Елизавета Сергеевна Прыткова
Санкт-Петербургский государственный университет, РФ
st121232@student.spbu.ru

Ольга Викторовна Медяник
Санкт-Петербургский государственный университет, РФ
o.medyanik@spbu.ru

ВЛИЯНИЕ КИБЕРМОШЕННИЧЕСТВА НА ДЕЯТЕЛЬНОСТЬ СТРАХОВЫХ КОМПАНИЙ В РОССИИ

Аннотация. В статье рассматриваются основные проблемы и вызовы, с которыми сталкиваются страховые компании в борьбе с кибермошенничеством. Актуальность данной темы обусловлена необходимостью разработки и внедрения новых подходов и инструментов для защиты от кибермошенничества, чтобы минимизировать потери и обеспечить надежную защиту интересов как компаний, так и их клиентов. Страховой сектор, как один из ключевых элементов финансовой системы, нуждается в постоянном анализе угроз и разработке эффективных мер противодействия киберпреступности. В статье представлена классификация видов украденных данных при осуществлении кибератак на финансовый сектор, а также сформированы и описаны основные виды кибермошенничества в страховой отрасли, возможные варианты ущерба в результате данного вида мошеннических действий. Указаны методы борьбы страховых компаний с кибермошенничеством в технологическом, образовательном и правовом аспектах.

Ключевые слова: страхование, кибермошенничество в страховании, виды кибермошенничества, методы борьбы с кибермошенничеством в страховых компаниях

Elizaveta S. Prytkova
St. Petersburg State University, Russian Federation
st121232@student.spbu.ru

Olga V. Medyanik
St. Petersburg State University, Russian Federation
o.medyanik@spbu.ru

IMPACT OF CYBER FRAUD ON THE ACTIVITIES OF INSURANCE COMPANIES IN RUSSIA

Annotation. The article discusses the main problems and challenges that insurance companies face in the fight against cyber fraud. The relevance of this topic is due to the need to develop and implement new approaches and tools for protection against cyber fraud in order to minimize losses and ensure reliable protection of the interests of both companies and their clients. The insurance sector, as one of the key elements of the financial system, needs to constantly analyze threats and develop effective measures to combat cybercrime. The article presents a classification of the types of stolen data during cyber attacks on the financial sector, as well as the main types of cyber fraud in the insurance industry and possible damage options as a result of this type of fraudulent activity. Methods for insurance companies to combat cyber fraud in technological, educational and legal aspects are indicated.

Keywords: insurance, cyber fraud in insurance, types of cyber fraud, methods of combating cyber fraud in insurance companies

Введение.

В современном мире, где большинство операций и взаимодействий происходит в цифровом пространстве, кибермошенничество является одной из ключевых угроз для всех секторов экономики, включая страховую отрасль. Кибермошенничество в страховой отрасли представляет собой серьезную угрозу, поскольку оно не только влечет за собой финансовые потери для компаний, но и подрывает доверие клиентов к страховому сектору в целом.

Количество успешных кибератак в финансовом секторе год от года растет. К последствиям подобного рода атак относятся: утечка данных, остановка работы отдельных сервисов или ключевых бизнес-процессов. Подавляющее большинство утечек содержат персональные данные клиентов и коммерческую информацию организаций. Кроме того, среди утечек нередко можно обнаружить

номера платежных карт и учетные данные, в утечках страховых компаний присутствует медицинская информация.

На рисунке 1.1 представлены типы украденных данных в осуществленных атаках на финансовые организации (в том числе страховые компании) за период с первых трех кварталов 2023 года.

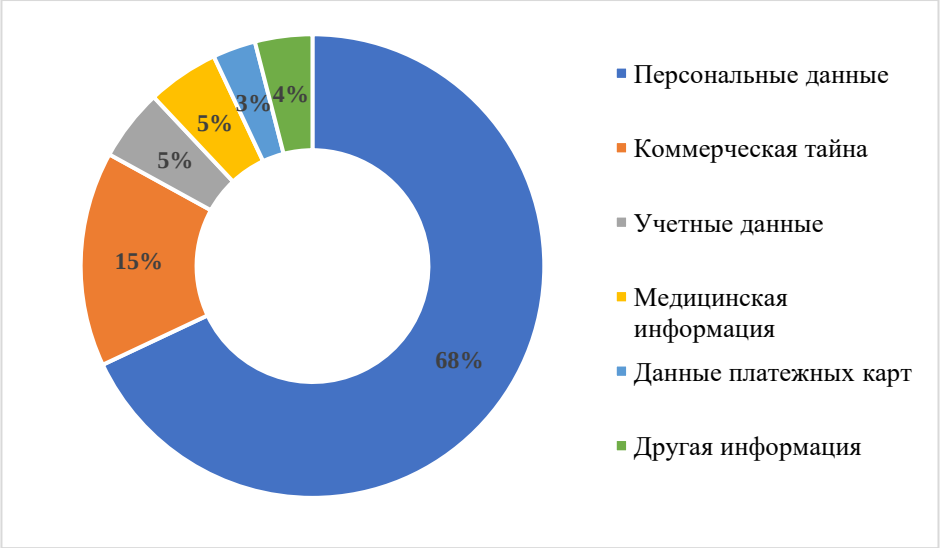

Рисунок 1.1 Типы украденных данных в успешных атаках на финансовые организации

Источник: Positive Technologies: https://www.ptsecurity.com/ru-ru/

В июне 2023 года «Ренессанс Страхование» подверглась кибератаке на один из разделов сайта — сервис еОСАГО, в результате которой преступники получили доступ к примерно 2% клиентской базы[1]. С каждым днем кибермошенничество становится все более сложным и разнообразным, поэтому требует соответствующей реакции от страховых компаний.

[1] https://www.ptsecurity.com/ru-ru/research/analytics/financial-industry-security-interim-2023/#id1 (дата обращения 21.02.2024).

Кибермошенничество – сравнительно новый феномен, представляющий собой активные действия в онлайн-формате с целью получения выгоды посредством манипуляций сознанием человека. Кибермошенничество появилось и развивается в Интернет-пространстве. Оно связано с похищением и использованием личных данных человека для совершения экономических преступлений, а также используется и в других сферах – политике, рекламе [2].

Кибермошенничество в страховании можно классифицировать следующим образом:

– фишинг;

Фишинговые атаки, в первую очередь, направлены на получение конфиденциальной информации (паролей и логинов от личных кабинетов на сайтах страховых компаний, данных банковских карт и т.д.). Мошенники обычно используют 2 основных метода сбора информации: электронные письма и сайты-клоны. В первом методе происходит отправка сообщений от имени ранее известных страховых компаний с просьбой обновить личные данные или подтвердить информацию о страховке. Сайты-клоны подразумевают создание веб-сайтов, визуально похожих на официальные сайты страховых компаний, для кражи данных всех пользователей.

– атаки на информационные системы;

Данные атаки направлены на нарушение работы информационных систем страховых компаний или кражу конфиденциальных данных. Это могут быть вирусы и троянские программы, которые распространяют вредоносное программное обеспечение для получения доступа к системам и данным, а также

DDoS-атаки, представляющие собой организацию массированных запросов к серверам компании с целью их перегрузки и выведения из строя.

– мошенничество с использованием искусственного интеллекта и машинного обучения.

Вместе с прогрессом в области искусственного интеллекта и машинного обучения появляются новые возможности для мошенников в том числе в сфере страхования. Данные технологии могут использоваться для создания поддельных документов (например, алгоритмы глубокого обучения для генерации документов, которые сложно отличить от настоящих) или автоматизации фишинга (создание алгоритмов, способных автоматически отправлять персонализированные фишинговые сообщения большому количеству потенциальных жертв).

Каждый из этих видов кибермошенничества требует от страховых компаний постоянного совершенствования своих методов защиты и внедрения новейших технологических решений для обеспечения безопасности данных и финансовых активов.

Влияние кибермошенничества на страховые компании проявляется в многоаспектном воздействии как на внутренние процессы фирмы, так и на её внешнее восприятие. Основными последствиями в результате кибермошенничества являются:

– финансовые потери;

Кибермошенничество может привести к значительным финансовым потерям для страховых компаний через незаконные выплаты по поддельным или преувеличенным страховым требованиям. Банк России, страховщики и их объединения ежегодно выявляют в социальных сетях, сервисах обмена

мгновенными сообщениями и на интернет-сайтах более 5 тыс. источников активного распространения информации о предоставлении услуг по оформлению договоров страхования со стороны нелегальных страховщиков и незаконных посредников. Существенная доля договоров ОСАГО в электронном виде заключается с аномально низкой страховой премией.

По оценкам Банка России, число заключенных в электронном виде договоров ОСАГО с недостоверными сведениями составляет не менее 1,1 млн (около 3% рынка ОСАГО), а ущерб автовладельцев (присвоение средств страхователей) и страховщиков (недополученные страховые премии) от противоправной деятельности в сфере электронного ОСАГО составляют не менее 4,2 млрд рублей[2].

– репутационный ущерб;

Репутация страховой компании играет ключевую роль в привлечении новых клиентов и удержании текущих. Информация о случаях кибермошенничества может нанести серьезный ущерб репутации компании, что затруднит привлечение новых клиентов и расширение бизнеса.

– правовые последствия.

В случае несоблюдения законодательства о защите данных или неспособности должным образом реагировать на кибератаки, страховые компании могут столкнуться с штрафами и санкциями со стороны регуляторных органов.

На данный момент в РФ за утечку персональных данных компании грозит фиксированный штраф (ч.1 ст. 13.11 КоАП) [1]. В

[2] https://cbr.ru/press/event/?id=12790 (дата обращения 22.02.2024).

свою очередь, в январе 2024 года Госдума на пленарном заседании приняла законопроект об усилении ответственности за утечку персональных данных.

В связи с перечисленными последствиями влияния кибермошенничества на страховую отрасль, компании данного сектора используют комплексный подход в борьбе с данным видом мошенничества, включающий в себя методы, связанные с технологическими, образовательными и правовыми мерами.

Технологические меры включают в себя:

– использование многофакторной аутентификации (MFA);

MFA значительно усложняет несанкционированный доступ к системам, требуя от пользователя предоставления двух или более факторов аутентификации перед доступом к аккаунту. MFA служит мощным защитным механизмом против фишинговых атак

– технология «блокчейн»;

Обеспечивает криптографическую защиту при хранении конфиденциальной информации. Это важно для страховщиков, поскольку им приходится взаимодействовать со множеством посредников, и на каждом этапе есть риск утечки данных. Также блокчейн-технологии снижают издержки и упрощают бизнес-процессы. Не нужно подписывать договоры вручную и хранить полисы: все это можно сделать онлайн и отправить в распределенную базу данных, которая гарантирует, что документы не украдут и не подделают.

– шифрование данных.

Защита конфиденциальной информации с помощью шифрования как в состоянии покоя, так и при передаче данных

помогает предотвратить утечки информации даже в случае проникновения мошенников в систему.

Образовательные меры сводятся, в первую очередь, к обучению персонала, повышению осведомленности сотрудников в сфере кибермошенничества. Для этого в страховых компаниях регулярно проводятся тренинги по кибербезопасности для обучения сотрудников распознаванию и правильному реагированию на попытки фишинга, социальной инженерии и другие виды киберугроз.

Сотрудничество с правоохранительными органами и обмен информацией на предмет новых мошеннических схем – правовые меры борьбы страховых компаний с кибермошенничеством. Также страховые компании могут сотрудничать в рамках государственных и международных программ по кибербезопасности, обмениваться информацией о новых методах мошенничества и киберугрозах не только с правоохранительными органами, но и с другими организациями.

Заключение.

Кибермошенничество представляет серьезную угрозу для страховой отрасли, требующую комплексного подхода к решению. Страховые компании должны постоянно совершенствовать свои методы защиты, а также развивать сотрудничество с другими участниками рынка и правоохранительными органами для эффективной борьбы с этим явлением.

Методы, перечисленные в данной статье, не являются исчерпывающими и должны рассматриваться как часть комплексной стратегии кибербезопасности. Для того чтобы страховые компании смогли эффективно бороться с

кибермошенничеством и защищать своих клиентов от потенциальных угроз, необходимо обеспечить такую систему безопасности, которая позволит исключить возможность нанесения неприемлемого ущерба страховой организации даже в случае проникновения нарушителя.

Список литературы.

1. "Кодекс Российской Федерации об административных правонарушениях" от 30.12.2001 N 195-ФЗ (ред. от 25.12.2023) (с изм. и доп., вступ. в силу с 05.01.2024). – URL: https://base.garant.ru/12125267/b369434ee740927935cc6f0a04242543/?ysclid=lt4wnvkt1k534125957

2. Красовская Н.Р., Гуляев А.А. К вопросу о кибермошенничестве // Вестн. Удм. ун-та. Социология. Политология. Международные отношения. 2022. Т. 6, вып. 1. С. 133–138. https://doi.org/10.35634/2587-9030-2022-6-1-133-138

3. Банк России : Противоправная деятельность в сегменте онлайн-страхования: масштабы, причины, противодействие. – URL: https://cbr.ru/press/event/?id=12790 (дата обращения 22.02.2024). – Текст: электронный.

4. Positive Technologies : Киберугрозы финансовой отрасли: промежуточные итоги 2023 года. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/financial-industry-security-interim-2023/#id1 (дата обращения 20.02.2024). – Текст: электронный.