Анастасия Владимировна Милойчикова
студентка специальности «Экономическая безопасность» Владимирского государственного университета им. А. Г. и Н. Г. Столетовых, г. Владимир, nastya.miloychikova.02@mail.ru

Марина Александровна Гундорова
кандидат экономических наук, доцент кафедры «Экономика инноваций и финансы» Владимирского государственного университета им. А. Г. и Н. Г. Столетовых, г. Владимир, mg82.82@mail.ru

К ВОПРОСУ ЦИФРОВИЗАЦИИ БИЗНЕС-ПРОЦЕССОВ

Аннотация. В настоящей статье авторами рассматриваются киберпреступления как один из способов подрыва экономической безопасности предприятий. В работе приводится статистика в области цифрового мошенничества и производится анализ влияния мошеннических операций на финансово-экономическое состояние компаний. Работа завершается предложением мер по снижению вероятности реализации мошеннических схем в организациях.

Ключевые слова: экономическая безопасность, цифровизация, технологический прогресс, мошенничество, киберпреступления.

Anastasia Vladimirovna Miloychikova
Student of the specialty "Economic security" of the Vladimir State University named after A. G. and N. G. Stoletov, Vladimir, nastya.miloychikova.02@mail.ru

Marina Alexandrovna Gundorova
Candidate of Sciences (Economics), Associate Professor of the Department of Economics of Innovation and Finance Vladimir State University named after A. G. and N. G. Stoletov, Vladimir, mg82.82@mail.ru

ON THE ISSUE OF DIGITALIZATION OF BUSINESS PROCESSES

Abstract. In this article, the author examines cybercrimes as one of the ways to undermine the economic security of enterprises. The paper provides statistics in the field of digital fraud and analyzes the impact of fraudulent transactions on the financial and economic condition of companies. The work ends with a proposal of measures to reduce the likelihood of fraudulent schemes in organizations.

Keywords: economic security, digitalization, technological progress, fraud, cybercrime.

Жизнь человека не стоит на месте — технологии идут вперед. Меняются механизмы управления ресурсами, меняются инструменты экономической системы, вводятся новые правила и возникают новые условия как со стороны внешней среды, так и с точки зрения внутрикорпоративных требований. Безусловно, политика предприятий во многом обусловливается внешними факторами, однако стратегии развития формируются внутри самой организации — выбор точек роста, методов и инструментов ведения экономической борьбы, способы реализации намеченных текущих и оперативных планов. Все это — выбор руководителей организации.

Рыночная система обусловливает наличие выбора как для самих предпринимателей, так и для субъектов, вступающих с ними в экономические отношения. Для свободного рынка это абсолютное преимущество. Но если говорить об экономической безопасности как предприятий, так и страны — свобода выбора, плюрализм решений в сфере управления и финансово-экономических отношений время от времени представляют для организации значительные риски.

Повсеместное распространение информационных технологий, расширение перечня удаленных специальностей, дистанционное обучение и многое

другое позволяет осуществлять переход российского общества от индустриального к постиндустриальному этапу развития. Особенно активно цифровая трансформация в России началась в период пандемии Covid-19, когда многие специалисты были вынуждены продолжать работу несмотря на отсутствие возможности физического присутствия на рабочем месте. По результатам социологического исследования, проводимого в 2023 году Банком Открытие, были получены следующие данные об индексе цифровизации бизнеса (рис. 1).

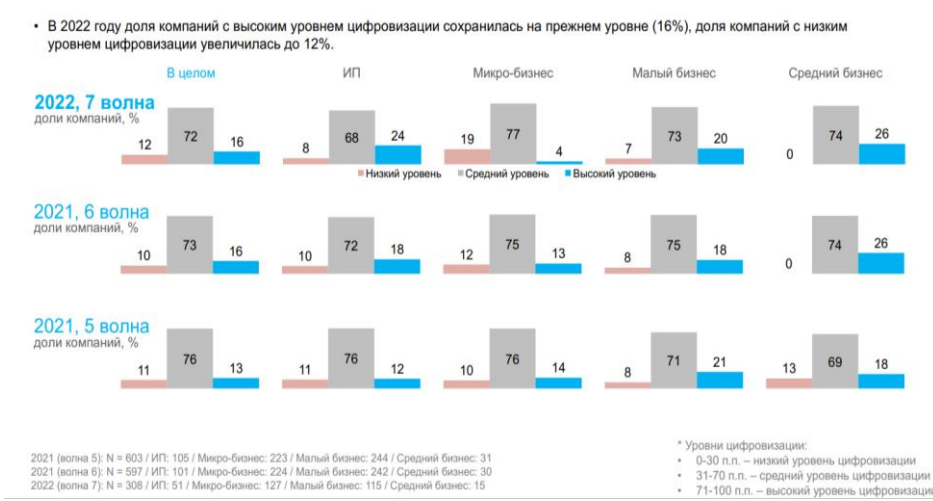

Рис. 1. Индекс цифровизации бизнеса

Источник: составлено авторами на основе данных [1].

Анализ представленной статистики показал, что среди ИП, малого и среднего бизнеса сократилась доля компаний с низким индексом цифровизации. Увеличился и объем ИП и МСБ с высоким уровнем цифровизации.

Расчет индекса цифровизации бизнеса включает в себя анализ таких показателей, как:

– цифровые каналы передачи данных — показатель уровня использования цифровых каналов для передачи и хранения информации (сюда входят облачные хранилища, корпоративные сети, автоматизированные системы, локальные мессенджеры и пр.);

– интеграция цифровых технологий — это показатель, отражающий объем внедренных в компании цифровых технологий (использование искусственного интеллекта, 3D-печать и пр.);

– использование интернет-инструментов — сайты компаний, аккаунты и каналы в социальных сетях и мессенджерах, HR- и PR-инструменты поиска сотрудников и узнаваемости компаний;

– уровень информационной безопасности;

– квалификация сотрудников — работа над обучением персонала, инвестиции в увеличение человеческого капитала.

Цифровые технологии повсеместно распространяются во всех сферах жизни, что значительно упрощает работу и обуславливает автоматизацию ряда процессов.

Однако развитие информационных технологий обусловило не только выход на новый уровень, но и определило ряд проблем для финансово-хозяйственной деятельности, которые зачастую приносят серьезные убытки компании, если вовремя их не обнаружить.

Согласно данным исследований компании Positive Technologies (российская компания, занимающая разработкой решений в области информационной безопасности) число успешно реализованных кибератак в сфере финансов ежегодно растет. Так, за третий квартал 2022 года насчитывалось в два раза меньше совершенных киберпреступлений, чем в аналогичном периоде 2023 года.

Среди наиболее популярных последствий кибератак выделяют утечку данных и остановку работы отдельных сервисов или ключевых бизнес-кейсов (рис. 2).

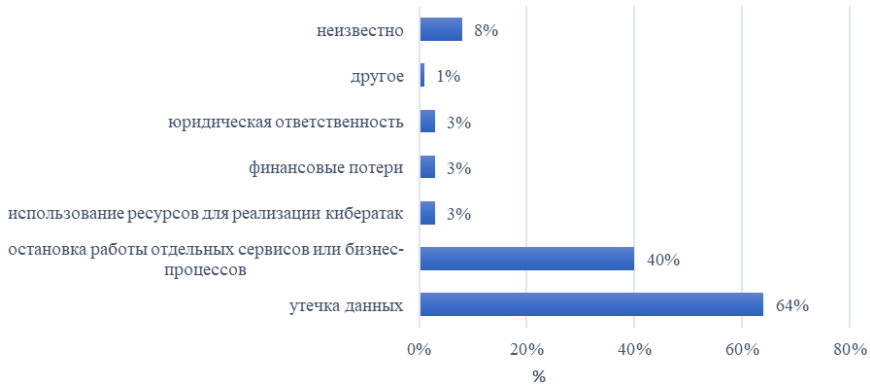

Рис. 2. Последствия кибератак в процентах за 2023 год

Источник: составлено авторами на основе данных [2].

В большинстве случаев утечка данных представляет собой «слив» персональных данных клиентов компаний и корпоративные сведения. Несколько реже распространяются учетные данные, реквизиты банковских карт, а в сфере страхования — медицинская информация (рис. 2).

Рис. 3. Статистика украденных данных компаний

Источник: составлено авторами на основе данных [2].

В августе 2023 года кибератаке подверглась компания «Ренессанс страхование», в результате чего преступниками было получено около 2% персональных данных клиентов [3].

По данным Роскомнадзора, в октябре 2023 года в результате кибератаки утекла персональная информация миллиона клиентов МТС Банка (в числе таких данных — ФИО, номера телефонов, ИНН, даты рождения, некоторые номера банковских карт) [4].

Примечательно, что в 2022 году объем утечки информации составлял 51%, что на 13% меньше имеющегося на конец 2023 года показателя, а вот вывести из строя основную деятельность компаний различного рода инцидентами удалось в 42% случаев, что на 2% больше, чем за последний анализируемый период. Такая тенденция объясняется тем, что среди мошеннических схем большее распространение получают более простые махинации, основным объектом которых становятся не юридические лица, а клиенты различных компаний. Таким образом, мошеннические схемы все больше проникают в жизнь обычных людей, что говорит о более частом их возникновении, но меньшими, с точки зрения доходности махинаций, результатами.

Несмотря на то, что штрафные санкции за утечку информации не приносят значительного ущерба компаниям, возникает риск подрыва репутации — так, например, нередки случаи, когда известия о кибератаках и хищении персональных данных клиентов приводили к снижению стоимость акций компаний.

Наибольшую распространенность получили шифровальщики — вредоносные программы, блокирующие доступ для авторизованных пользователей к системам и предоставляющие возможность управления и контроля злоумышленникам.

На втором месте по степени распространенности находится программное обеспечение типа «загрузчик», принцип работы которого основывается на установлении соединения с удаленным сервером, в следствие чего преступник устанавливает вредоносные программы (рис. 4).

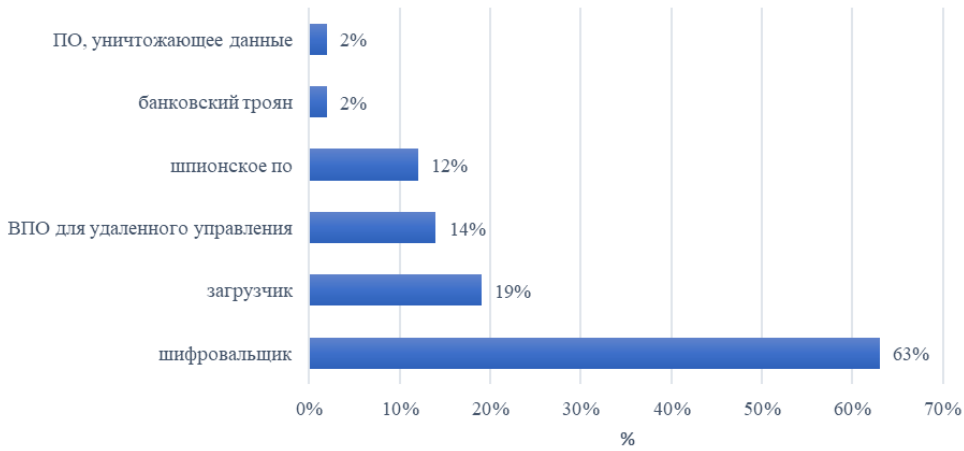

Рис. 4. Применяемые вредоносные программные обеспечения

Источник: составлено авторами на основе данных [2].

Исследователями было выявлено, что топ кибератак приходится именно на финансовую сферу.

Для того чтобы минимизировать количество киберпреступлений в финансовой сфере, со стороны правительства ужесточаются меры ответственности за несанкционированный доступ к персональным данным клиентов и их обработку. Сами же компании ведут активную работу над мерами обеспечения информационной и экономической безопасности.

В рамках работы автором предлагаются следующие мероприятия, которые бы способствовали обеспечению высокого уровня финансовой и экономической безопасности компании:

1) разработка и внедрение локальных программных обеспечений;

2) разработка отечественных антивирусных программ;

3) увеличение доли IT-специалистов на предприятии;

4) разработка локальных программ с разграничениями уровней доступа к информации;

5) периодическая проверка работников;

6) расширение отдела безопасности на предприятиях;

7) ужесточение контрольных мероприятий;

8) хранение персональных данных в локальных сетях компаний;

9) ужесточение ответственности за распространение и неправильное хранение и обработку персональных данных клиентов в компаниях.

Таким образом, реализациях предложенных мероприятий может способствовать сокращению числа кибератак на организации, ведь мошенники просто не смогут получить доступ к имеющимся в архивах данным.

В рамках работы была рассмотрена одна из глобальных угроз экономической безопасности предприятий — киберпреступления, число которых в последние годы только растет. В статье также приводится статистика индекса цифровизации ИП, МСБ и микробизнеса, производится анализ динамических показателей и делается вывод об актуальных трендах. Анализ и обработка изученной информации позволили определить меры по минимизации риска столкновения компаний с кибератаками.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Индекс цифровизации малого и среднего бизнеса business digitalization index — BDI Результаты социологического исследования 2022 (7 ВОЛНА) — Москва // Банк Открытие: сайт. — URL: https://academyopen.ru/media/news/ material/BDI_7_%D0%B2%D0%BE%D0%BB%D0%BD%D0%B0_2022.pdf?ysclid=lv84fakdg1129004326 (дата обращения: 12.04.2024).
2. Киберугрозы финансовой отрасли: промежуточные итоги 2023 года // Positive Technologies: сайт. — URL: https://www.ptsecurity.com/ru-ru/research/analytics/financial-industry-security-interim-2023/ (дата обращения: 12.04.2024).
3. Резанова-Яцкевич Е. В «Ренессанс Страховании» сообщили о прицельной хакерской атаке / Е. Резанова-Яцкевич // Газета.ru: сайт. — URL: https://www.gazeta.ru/business/news/ 2023/06/02/20585216.shtml (дата обращения: 12.04.2024).
4. Тюняева М. Роскомнадзор подтвердил факт утечки данных из МТС-банка / М. Тюняева // Ведомости: сайт. — URL: https://www.vedomosti.ru/finance/articles/2023/10/19/1001370-roskomnadzor-podtverdil-fakt-utechki-dannih-iz-mts-banka (дата обращения: 12.04.2024).