Криворотова Влада Андреевна

студентка специальности «Экономическая безопасность» Тюменского государственного университета, г. Тюмень, vlada.krivorotova@mail.ru

Туровинина Мария Сергеевна

студентка специальности «Экономическая безопасность» Тюменского государственного университета, г. Тюмень, turovinina.mariya@mail.ru

Зылёва Наталья Владимировна

кандидат экономических наук, доцент, доцент кафедры экономической безопасности, учета, анализа и аудита Тюменского государственного университета, г. Тюмень, n.v.zylyova@utmn.ru

ЦИФРОВЫЕ ТЕХНОЛОГИИ И ВОЗМОЖНЫЕ ЭКОНОМИЧЕСКИЕ РИСКИ

Аннотация. С развитием цифровизации многие организации, особенно вновь созданные, используют в своей деятельности цифровые технологии и системы, такие как: 20 АРМ, 1С, принт-сервер, контролер домена, и Web-сайт (Веб-сайт). При этом, использование данных технологий может служить причиной возникновения разных рисков, например, потери клиентов и партнеров, утечка данных, в том числе конфиденциальных, снижение эффективности производства и другие, приводящие к экономическим потерям, риски. В данной работе анализируются вышеуказанные цифровые технологии с позиции обеспечения безопасного их применение в деятельности хозяйствующих субъектов.

Ключевые слова: цифровизация, 20 АРМ, 1С, принт-сервер, контролер домена, Web-сайт (Веб-сайт).

Krivorotova Vlada Andreyevna

Student of the specialty "Economic security" of the Tyumen state University, Tyumen, vlada.krivorotova@mail.ru

Turovinina Maria Sergeevna

Student of the specialty "Economic security" of the Tyumen state University, Tyumen, turovinina.mariya@mail.ru

Zyleva Natalya Vladimirovna

Candidate of Economic Sciences, Associate Professor, Associate Professor of the Department of Economic Security, Accounting, Analysis and Audit of Tyumen State University, Tyumen, n.v.zylyova@utmn.ru

DIGITAL TECHNOLOGIES AND POSSIBLE ECONOMIC RISKS

Abstract. With the development of digitalization, many organizations, especially newly created ones, use digital technologies and systems in their activities, such as: 20 APM, 1C: Enterprise, print server, domain controller and Web site. At the same time, the use of these technologies can cause various risks, such as loss of customers and partners, data leakage, including confidential data, reduced production efficiency, and other risks that lead to economic losses. This paper analyzes the above-mentioned digital systems from the point of view of ensuring their safe use in the activities of organizations.

Keywords: 20 APM, 1C: Enterprise, print server, domain controller, Web site.

На деятельность современных организаций оказывают влияния два вектора – «цифровая экономика» и «экономическая безопасность».

Цифровая экономика основана на цифровых технологиях, которые, в свою очередь, являются системой информационных технологий, кодирующей информацию из базы данных [1, с. 40] Совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств, закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ называет «системой», что и привело к тому, что в обиход современных пользователей вошло словосочетание «цифровые системы», под которым понимают информационные системы и оборудования, обеспечивающие их функционирование.

Экономическая безопасность организации отражает способность хозяйствующего субъекта предвидеть внутренние и внешние угрозы деятельности, минимизировать или предотвращать возможные риски, и в целом эффективно использовать имеющиеся ресурсы для стабильного функционирования. Цифровые новшества нашего времени, вошедшие в жизнь организаций, стали причиной появления новых рисков, быть готовыми к которым должны специалисты службы экономической безопасности.

Распространенными цифровыми системами, которыми большинство организаций пользуются ежедневно, являются «20 АРМ», «1С», принт-сервер, контролер домена, Web-сайт (Веб-сайт).

В распределении информационно-вычислительных ресурсов и продуктивном взаимодействии участников оборота информации, огромную роль в условиях цифровизации играет автоматизированное рабочее место (АРМ) [2]. Система «20 АРМ» совмещает в себе работу вычислительной техники (разработана для хранения, накопления и переработки

информации) и решение человека (требует выполнение управленческих действий, нахождение гибких решений).

Автоматизированное рабочее место необходимо защищать от:

- злоумышленников, способных уничтожить, изменить или скопировать данные;
- технических каналов с несанкционированными взломами;
- чрезвычайных ситуаций.

Защита любой цифровой системы, в том числе «20 АРМ» должна входить в функциональные обязанности специалиста по компьютерной безопасности, как сотрудника, обладающего необходимыми знаниями в области информационных систем. В свою очередь, специалист по экономической безопасности в рамках минимизации кадровых рисков, должен проверить компетентность сотрудника, отвечающего за безопасность используемых информационных систем,

Способы защиты автоматизированного рабочего места, которые должен предусмотреть специалиста по компьютерной безопасности и проверить специалист службы экономической безопасности:

- исследование уязвимых мест;
- антивирус;
- мониторинг и контроль;
- защита компьютерной сети;
- система пожаротушения;
- блок бесперебойного питания.

Решения для комплексной автоматизации деятельности производственных, торговых и сервисных предприятий уже несколько лет как предложены цифровой системой «1С». Система программ «1С» предназначена для автоматизации управления и учета на предприятиях различных отраслей, видов деятельности и типов финансирования, и включает в себя программы ведения бухгалтерского учета, расчета заработной платы и управления кадрами, учета в бюджетных учреждениях, разнообразные отраслевые и специализированные решения, разработанные самой фирмой «1С», ее партнерами и независимыми организациями [3].

Использования программ системы «1С» может быть причиной следующих рисков:

- файловый формат использования программы с базами данных. Подобная ситуация может быть вызвана физическим воздействием лиц со стороны: данные могут быть скопированы (целенаправленная кража) или удалены (потери);

- доступ к серверному оборудованию. Риск физического доступа к «серверной» организации. В этом случае шансы несанкционированных действий (копирование, кража, изменение, уничтожение) увеличивается в несколько раз;

- безопасность сети. При недостаточной или не качественной ИТ-поддержки системы предприятия возможны угрозы несанкционированных доступов.

Методы минимизации информационных рисков:

- персональная авторизация рабочих станций для пользователей отчетности;

- разделение права доступа к информации в 1С, т.е. все сотрудники будут получать доступ именно к той информации, с которой имеют непосредственное взаимодействие;

- своевременная блокировка профиля при прекращении работы с информацией;

- ограничение доступа к серверным системам предприятия, вход разрешить только уполномоченным лицам;

- установка паролей на резервные копий или шифрование данных;

- пропускная система для физического обеспечения безопасности;

- засекречивание места нахождения средств обработки информации (оно не должно быть известно широкому кругу лиц);

- соблюдение техники безопасности в местах обработки данных;

- дополнительная система пожаротушения и блок бесперебойного питания.

Следует отметить, что применение программ 1С может привести и к юридическим рискам. Поводом для возбуждения дела может быть использование «пиратской» версии программы. В функции специалиста службы экономической безопасности должен входить мониторинг цифровых систем программного обеспечения для предотвращения административной или уголовной ответственности за нарушение авторских прав программы.

Самая популярная программа из семейства «1С», это программа «1С: Бухгалтерия», которая распространена не только в нашей стране, но и является самой известной учетной программой в ряде стран. При этом, бухгалтерские программы часто подвергаются атакам злоумышленников, что и произошло в 2016 году. В одной из российских компаний перестала работать программа «1С: Бухгалтерия» и злоумышленник под видом администратора запросил разрешение переместить базу данных в другую папку. Вместо базы данных преступник оставил текстовый документ со своим email-адресом и письмо, в котором потребовал 30 000 рублей за возврат базы [4].

Бесспорно, разглашение информации может создать угрозу хозяйствующему субъекту и привести к негативным последствиям. Самым распространенным риском является утрата финансовых отчетов, персональных данных сотрудников, информации клиентов и партнеров.

При этом, разглашение некоторой информации приводит к более негативным последствиям, чем просто ее утрата.

Разглашение информации, чаще всего даже случайно, происходит при применении «Принт-сервера» – цифровой программы, которая прослеживает состояние всех соединенных принтеров и занимающаяся выборкой задания в соответствии с очередью печати [5]. Если принтер используется одним пользователем и на рабочем столе этого пользователя, то риск раскрытия конфиденциальной информации минимален, но если один принтер предназначен для 5-10 и более пользователей и находится от сотрудника, которому необходимо распечатать документ с конфиденциальной информацией, на удалении (например, в соседнем кабинете), то подобный риск возможет.

Для предотвращения неблагоприятных последствий разглашения информации специалисту службы информационной безопасности стоит рассмотреть возможность внедрения в деятельность организации инструментов мониторинга за процессом печати и сканирования документов, а также отправки данных по сети. Это возможно при индивидуальной аутентификации пользователя при вводе личного пароля, который позволяет получить доступ к процессу печати. Подобный способ экономически выгоден, т.к. для него не требуется дополнительного приобретения оборудования и его настройки. Более затратным является способ аутентификации по ID-картам сотрудников, подобное используется при входе в здания или защищенные помещения. При обоих этих способах срабатывает функция отложенной печати, т.е. пока пользователь не авторизуется, документ находится в очереди локального сервера [5].

Внедрения в деятельность организации инструментов мониторинга за процессом использования «Принт-сервера» позволяет также предотвращать хакерские атаки на принтер. В 2018 году произошло 50 000 тысяч хакерских атак принтеров по всему миру. Хакеры использовали поисковую систему, которая выдает устройства с открытым портом. Таким способом, возможно, не только получить доступ к напечатанным файлам, которые хранятся на принтерах, но также блокировать устройства [6].

Обмен данными между компьютерами, серверами, оборудованием и программным обеспечением обеспечивает компьютерная сеть, контролирует которую контроллер домена. Контроллер домена – это физическое хранилище виртуальных баз данных, позволяющее организациям эффективно управлять своими серверами, рабочими станциями, пользователями и приложениями. Если злоумышленник получит преимущественный доступ к контроллеру домена, то сможет использовать базу данных в своих корыстных целях.

Существует несколько видов атак, которые необходимо предотвращать, для того чтобы обезопасить свою базу данных. Самый распространенный вид атак – регистрация

злоумышленника на удаленном устройстве, представляющее собой сервис «клиент-сервер» (хост), с применением пароля, который можно найти в памяти компьютера. Благодаря извлеченному паролю происходит взлом сервера с базой данных. Еще один вид атак – это использование специальной компьютерной программы, которая позволяет сделать снимок информации о состоянии компьютерной системы («дамп-памяти»). Также преступники используют атаку через подбор паролей.

В 2019 году произошла серия атак контроллеров домена, которые попытались взломать, представившись регистратором домена Ru-Center (АО «Региональный сетевой информационный центр»). Так, на **с**айт редакции ComNews.ru была доставлена мошенническая рассылка о том, что необходимо оплатить услуги домена и для этого нужно заполнить учетные данные клиента Ru-Center. Таким образом злоумышленники пытались получить доступ к управлению доменом компании, что в свою очередь позволило бы им завладеть данными официального сайта, **а** затем потребовать выкуп с владельцев [7]. Данный пример говорит еще об одном виде атак – атаки через мошеннические схемы получения конфиденциальной информации.

Предотвращать атаки злоумышленников на контроллеры домена входит в функции специалиста по кибербезопасности, которые, кроме прочего, предлагают разделения хранилища виртуальных данных, для предотвращения доступа к файлам виртуальных машин. Для специалиста службы экономической безопасности в приоритете защита физической составляющей домен, т.е. физических узлов, на которых работают виртуальные машины. Так, в первую очередь, стоит предусмотреть место расположения контроллера домена (рекомендуется использовать отдаленное место, с которым не сталкиваются в течение дня работники предприятия), далее следует установить защитные стойки и соблюсти правила пожарной безопасности.

У всех современных организаций есть свой сайт в сети Интернет, благодаря которому все желающие (контрагенты, конкуренты, контролирующие органы и т.п.) получают обновляемую информацию о хозяйствующем субъекте.

Web-сайт (Веб-сайт) – это много страниц, с определенной структурой, разными разделами и гиперссылками [8]. Место, где хранятся файлы с сайта – хостинг. Защита сайта и хостинга необходима для недоступности выполнения действий злоумышленником. При помощи взломов и заражения сайта вирусами мошенники извлекают материальную выгоду через махинации с «открытыми» данными либо через использование ресурсов хостинга. Так, в 2018 году Японский сайт криптовалютной биржи Coincheck подтвердил информацию о хищении средств с платформы на 58 млрд. иен. Сайт претерпел атаки вируса, который распространял спам-рассылку внутри компании, блокировал работу компьютеров, а

мошенники потребовали денежное вознаграждение за восстановление доступа [9]. Таким образом, для защиты конфиденциальной информации от незаконного использования и защиты сайта от эксплуатации посторонними лицами, следует применить защиту своего Интернет-ресурса.

Управлять сайтом и информацией в нем помогает система защиты Content Management System (Системы управления содержимым сайта). Система ограничивает пользователей сайта в правах на доступ к базе данных, отслеживает информацию, которую вводит посетитель, что помогает защитить сайт от вредоносного спама и XSS-атак (межсайтовый скриптинг), которые могут произойти через формы обратной связи (например, интернет-заказ).

Для безопасной работы сайта необходима защита персональных компьютеров организации через установление антивирусной программы. Специалист службы экономической безопасности может взять на себя функцию согласования условий выгодного экономического сотрудничества с передовыми компаниями по установлению антивируса. Для хозяйствующего субъекта возможно предоставление индивидуальных услуг с учетом особенностей деятельности организации и программного обеспечения.

В заключение отметим, что внедрение цифровых технологий в жизнь хозяйствующих субъектов накладывает отпечаток не только на деятельность специалистов по кибербезопасности, но и на деятельность сотрудников службы экономической безопасности. Экономические риски, связанные с использованием цифровых систем и программного обеспечения, необходимо минимизировать, а для этого нужно не только контролировать компетентность сотрудников, отвечающих за компьютерную безопасность, но и самому, по возможности, разбираться в вопросах защиты систем и оборудования хозяйствующего субъекта. Прогнозирование возможных рисков кадровой, правовой, информационной и физической безопасности, позволит сэкономить денежные средства организации через предотвращение: утечки конфиденциальной информации об организации и ее контрагентах; утраты учетной и отчетной информации; утраты имущества (оборудования) в связи с умышленной ее порчей; судебных исков от правообладателей. Надежная защита программного обеспечения, серверов и сайтом организации – первостепенная задача, ведь на безопасности предприятия нецелесообразно экономить, иначе восстановление данных выйдет намного дороже, чем поддержание защиты.

Библиографический список

1. Зылева Н.В. Информационные технологии и системы в геологоразведке: влияние на экономическую безопасность// Цифровая экономика: перспективы аудита и безопасности бизнеса: сборник статей по материалам Всероссийской научно-практической конференции, г.

Тюмень, 5 ноября 2020 г. / [отв. ред. Д. Л. Скипин] – Тюмень: Издательство Тюменского государственного университета, 2020. С.40-49. URL: https://www.elibrary.ru/item.asp?id=44354342 (дата обращения: 12.04.2021).

2. Чаус Е.А. Система автоматизированных рабочих мест в структуре ЛВС // Международный научно-исследовательский журнал. № 8 (40). 2016. С. 103-106. URL: https://cyberleninka.ru/article/n/sistema-zaschity-avtomatizirovannyh-rabochih-mest-v-strukture-lvs/viewer (дата обращения: 12.04.2021).

3. Фирма «1С» // 1С. ру [официальный сайт] 2008-2021. URL: https://1c.ru/rus/firm1c/firm1c.htm (дата обращения: 12.04.2021).

4. Иванов В. Взлом и защита 1С: Предприятия Анализ проблемы инсайдерского взлома для менеджеров // Клейр.ру [официальный сайт] 2001-2021. URL: https://www.klerk.ru/soft/articles/818/ (дата обращения: 15.04.2021).

5. Рябов А.С. Обеспечение информационной безопасности процессов печати // Вопросы защиты информации. № 4 (107). 2014. С. 29-31. URL: https://www.elibrary.ru/download/elibrary_22867719_72241341.pdf (дата обращение: 15.04.2021).

6. Взломать 50 000 сетевых принтеров и распечатать произвольный текст? Нет ничего проще! // GlobalSign Компания. [официальный сайт] 2006-2021. URL: https://habr.com/ru/company/globalsign/blog/431852/ (дата обращение: 15.04.2021).

7. Устинова А. Мошенники подставили Ru-Center // Новости цифровой трансформации, телекоммуникации, вещания и ИТ. COMNEWS.RU [официальный сайт] 1999-2021. URL: https://www.comnews.ru/content/119249/2019-04-22/moshenniki-podstavili-ru-center (дата обращение: 15.04.2021).

8. Беляева Н.А. Создание Интернет-сайта // Правовое регулирование. № 6(198). 2007. С. 37-43. URL: https://cyberleninka.ru/article/n/sozdanie-internet-sayta-1/viewer (дата обращение: 15.04.2021).

9. Асмаков А. Биткоин-биржа Coincheck подтвердила хищение более полумиллиарда долларов в криптовалюте NEM // FORKLOG [официальный сайт] 2014-2021. URL: https://forklog.com/bitkoin-birzha-coincheck-podtverdila-hishhenie-bolee-polumilliona-dollarov-v-kripovalyute-nem/ (дата обращение: 15.04.2021).