8. Бабкин А.В., Трысячный В.И. Стратегические направления совершенствования управления экономической безопасностью региона // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Экономические науки. 2009. № 4 (81). С. 201-205.

DOI: 10.18720/IEP/2021.3/214

Феофилова Т.Ю.[1], Маркин Л.К.[1]

КОРПОРАТИВНЫЕ ЗЛОУПОТРЕБЛЕНИЯ С ИСПОЛЬЗОВАНИЕМ ЦИФРОВЫХ ТЕХНОЛОГИЙ

[1]Санкт-Петербургский политехнический университет Петра Великого, Санкт-Петербург, Россия

Аннотация

Исследуются основные виды корпоративных злоупотреблений в цифровой среде, группы киберпреступлений, наносимый ущерб компаниям и выявление причин фактов злоупотреблений. Проведен анализ существующих практических методов предупреждения корпоративных злоупотреблений с использованием цифровых технологий, способов их применения и эффективности. Рассмотрены три группы злоупотреблений в цифровой среде компании, выявлены наиболее распространенные способы корпоративных злоупотреблений в каждой из групп. Сформированы практические рекомендации по модернизации внутреннего контроля с учетом осуществляемой деятельности и вероятности возникновения определенных злоупотреблений с использованием цифровых технологий внутри компании.

Ключевые слова: цифровизация экономики, корпоративные злоупотребления, цифровые технологии, экономическая безопасность, киберпреступность, методы противодействия злоупотреблениям.

Feofilova T.Y.[1], Markin L.K[1].

CORPORATE OVERINDULGENCE USING DIGITAL TECHNOLOGIES

[1]Peter the Great St. Petersburg Polytechnic University, St. Petersburg, Russia

Abstract

The main types of corporate misuses in the digital environment, groups of cybercrimes, damage to companies and the identification of the causes of abuse are investigated. The analysis of existing practical methods of preventing corporate overindulgence with the use of digital technologies, methods of their application and efficiency is carried out. Three groups of abuse in the digital environment of a company are considered, and the most common methods of corporate abuse in each of the groups are identified. Practical recommendations for the modernization of internal control have been formulated, considering the ongoing activities and the likelihood of certain misuses with the use of digital technologies within the company.

Keywords: digitalization of the economy, corporate overindulgence, digital technologies, economic security, cybercrime, methods of countering overindulgence.

Введение

В последние годы растет число киберпреступлений, значительная часть из них относится к корпоративным злоупотреблениям и совершается сотрудниками компаний. Проблема корпоративных злоупотреблений с использованием цифровых технологий стоит довольно остро, среди ключевых причин – цифровизация экономики, повсеместное внедрение новых информационных технологий и программного обеспечения, обусловленных переходом части компаний на удаленную работу. Все эти факторы, в совокупности, создают условия для осуществления корпоративных злоупотреблений в цифровой среде.

По данным исследования Forensic & Business Solutions на глобальном уровне 23% респондентов отметили, что их компании столкнулись с киберпреступлениями, которые стали вто-

рым самым распространенным видом корпоративного мошенничества после незаконного присвоения активов как в 2019, так и в 2020 году [1].

Целью исследования является исследование корпоративных злоупотреблений с использованием цифровых технологий и анализ, применяемых компаниями, методов противодействия злоупотреблениям данного вида.

Методы исследования

Для достижения целей исследования были использованы такие методы научного исследования, как: анализ, синтез, сравнение и выявление причинно-следственных связей. На первом этапе исследования была изучена теоретическая информация, представленная в ресурсах сети интернет, а также был проведен анализ полученной информации. На втором этапе был проведен анализ практических методов противодействия злоупотреблениям в цифровой среде, посредством изучения информации с сайтов профильных компаний и соответствующих исследовательских работ. Третий этап исследования заключался в сравнении полученной информации, выявлении причинно-следственных связей и формулировке выводов по результатам исследования.

Результаты

В публикациях представлены различные понятия определяющие противоправные деяния в цифровой среде. При этом наиболее используемым является понятие «киберпреступление», которое чаще всего понимается как преступная деятельность, осуществляемая с целью неправомерного использования компьютера, сетевого устройства или компьютерной сети. Также необходимо понимать, что можно правомерно использовать компьютер, но в преступных целях [2].

Исследователи выделяют несколько основных видов киберпреступлений. Э.Л. Кочкина подробно рассматривает несколько видов киберпреступлений: финансовые преступления, фишинг, кибертерроризм и незаконный оборот наркотиков и оружия посредством сети интернет [3]. Множество других исследователей также выделяют именно эти виды киберпреступлений в своих работах.

Злоупотребления в цифровой среде осуществляются и часто связаны с финансовыми потоками. Аналогичную точку зрения разделяют А.П Мальцева и А.В. Лошкарев, которые дают следующее определение: «корпоративные злоупотребления в информационной среде напрямую связаны с финансовыми преступлениями, данные злоупотребления – отдельный вид, характерным признаком которого является противозаконное использование своих должностных прав и возможностей с целью увеличения собственной прибыли в ущерб интересов компании, непосредственно совершенное с использованием цифровых систем компании.» [4].

В современных исследованиях принято классифицировать корпоративные злоупотребления по трем группам:

— неправомерное присвоение активов;

— фальсификация отчетности;

— корпоративная коррупция и взяточничество [5].

Цель цифровизации экономики – оптимизация бизнес-процессов, создание комфортной, «прозрачной» и безопасной среды, в которой компании ведут свою деятельность. Злоумышленники для себя находят в цифровизации иные преимущества – анонимность, моментальная передача данных и наличие уязвимостей даже в самых защищенных системах. Фродстеры используют цифровые технологии с целью получения собственной выгоды в каждой из трех групп корпоративных злоупотреблений.

Рассмотрим некоторые из существующих схем. Клиентская база – один из важнейших активов любой компании, технический прогресс позволил уйти от много килограммовых архивов, заполненных данными клиентов, к архивам на жестких дисках или облачных сервисах.

95% утечек информации происходит по достаточно простому сценарию: сотрудник (или иное лицо) скачивает файлы в папку, а затем отправляет их по почте. При этом, как правило, используют личные почтовые ящики, но несанкционированная передача происходит в рабочее время с использованием рабочих компьютеров. Реже злоумышленники скачивают информацию на носители, пересылают файлы через социальные сети и мессенджеры или отправляют на печать.

Для противодействия таким злоупотреблениям следует применять совокупность мер, используя комплексный подход. Однако, на первоначальном этапе, следует определить перечень информации, составляющей коммерческую тайну. Предотвратить утечку информации можно посредством контроля буфера обмена компьютеров сотрудников. Если работник скопирует файл на сторонний накопитель или прикрепит его к электронному письму – службе безопасности поступит уведомление о подозрительных операциях.

Взяточничество и корпоративная коррупция также практически полностью перешли в цифровую среду. Анонимность, моментальная передача данных и отсутствие необходимости в личных встречах, создают практически идеальные условия для коррупционеров. Сотрудники осознают опасность обсуждения подобных вопросов через корпоративные профили и стараются перевести разговор в мессенджер или на личный телефонный номер. Для организации противодействие такого вида злоупотреблениям, без привлечения правоохранительных органов задача крайне непростая, но существует ряд профилактических и предупреждающих мер, которые могут усложнить действия злоумышленников. Все переговоры с поставщиками, клиентами и иными лицами по рабочим вопросам должны совершаться только через официальные средства связи компании (корпоративная почта, рабочие сотовые и стационарные телефоны, факсы). При попытке перевести диалог в иное место, службе безопасности должно поступать соответствующее уведомление. Разработан ряд специальных программных обеспечений, позволяющих осуществлять мониторинг деловой переписки и телефонных звонков, по ключевым словам, или фразам, также есть возможность сортировки звонков и сообщений по времени, адресатам, и количеству контактов, что позволит службе безопасности увидеть, с кем, как часто и на какие темы сотрудник общается на рабочем месте.

Фальсификация отчетности все еще остается одним из самых распространенных корпоративных злоупотреблений. Среди схем мошенничества с отчетностью – завышение стоимости материалов, искажение остатков, завышение или занижение финансовых результатов и так далее. В настоящее время мошенникам становится труднее осуществлять махинации с отчётностью, в случае несанкционированного вмешательства остается след в информационно-технической среде. Он может быть не виден при непосредственном изучении данных, но хорошо распознается специальными компьютерными алгоритмами.

В 2021 году одна из компаний «большой четверки» - «Делойт Форензик» опубликовала свое исследование, посвященное проблемам злоупотреблений, с которыми пришлось столкнуться компаниям России и СНГ в последние годы. Согласно проведенному опросу, 56% респондентов отметили, что виновниками мошеннических действий являются сотрудники среднего звена, к такому мнению пришли все компании, вне зависимости от отрасли деятельности и численности сотрудников, и в 27% случаев правонарушения были связаны с утечкой данных и киберпреступлениями [6]. Респонденты также отмечают, что наиболее подвержены злоупотреблениям отделы закупок и продаж. Такие отделы, практически в каждой компании являются наиболее «цифровизированными», что на практике доказывает возможность использования цифровых и информационных технологий злоумышленниками в преступных целях.

При использовании в компании мобильного приложения, можно получать регулярные отчеты о передвижении своего персонала, что особенно актуально для компаний, имеющих мобильные офисы продаж или работающих с курьерами.

Заключение

Для компаний ущерб от корпоративных злоупотреблений не так заметен, как от сторонних мошеннических действий. Статистически, ущерб от корпоративных злоупотреблений для компаний с выручкой менее 10 млн долл. США составляет 1–2% от выручки за год, такие же средние значения ущерба и для компаний с годовой выручкой 10–500 млн долл. США и 500+ млн долл. США.

Нельзя отрицать очевидные преимущества повсеместной цифровизации экономики и внедрения все большего количества информационных технологий для упрощения ведения бизнеса, составления финансовой отчетности и создания более безопасной экономической среды для компаний. Технический прогресс невозможно остановить, он будет охватывать практически все сферы хозяйственной деятельности организаций, устанавливать новые правила рынка и модернизировать сложившуюся экономику. Компаниям, в этих условиях, следует особое внимание уделять повышению эффективности обеспечения экономической безопасности. Для этого компаниям, помимо внедрения новых программных обеспечений и систем, следует заранее продумывать методы контроля за использованием этих систем сотрудниками и обеспечить построение эффективной службы безопасности и мониторинга существующих рисков.

Литература

1. *Прогноз потерь Российского бизнеса и руководство по борьбе с мошенничеством и конфликтом интересов ООО «Бизнес Форензик Компани» [Электронный ресурс] // Сайт ООО «Бизнес Форензик Компани» URL: https://forensic.su/fraudpreventionguide2020 (дата обращения: 26.10.2021).*

2. *Бертовский, Л. В. К вопросу о понятии киберпреступления / Л. В. Бертовский // Расследование преступлений: проблемы и пути их решения. – 2020. – № 4. – С. 84–88.*

3. *Кочкина, Э. Л. Определение понятия "киберпреступление". Отдельные виды киберпреступлений / Э. Л. Кочкина // Сибирские уголовно-процессуальные и криминалистические чтения. – 2017. – № 3(17). – С. 162–169.*

4. *А. П. Мальцева, А. В. Лошкарев Влияние цифровой экономики на киберпреступность // Международный журнал гуманитарных и естественных наук. 2019. №10–2.*

5. *Когденко В.Г. Корпоративное мошенничество: анализ схем присвоения активов и способов манипулирования отчетностью // Экономический анализ: теория и практика. 2015. №4 (403).*

6. *Корпоративное мошенничество АО «Делойт СНГ» [Электронный ресурс] // Сайт АО «Делойт СНГ» URL: https://www.deloitte.com/2021/corporate-fraud-results.html (дата обращения: 26.10.2021).*