УДК 330
DOI 10.21685/2309-2874-2019-1-4

В. Ю. Щеглов, А. А. Надькина

УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЙ В СВЯЗИ С ЦИФРОВОЙ ТРАНСФОРМАЦИЕЙ ЭКОНОМИКИ И ВОЗМОЖНОСТИ ИХ НЕЙТРАЛИЗАЦИИ

Аннотация.

Актуальность и цели. Проникновение цифровизации во все сферы жизни человека способствовало не только улучшению качества жизни, но и создало ряд проблем. Одной из таких проблем является угроза информационной безопасности предприятий, что вызвано проникновением внутрь предприятия и дальнейшей кражы информации с возможностью получения за это денежных средств или ее продажей на сторону. Цель работы – провести анализ возможных мест утечки информации на предприятиях и определить влияние цифровой экономики на информационную безопасность предприятия.

Материалы и методы. Реализация исследовательских задач была достигнута путем проведения анализа сбора, хранения информации компьютерами предприятий и ее защиты от возможных краж. Особое место в проведенном исследовании занимает оценка риска безопасности для малого и среднего бизнеса. Особо стоит выделить фишинг, APT-угрозы, вымогательства, DDOS-атаки. Исследование информационной безопасности было произведено на основании метода причинных связей, который позволил сопоставить различные способы проникновения внутрь системы и кражи из нее информации.

Результаты. Рассмотрены угрозы информационной безопасности, которые появляются в процессе становления цифровой экономики. Также выявлены барьеры формирования цифровизации, являющиеся и предметом угроз. Отмечен ряд рисков, которые несет в себе цифровизация. Предложены меры, которые вследствие их применения дадут возможность регулировать появляющиеся информационные угрозы и повысить цифровой уровень российских предприятий.

Выводы. Изучение краж информации и денежных средств различными способами дает возможность понять, что основными причинами проникновения внутрь компьютеров предприятия является желание заработать на этом денежные средства путем применения различных схем. Для предотвращения потерь предприятий необходимо комплексно подходить к защите компьютерных систем.

Ключевые слова: цифровая экономика, угрозы информационной безопасности, цифровая трансформация экономики.

V. Yu. Shcheglov, A. A. Nad'kina

THREATS TO INFORMATION SECURITY OF ENTERPRISES ASSOCIATED WITH DIGITAL TRANSFORMATION OF THE ECONOMY AND THEIR POSSIBLE NEUTRALIZATION

Abstract.

Background. Penetration of digitalization in all spheres of human life contributed not only to improve the quality of life, but also created a number of problems. One of these problems is the threat to the information security of enterprises, which is caused by penetration into the enterprise and further theft of information with the possibility of obtaining funds for it or selling it to the side. The purpose of the work is to analyze the possible places of information leakage in enterprises and the impact of the digital economy on the information security of the enterprise.

Materials and methods. The implementation of the studied tasks was achieved by analyzing the collection, storage of information by computers of enterprises and its protection from possible theft. A special place in the study is occupied by security risk assessment for small and medium-sized businesses. Among which it is worth to highlight phishing, the ART of threat, extortion, DDOS attacks. The study of information security was carried out on the basis of the method of causation, which allowed to compare the different ways of penetration into the system and theft of information from it.

Results. The threats to information security, which appear in the process of digital economy formation, are considered. Barriers to the formation of digitalization, which are also the subject of threats, are also identified. A number of risks that "digitalization"carries are noted. The measures that, as a result of their application, will make it possible to regulate emerging information threats and improve the digital level of Russian enterprises.

Summary. The study of theft of information and money in various ways makes it possible to understand that the main reasons for the penetration into the company's computers are the desire to earn money through the use of various schemes. To prevent losses of enterprises, it is necessary to take an integrated approach to the protection of computer systems.

Keywords: digital economy, threats to information security, digital transformation of the economy.

Цифровизация – это все, что связано с использованием цифровых прорывных технологий. Цифровые технологии внедрились едва ли не во все сферы бизнеса, и этот процесс будет продолжаться. Уже сегодня процесс цифровизации предприятий составляет колоссальную долю задач экономики. Цифровизация менеджмента дает возможность гибко управлять организацией, делегируя часть функций программам [1].

Как известно, действия данных программ обширны, и риски утечки информации через них трудно прогнозируются. В последнее время причины появления утечки данных связаны именно с развитием цифровых технологий. Вследствие этого возникает необходимость формирования системных мер по эффективному встраиванию всей экономики в цифровую трансформацию. В этих условиях именно информационная безопасность обеспечивает нормальное функционирование основного бизнес-процесса. Однако, с другой стороны, его защита – это до такой степени важный вопрос, что служба безопасности из дополнительного отделения становится структурой первостепенной важности. И хотя киберугрозы не несут непосредственного вреда здоровью людей, все же безопасность информации на предприятиях является актуальным вопросом, так как угрозы информационной безопасности могут поставить светлое цифровое будущее под большой вопрос.

То есть следует признать, что ключевым фактором построения цифровой экономики является защита информации [2]. Не случайным является и то,

что формулировка понятия цифровой экономики дана непосредственно в Стратегии развития информационного общества. Это подчеркивает, что информационная составляющая кардинально трансформирует сам тип всей хозяйственной деятельности, а обработка больших объемов данных и применение результатов анализа в цифровой экономике акцентируют повышенное внимание на обеспечении безопасности [3].

Каждое действие, сделанное в цифровом пространстве, оставляет свой след. Поэтому необходимо в этих условиях собрать всю эту обширную информацию, проанализировать и сохранить. Однако следует признать, на практике у традиционных предприятий вопросы безопасности не решены. Несоблюдение инфогигиены заключается [1]:

– в факте необновления программного обеспечения (ПО);

– в отсутствии культуры патч-менеджмента (процесса управления обновлениями программного обеспечения);

– в так называемом «дырявом» периметре (когда предприятие рассчитывает на устаревший антивирус в борьбе с современным вредоносным ПО);

– в сращивании и взаимопроникновении ИТ – веб-сервисов, телекоммуникационных систем, систем защиты, информационных систем и др. На их стыках образуются «слепые для узкоотраслевых экспертов зоны», дающие киберпреступникам новые внутренние резервы для гибридных атак уязвимости самых различных технологий. Ранее подобных атак было меньше, сегодня их число неуклонно растет ввиду прогресса кибертехнологий. Они с большим успехом применяют все нюансы цифровизации [1].

Существует масса барьеров, затрудняющих внедрение цифровой экономики в РФ. Следует учесть, что данные барьеры сами, в свою очередь, зачастую представляют собой предмет угроз.

I барьер – отсутствие у предприятий необходимости в развитии с внедрением цифровых технологий. Причина – сознание и уровень квалификации менеджмента [4].

II барьер – недостаточное количество специалистов: 90 % международных организаций подтверждают острый дефицит «цифровых» талантов, разновидность которых представлена на рис. 1.

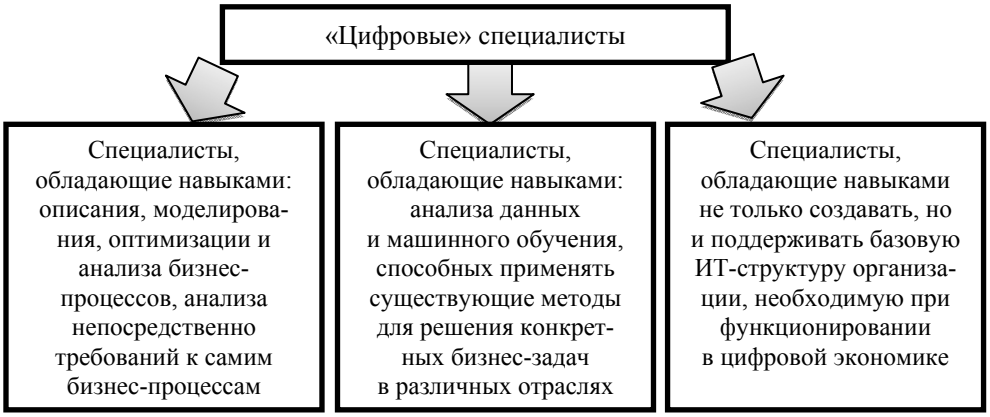

Рис. 1. Виды «цифровых» специалистов, необходимых в цифровой экономике [5]

III барьер – обеспечение кибербезопасности. Проблема РФ – в недооценке рисков. Также ощутимо отсутствие важных поправок в сфере взаимодействия государства и бизнеса; недостаток мер правоприменения и правоохранения, для того чтобы блокировать угрозу. Актуальной предстает схема: организации формируют собственные центры противодействия киберугрозам, они в свою очередь преобразуются в фьюжн-центры, а те уже смогут управлять инцидентами, результаты работы переходят к госинститутам, после чего разрабатывается правоприменение [5].

На сегодняшний день известны пять рисков в области безопасности среднего и малого бизнеса.

1. Фишинг (79 %) – вид интернет-мошенничества, построенный на принципах получения доступа к критически важным данным (например, паспортным), учетным записям и т.д.

Рекомендованы меры, позволяющие управлять возникшей информационной угрозой и повысить цифровой уровень российских предприятий [6]:

–при получении подозрительной ссылки стоит убедиться, что на другом конце провода реально существующий человек;

– на сайты, требующие ввода личных данных, входить по ссылкам вообще не стоит, лучше набрать адрес вручную (вход должен осуществляться через надежные устройства и сети);

– необходимо использовать и регулярно обновлять антивирусные продукты, особенно если они представляют антифишинговые решения (модуль «Антифишинг», встроенный в Kaspersky Internet Security, сверяющий со списком уже известных мошеннических сайтов и опознающий потенциально опасные по более чем 200 критериям).

2. APT-угрозы (77 %) – сложная постоянная угроза (APT) является высокоточной кибератакой, с помощью которой происходит кража конфиденциальной информации.

Для эффективной борьбы с APT-угрозами целесообразно применять прогрессивные меры [7]:

– интеллектуальные методы детектирования аномалий в компьютерной системе: экспертный анализ сетевого трафика, диагностика приемов социальной инженерии пользователями, обученными по особым программам и др.;

– сигнатурные методы в этом случае малоэффективны, поскольку атаки узконаправлены, а средства совершения киберпреступлений неповторимы.

3. Вымогательское ПО (77 %) – вредоносная программа-вымогатель, содержащая сообщение и изображение активиста Anonymous в маске и надпись «You have been Hacked» («Вас взломали»), текст на фарси с требованием оплаты выкупа в обмен на восстановление закодированных файлов.

Меры успешной борьбы – не кликать на экране кнопку с надписью «Click Me» («Кликни на меня») [8].

4. DDOS-атаки (75 %) – это враждебное внешнее воздействие на вычислительные источники сервера или рабочей станции, проводимое с целью доведения их до отказа.

Меры успешной борьбы – контроль за тем, чтобы устройства не были заражены разного рода вирусами и вовремя получали обновления.

5. Распространение BYOD (74 %) – так называемая «корпоративная мобильность», возможность хранить персоналу корпоративные данные локально на персональных мобильных устройствах.

Меры успешной борьбы – акцентировать внимание на риске физической утери или кражи мобильных устройств. Стратегия безопасности BYOD следующая (табл. 1).

Таблица 1

Меры борьбы с угрозами при использовании BYOD [9]

Понятие	Содержание
Безопасность BYOD = «MDM» + «App» + «VPN» + «VM» + «DLP»	
«MDM»	Система для контроля локальных приложений на устройствах, удаленного уничтожения данных, обеспечения надежной парольной защиты устройства и шифрования данных и т.п.
«App»	Приложение для удаленного подключения мобильного устройства через Интернет к виртуальному хостингу приложений организации (например, Citrix Receiver)
«VPN»	Защищенное криптографическим протоколом SSL подключение к виртуальной частной сети организации (Virtual Private Network), используемое опубликованными приложениями, в том числе для дополнительной аутентификации пользователей
«VM»	Виртуальная реализация Windows-системы на базе средств виртуализации Citrix/WTS/MS RDx и др., предоставляющая пользователям рабочую среду, в которой могут быть опубликованы и доступны необходимые для работы приложения и данные
«DLP»	Система предотвращения утечек данных, интегрированная в виртуальную рабочую среду Windows, обеспечивающая контроль доступных в этой виртуальной среде каналов передачи данных (электронная почта, веб-сайты, мессенджеры, канал печати, перенаправленные в виртуальную среду локальные USB-устройства) для предотвращения утечек данных с BYOD-устройства

В заключение можно сделать вывод о том, что преступники в области информационных атак обращают свое внимание в большинстве своем на новые цифровые технологии для достижения своих целей. Появился на горизонте новый ресурс информационной безопасности предприятия – они тут же учатся использовать это предприятие для добычи необходимых данных. Так что в последующие годы придется наблюдать за этой гонкой технологий и противостоянием экспертов в области защиты информационной безопасности.

Библиографический список

1. Кибербезопасность – 2018−2019: итоги и прогнозы // Positive Technologies : сайт. – URL: https://www.ptsecurity.com/2018
2. Программа «Цифровая экономика Российской Федерации». – URL: http:// govemment.ru/docs/2865з (дата обращения: 01.02.2018).
3. О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы : Указ Президента РФ от 09.05.2017 № 203 // СПС «КонсультантПлюс».
4. **Махалин, В. Н.** Управление вызовами и угрозами в цифровой экономике России / В. Н. Махалин, О. М. Махалина. – URL: https://cyberleninka.ru/2018
5. **Коваленко, А.** Играем с первой цифры // Эксперт-Урал. – 2017. – № 26 (733). – С. 12–20. – URL: http://www.acexpert.ru/ агсЬIуе/потег-26-733^гает-8-регуоу-с1М.Мт1 (дата обращения: 01.02.2018).

6. Почему работает фишинг и как с ним бороться / Блог Евгения Касперского. – URL: https://www.kaspersky.ru/2014
7. Компания «FRinted». Проблемы информационной безопасности: направленные атаки. – URL: https://arinteg.ru/ (дата обращения: 17.04. 2019).
8. Новое вымогательское ПО маскируется под игру Click Me // Pikabu : сайт. – URL: https://pikabu.ru
9. Блог Devicelock 5 мифов о безопасности BYOD. – URL: https://www.devicelock.com/ (дата обращения: 01.02.2018).

References

1. *Sayt Positive Technologies Kiberbezopasnost' – 2018−2019: itogi i prognozy* [The website “Positive Technologies” Cyber Security – 2018-2019: results and forecasts]. Available at: https://www.ptsecurity.com/2018 [In Russian]
2. *Programma «Tsifrovaya ekonomika Rossiyskoy Federatsii»* [Program “The digital economy of the Russian Federation”]. Available at: http://govemment.ru/docs/2865z (accessed Febr. 01, 2018). [In Russian]
3. *O Strategii razvitiya informatsionnogo obshchestva v Rossiyskoy Federatsii na 2017–2030 gody: Ukaz Prezidenta RF ot 09.05.2017 № 203* [On the Strategy of informational society development in the Russian Federation in 2017-2030]. RRS «ConsultantPlus». [In Russian]
4. Makhalin V. N., Makhalina O. M. *Upravlenie vyzovami i ugrozami v tsifrovoy ekonomike Rossii* [Managing challenges and threats to the digital economy of Russia]. Available at: https://cyberleninka.ru/2018 [In Russian]
5. Kovalenko A. *Igraem s pervoy tsifry* [Playing from the first digit]. Ekspert-Ural. 2017, no. 26 (733), pp. 12–20. Available at: http://www.acexpert.ru/ agsYue/poteg-26-733^gaet-8-reguou-s1M.Mt1 (accessed Febr. 01, 2018). [In Russian]
6. *Pochemu rabotaet fishing i kak s nim borot'sya* [Why fishing works and how to fight it]. Blog Evgeniya Kasperskogo. Available at: https://www.kaspersky.ru/2014 [In Russian]
7. *Kompaniya «FRinted». Problemy informatsionnoy bezopasnosti: napravlennye ataki* [“FRinted” company. Information security problems: direct attacks]. Available at: https://arinteg.ru/ (accessed Apr. 17, 2019). [In Russian]
8. *Novoe vymogatel'skoe PO maskiruetsya pod igru Click Me* [A new extortion software disguising as Click Me game]. Pikabu: site. Available at: https://pikabu.ru [In Russian]
9. *Blog Devicelock 5 mifov o bezopasnosti BYOD* [Devicelock blog. 5 myths about BYOD security]. Available at: https://www.devicelock.com/ (accessed Febr. 01, 2018). [In Russian]

Щеглов Вадим Юрьевич
старший преподаватель, кафедра менеджмента и экономической безопасности, Пензенский государственный университет (Россия, г. Пенза, ул. Красная, 40)

E-mail: sheglov.pgy@mail.ru

Надькина Алена Алексеевна
студентка, Пензенский государственный университет (Россия, г. Пенза, ул. Красная, 40)

E-mail: tatyananadkina@yandex.ru

Shcheglov Vadim Yur'evich
Senior lecturer, sub-department of management and economic security, Penza State University (40 Krasnaya street, Penza, Russia)

Nad'kina Alena Alekseevna
Student, Penza State University (40 Krasnaya street, Penza, Russia)

Образец цитирования:

Щеглов, В. Ю. Угрозы информационной безопасности предприятий в связи с цифровой трансформацией экономики и возможности их нейтрализации / В. Ю. Щеглов, А. А. Надькина // Известия высших учебных заведений. Поволжский регион. Экономические науки. – 2019. – № 1 (9). – С. 33–39. – DOI 10.21685/2309-2874-2019-1-4.