.А. Информационные технологии в условиях цифровой трансформации // Modern Economy Success. – 2021, №4. – 50-55 с.

УДК 338

ОСНОВНЫЕ КОМПОНЕНТЫ И ИНСТРУМЕНТЫ ЗАЩИТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Д.С. Маликов, Е.П. Дружникова
г. Белгород, Россия
Белгородский государственный национальный исследовательский университет

Аннотация: *В научной статье представлены основные компоненты и инструменты защиты информационной безопасности. Актуальность обусловлена постоянно увеличивающейся ролью информации для организаций. Несмотря на это, до сих пор в некоторых фирмах информационной безопасности уделяется недостаточное внимание. В заключении статьи автор предлагает применять на практике все выделенные инструменты информационной безопасности для существенного увеличения защиты этого объекта повсеместно по стране.*

Ключевые слова: *информационная безопасность, компоненты информационной безопасности, инструменты информационной безопасности, доступ к сведениям, защита информационных систем.*

THE MAIN COMPONENTS AND TOOLS OF INFORMATION SECURITY PROTECTION

D.S. Malikov, E.P. Druzhnikova
Belgorod, Russia,
Belgorod State National Research University

Abstract: *The scientific article presents the main components and tools of information security protection. The relevance is due to the ever-increasing role of information for organizations. Despite this, insufficient attention is still being paid to information security in some companies. In conclusion, the author suggests applying in practice all the highlighted information security tools to significantly increase the protection of this object throughout the country.*

Keywords*: information security, information security components, information security tools, access to information, protection of information systems.*

Информационная безопасность с каждым годом становится все более важной для любой организации. Причина заключается в роли информации для современной организации – это, либо самый ценный, либо один из наиболее ценных активов организации. Однако, до сих пор многие руководители фирм не уделяют достаточного внимания, как идентификации рисков в отношении основных компонентов информационной безопасности, так и их защите. Это создает значительные угрозы, которые, в случае реализации, могут привести компанию даже к состоянию банкротства. Таким образом, тема актуальна, так как важно выделять риски в основных компонентах информационной безопасности, а также рекомендовать наиболее эффективные универсальные практические инструменты защиты информационной безопасности фирмы.

Первоначально укажем, что под информационной безопасностью в рамках данной работы предполагается комплекс мер, направленных на защиту конфиденциальных сведений от возможного несанкционированного доступа. Авторы различно подходят к данному понятию, однако, в этой научной статье будет применяться именно такая трактовка.

Можно выделить следующие компоненты информационной безопасности:

1. Доступность. Под этим компонентом необходимо понимать доступ лиц к конкретной информации, исходя из имеющихся у них прав. Примером может стать проникновение определенных, не желаемых сведений о фирме в Интернет через сбои в информационной системе;
2. Целостность. В данном случае речь идет о защите информации от любой трансформации и удаления без санкции на это действие. Если существуют угрозы целостности, компания может, как лишиться важной информации, так и использовать в дальнейшем сведения, являющиеся априори недостоверными;
3. Конфиденциальность. Компонент схож с доступностью, однако, в этом случае доступ лица получают незаконно, вследствие намеренных мероприятий, а не по причине случайных, неумышленных ошибок [3]. Предположим, генеральный директор, в большинстве случаев, имеет неограниченный доступ к сведениям, в отличие от рядового работника, у которого он наиболее незначителен, однако, он намеренно завладевает сведениями, к которым у него нет легального доступа.

Теперь необходимо выделить, какие риски и угрозы существуют в отношении всех выделенных компонентов информационной безопасности. Начнем с компонента доступность – ключевая угроза здесь – распространение сведений среди ряда лиц, несмотря на отсутствие желания у компании. Она может реализоваться с помощью допущения следующих рисков: отсутствие у сотрудников, как желания выполнять технику информационной безопасности, так и объективной возможности (например, не обучены в этом направлении, нет технической поддержки, которая могла бы предоставить рекомендации по решению проблем); программные сбои; случайные человеческие ошибки при наличии достаточной поддержки и/или квалификации, например, неверная конфигурация программного обеспечения [2]. Можно считать, что минимизация рисков и угроз здесь заключается в контрмерах. Так, если работников в достаточной степени обучить работе с полагающимся им по должности программным обеспечением,

предоставить всегда доступную техническую поддержку, а также установить санкции за нарушения установленного режима информационной безопасности, риски и угрозы компоненту «доступность» будут сведены к минимуму.

Перейдем к изучению компонента «целостность». Угрозами здесь являются: 1) функционирование фирмы с применением неверных, трансформированных сведений, что уменьшает эффективность или ведет к неверным действиям, наносящим ущерб; 2) отсутствие информации, являющейся ценной для организации, что, либо ведет к прямому экономическому ущербу (например, удалены сведения о разрабатываемой инновации), либо к возможности действовать неэффективно (например, удалены сведения относительно контрагента, потому невозможно определить риски работы с ним). Обычно угрозы реализуются через следующие риски: информационная система доступна для всех работников; нет защиты от удаления и изменения, например, пароля. Для недопущения реализации данных рисков, необходимо рекомендовать: 1) устанавливать пароли на все документы (отметим, что мера позволит снизить риски негативного воздействия на компоненты «доступность» и «конфиденциальность»); 2) напрямую ограничивать доступ работников к базе данных, например, сервера выделены, компьютеры работников не имеют доступа к базе или его необходимо получать через предоставление программных разрешений.

Изучим риски компонента «конфиденциальность». Угрозой здесь является намеренное изучение важных сведений злоумышленником, не имеющим легального доступа к информации. Обычно угроза реализуется, в случае наличия следующих рисков: 1) в компании применяются многоразовые пароли, практика одноразовых паролей или двухфакторной идентификации отсутствует; 2) пароли по разным базам данных одинаковые; 3) недостаточная защита информационной системы (например, система отражения хакерских атак несовершенна); 4) возможность злоупотребления полномочиями или ситуацией работниками; 5) игнорирование техники информационной безопасности при наличии доступа к конфиденциальным сведениям (например, ноутбук, на котором есть доступ к базе данных, оставлен без присмотра). Минимизировать риски можно с помощью соответствующих контрмер: формирование разных паролей, применение двухфакторной идентификации, создание системы штрафов за нарушения дисциплины в сфере информационной безопасности и так далее.

Кратко уже были выделены некоторые инструменты защиты информационной безопасности организации, исходя из основных рисков для компонентов этого объекта. Однако, необходимо более подробно рассмотреть ключевые инструменты для формирования возможности рекомендовать применять некоторые на практике. Начнем с организационно-правовых инструментов. Среди них можно рекомендовать следующие, наиболее эффективные: формирование официальных локальных правовых актов (например, регламентов) в отношении информационной безопасности, которые позволяют работникам получить всю необходимую информацию о своих действиях в основных рисковых ситуациях в рамках информационной безопасности; прописывание в договорах санкций за нарушение техники информационной безопасности; создание корпоративной культуры, в рамках которой нарушители информационной безопасности порицаются коллегами. Если эти меры будут повсеместными, работники будут мотивированы на недопущение реализации ошибок в сфере информационной безопасности, а также получат все необходимые сведения для минимизации случайных неверных действий.

Далее выделим некоторые инженерно-технические инструменты. Среди них наиболее важными являются: формирование и тестирование физической защиты помещений с базами данных от нарушителей (достаточная защита замками, ключами с доступом и так далее); формирование достаточных инженерно-технических методов отслеживания действий работников (например, видеонаблюдение); создание достаточного уровня пожарной безопасности.

Следующие группы инструментов более важны, так как они формируют наибольшую защиту информационной безопасности, однако, все предыдущие элементы тоже необходимо встраивать в рамках изучаемого объекта, так как без них информационная безопасность будет неполноценной [1]. Итак, следующая группа – криптографическая. В ее рамках необходимо рекомендовать следующие инструменты: 1) применение достаточного уровня шифрования сведений при их передаче; 2) использование флэш-носителей для получения доступа к определенному сегменту базы данных; 3) использование зашифрованного мобильного программного обеспечения для получения одноразовых паролей или доступа к двухфакторной идентификации; 4) программное обеспечение, отражающее хакерские атаки, вредоносное действие вирусов и подобное.

Последняя группа инструментов, рассматриваемая в рамках данной научной статьи – программно-аппаратная. Она тесно связана с инженерно-технической группой, но наполовину имеет отношение к цифровым технологиям. Выделим следующие инструменты: 1) доступ к наиболее важным помещениям, например, серверам с базами данных, может быть получен лишь при прохождении идентификации личности через сканирование (например, отпечатка пальца) или через предоставление физического подтверждения (ключ-карта, токен и так далее); 2) сигнализации, срабатывающие при несанкционированном доступе, например, приложена ключ-карта без соответствующего доступа, пароль набран два раза неверно и так далее; 3) программы, направляюще файлы на резервные системы при попытке взлома и удаляющие сведения после их перенаправления.

В заключении отметим, что каждый компонент информационной безопасности необходимо изучать для возможности минимизировать угрозы и риски в его отношении. Для этого необходимо применять многочисленные инструменты, представленные в работе. Автором данной научной статьи рекомендуется внедрять н практике все указанные инструменты, так как они являются наиболее эффективными. При этом нужно рекомендовать проводить регулярное (минимум раз в квартал) тестирование систем безопасности, создавая возможные угрозы и изучая ответную реакцию. Это позволит выявить слабые места, которые могут быть не полностью защищены. Если предлагаемые практические рекомендации будут реализованы каждой фирмой в реальности, уровень информационной безопасности в целом по стране существенно увеличиться, что приведет к минимизации утечки конфиденциальных данных, краж сведений и схожим негативным последствиям.

ЛИТЕРАТУРА

1. Основы информационной безопасности / Х. Р. Хамдохова, А. Б. Милованова, А. А. Анаев [и др.] // ЛУЧШИЙ ИССЛЕДОВАТЕЛЬСКИЙ ПРОЕКТ 2022: Сборник статей Международного научно-исследовательского конкурса, Петрозаводск, 04 мая 2022 года. – Петрозаводск: Международный центр научного партнерства «Новая Наука» (ИП Ивановская И.И.), 2022. – С. 42-45.

2. Саиег, Т. Х. Анализ комплексного метода предотвращения обхода систем обнаружения вторжения (IDS) / Т. Х. Саиег // Инновационная наука. – 2023. – № 11-1. – С. 54-57.

3. Федосенко, М. Ю. Особенности решения задачи управления рисками информационной безопасности при разработке методов защиты от скрытого (стеганографического) обмена информацией на публичных интернет-ресурсах / М. Ю. Федосенко // Проблемы информационной безопасности. Компьютерные системы. – 2024. – № 1(58). – С. 80-95. – DOI 10.48612/jisp/mpbx-putk-8uar.