УДК 004.056

ЗАЩИТА ИНФОРМАЦИОННЫХ ПОТОКОВ В ОРГАНИЗАЦИИ В ЭПОХУ ЦИФРОВИЗАЦИИ

В. В. Василевский

студент факультета экономики и права, Гомельский филиал Международного университета «МИТСО», г. Гомель, Республика Беларусь, e-mail: master_vlad.v@mail.ru

Научный руководитель: **Я. В. Емельянченко**

старший преподаватель кафедры экономики и информационных технологий, Гомельский филиал Международного университета «МИТСО», г. Гомель, Республика Беларусь, e-mail: yanina-email@yandex.by

В работе рассматриваются угрозы и риски информационной безопасности организаций, исследуются современные методы защиты информации.

Ключевые слова: информационные потоки; защита информации; кибербезопасность; цифровизация.

PROTECTION OF INFORMATION FLOWS IN THE ORGANIZATION IN THE ERA OF DIGITALIZATION

V. V. Vasilevsky

student of the faculty of economics and law, Gomel branch of the International University «MITSO», Gomel, Republic of Belarus, e-mail: master_vlad.v@mail.ru

Academic supervisor: **Y. V. Yemelyanchenko**

senior lecturer of the department of economics and information technology, Gomel branch of the International University «MITSO», Gomel, Republic of Belarus, e-mail: yanina-email@yandex.by

The article considers threats and risks of information security of organizations, examines the methods of protecting information.

Kew words: information flows; information security; cybersecurity; digitalization.

Информационная безопасность одна из актуальнейших проблем реального сектора экономики в условиях цифровизации, когда вносятся изменения в промышленные технологии, финансовые транзакции, механизмы создания новых продуктов и услуг.

Цифровизация – внедрение новых технологий в бизнес-процессы организаций для повышения их качества и эффективности. Но вместе с этим при управлении информационными потоками в «оцифрованной» среде возникают новые риски и угрозы информационной безопасности, с которыми сталкиваются компании.

Целью исследования является отражение основных методов защиты информационных потоков в организации с учетом вызовов современности.

Информационный поток в организации – физическое перемещение информации между элементами организации как сложной системы.

Внешними угрозами информационной безопасности организаций будем считать: 1) несанкционированный доступ к бумажным, электронным, цифровым и другим носителям информации; 2) утечка персональных данных сотрудников организации для шантажа или получения доступа в цифровую систему организации; 3) утечка данных организации (бухгалтерские данные, реквизиты, персональные данные сотрудников); 4) внедрение вредоносных программ и вирусов в электронные устройства для обработки и хранения данных; 5) перепады электричества или аварии. Также угрозу безопасности представляет нелицензированное программное обеспечение (ПО), которое не поддерживается разработчиками, а также может содержать в своей структуре вредоносное ПО.

К *внутренним* угрозам стоит отнести некомпетентность или небрежность персонала. Персонал может пользоваться служебной почтой в личных целях, посещать посторонние сайты, запускать случайные приложения и переходить по непроверенным ссылкам. Всё это может привести к получению злоумышленниками дистанционного доступа к компьютерам и информационной системе организации. Так же стоит отметить риск заражения персональных компьютеров работников организации вирусными ПО, в том числе рекламным спамом.

Появление рисков и угроз требует незамедлительного поиска их решения – методов защиты информационных потоков. Исследование литературы [4] позволяет выделить следующие современные методы защиты информации в организациях:

1. Организационные мероприятия: создание инструкций по пользованию компьютерной техники, обработке и хранению информации; разработка и ознакомление персонала с нормами и правилами относящиеся к информационной сфере; создание специальных отделов для управления информационной системой организации. В обязанности работников служб кибербезопасности входит мониторинг, контроль и управление безопасностью оборудования, и в случае возникновения угрозы – немедленное реагирование.

2. Метод инженерно-технической защиты – контроль за деятельностью сотрудников и их допуском к информации, видеонаблюдение и защита от чрезвычайных ситуаций, контроль за сохранность и работоспособностью информационных систем, компьютерной техники и оборудования.

3. Программно-аппаратный метод предусматривает использование оборудования для шифровки данных, оборудование, предотвращающее несанкционированное использование информационных систем, разработку и установку методов предотвращения и обнаружения угроз, сигнализацию.

4. Криптографический метод – шифрование данных, создание шифровальных каналов передачи данных. Популярными программами являются: «Secret Disk Crypto Pack», «InfoWatch CryptoStorage», «Rohos Disk».

5. Предупредительный метод – профилактические проверки оборудования на предмет вредоносных программ и спама.

В большинстве случаев методы защиты используются в совокупности.

Законодательно необходимость защиты и меры по защите информации закреплены в Законе Республики Беларусь «Об информации, информатизации и защите информации» [3]. В данном законе затронуты важные аспекты для организации необходимых условий, с помощью которых защита информации происходит по определённым требованиям.

С 2019 г. в РБ появилась «Концепция информационной безопасности Республики Беларусь» [2]. В данной концепции стоит отметить главу 19 «Противодействие киберпреступности», т. к. киберпреступность одна из главных угроз для информационных потоков и систем организаций.

Безопасность информационных потоков и информации так же затронута в государственной программе «Цифровое развитие Беларуси» на 2021–2025 годы, а именно в 8

главе сказано: «Развитие информационных технологий, основанных на них технических решений, государственных электронных сервисов приводит к необходимости непрерывного совершенствования инструментов, обеспечивающих стабильность их работы и защиту данных информационных систем (цифровых платформ)» [1].

Таким образом, безопасность и защита информационных потоков в эпоху цифровизации является актуальным вопросом как для государства, так и для организаций. Организации создают новые структурные подразделения (службы кибербезопасности), используют актуальные методы защиты информационных потоков, чтобы повысить уровень своей безопасности в «оцифрованной» среде.

Библиографические ссылки

1. Государственная программа «Цифровое развитие Беларуси» на 2021–2025 годы [Электронный ресурс] // Национальный правовой Интернет-портал Республики Беларусь. – URL: https://pravo.by/document/?guid=3871&p0=C22100066&ysclid=l915brbymw854564588 (дата обращения: 10.10.2022).

2. О концепции информационной безопасности Республики Беларусь: Постановление Совета Безопасности Республики Беларусь от 18.03.2019 № 1 [Электронный ресурс] // Национальный правовой Интернет-портал Республики Беларусь. – URL: https://pravo.by/document/?guid=3871&p0=P219s0001/ (дата доступа: 10.10.2022).

3. Об информации, информатизации и защите информации: Закон Республики Беларусь от 10.11.2008 № 455-З (с изм. и доп.) [Электронный ресурс] // Национальный правовой Интернет-портал Республики Беларусь. – URL: https://pravo.by/document/?guid=3871&p0=-h10800455&ysclid=l9d14v062d361572797 (дата доступа: 10.10.2022).

4. Скворцова Н. О., Чекулаева Е. Н. Защита информационных потоков на предприятии // Инженерные кадры – будущее инновационной экономики России. – 2016. – № 4. – С. 131–134.