УДК/UDC 658

Необходимость использования методов информационной безопасности для предотвращения эконмических потерь от киберпреступлений

Косюга Олег Сергеевич
студент факультета прикладной информатики
Кубанский государственный аграрный университет им. И. Т. Трубилина
г. Краснодар, Россия
e-mail:kosugaoleg1998@gmail.com

Лытнев Николай Николаевич
ассистент кафедры компьютерных технологий и систем
Кубанский государственный аграрный университет им. И. Т. Трубилина
г. Краснодар, Россия
e-mail:lytnev.nikolai@yandex.ru

Усенко Анатолий Сергеевич
аспирант кафедры криминалистики
Кубанский государственный аграрный университет им. И. Т. Трубилина
г. Краснодар, Россия
SPIN-код: 9594-2433
ORCID: 0000-0002-8332-9340
e-mail: ceo@epomen.ru

Аннотация

В современном мире происходит все более активное развитие и внедрение информационных технологий практически во всех сферах жизни человека и общества. В свою очередь, наблюдается рост преступности в данной сфере. Рассматриваемые преступления основываются на методах обхода защитных механизмов программ и сайтов, а также на различных способах незаконного получения конфиденциальной информации, в связи с чем возникает необходимость в оперативном реагировании на возникшие угрозы со стороны преступников. В статье авторами изучаются различные примеры экономических преступлений с использованием информационных

технологий. Также предлагаются методы борьбы с ними с целью предотвращения незаконного получения конфиденциальной информации от организаций, что влечет за собой финансовые потери самых разных масштабов.

Ключевые слова: интернет, электронный бизнес, киберпреступность, интернет-мошенничество, защита персональных данных.

The need to use information security techniques to prevent economic losses from cybercrime

Kosyuga Oleg Sergeyevich
student of the faculty of Applied Informatics
Kuban State Agrarian University
Krasnodar, Russia
e-mail:kosugaoleg1998@gmail.com

Lytnev Nikolay Nikolayevich
assistant of the Department of Computer Technologies and Systems
Kuban State Agrarian University
Krasnodar, Russia
e-mail:lytnev.nikolai@yandex.ru

Usenko Anatoliy Sergeyevich
graduate student of the Department of Criminology
Kuban State Agrarian University
Krasnodar, Russia
SPIN-код: 9594-2433
ORCID: 0000-0002-8332-9340
e-mail: ceo@epomen.ru

Abstract

In the modern world, there is an increasingly active development and implementation of information technologies in almost all spheres of human life and society. In turn, there is an increase in crime in this area. The crimes under consideration are based on methods of bypassing the protection mechanisms of programs and websites, as well as on various methods of illegally obtaining confidential information, and therefore there is a need for a prompt response to emerging threats from criminals. In the article, the authors study various examples of economic crimes using information technology. Methods are also

proposed to combat them in order to prevent the illegal receipt of confidential information from organizations, which entails financial losses of various scales.

Key words: internet, e-business, cybercrime, internet fraud, personal data protection.

С развитием информационного общества внедрение IT-технологий проходит огромными темпами. Информационные технологии развиваются и используются практически во всех сферах жизни общества. В свою очередь, не отстают и преступники. Они разрабатывают методы обхода защитных механизмов и способы кражи конфиденциальной информации. Из-за этого появляется острая необходимость оперативно реагировать на возникшие угрозы со стороны преступников. В 2019 г. в мире каждые 13–15 секунд происходили кибератаки. Это данные международных экспертов по кибербезопасности Cybersecurity Ventures. Также в 2019 г., по сообщениям специалистов Сбербанка, на 6% участились случаи мошенничества с использованием технологий социальной инженерии. Самой главной целью для хакеров являются данные корпораций, которые мошенники получают посредством целевых атак на персонал организации [1].

Перечислим основные схемы, которые применяют кибермошенники в странах СНГ:

1. Фишинг — отсылка специализированных электронных писем с вложенным в них вредоносным программным обеспечением, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям.
2. Вишинг — использование мобильной связи с целью украсть персональные и платежные данные. Когда мошенники под видом сотрудников банка, кредитных учреждений, работников правоохранительных органов и госучреждений пытаются узнать эти данные.
3. Использование банковских карт и платежных систем, в т. ч. заем денег у финансовых организаций. Чаще всего это про-

исходит после отправки или размещения в информационно-телекоммуникационной сети «Интернет» копий документов или платежных карт (счетов) будущих жертв преступлений.

4. Создание поддельных интернет-магазинов, которые продают несуществующий товар и просят внесение предоплаты, а также имитация реализации товаров или услуг через интернет-аукцион, виртуальные доски объявлений, выигрыш в лотерею или получение приза.
5. Использование поддельных сервисов для перевода денег или пополнения мобильных телефонов.

Скамер (от англ. scam — мошенничество, жульничество, обман) — это личность, которая совершает мошеннические сделки. Злоумышленник пользуется доверительным отношением людей и тем самым получает любые персональные данные пользователей для совершения киберпреступлений. Он хорошо знает психологию, поэтому легко входит в доверительные отношения с жертвой, получая всю необходимую информацию противоправными методами [2].

С ростом количества атак на организации растет и причиняемый ущерб. Специалисты Сбербанка предполагают, что размер причиненных убытков составил около 2,5 трлн долларов в 2019 г., а, например, в 2018 г. эта цифра равнялась 1,5 трлн долларов. Такими темпами сумма ущерба может вырасти до 8 трлн долларов во всем мире к 2022 г. Одной из причин такого роста киберпреступности является активное внедрение новых технологий в повседневную жизнь людей. За счет все большего числа подключенных разнообразных устройств к информационно-телекоммуникационной сети «Интернет» у злоумышленников появляется все больше возможностей для успешного совершения преступления. Так, к 2023 г. около 80% людей будет иметь доступ к большому количеству интернет-ресурсов, которые, в свою очередь, предоставляют возможность киберпреступнику осуществлять разные виды атак на пользователей [3].

Хотя и существует множество алгоритмов защиты информации, самым уязвимым звеном всегда будет сам человек (пользователь). Какой бы надежной ни является система защиты данных, если сотрудник подвергнется атаке социального инженера, то не будет никакой гарантии, что через него не произойдет утечки конфиденциальной информации организации. Последствия могут быть самыми разными: сотрудник будет являться либо частью более крупного мошеннического плана, либо основной жертвой злоумышленников, что повлечет за собой фатальные последствия для организации или даже причинение вреда здоровью людей [4].

Для предотвращения подобных случаев необходимо создание высокоэффективного отдела по защите информации и защите доступа. Первостепенной задачей данного отдела является внедрение системы контроля доступа и обучение сотрудников правилам противодействия всевозможным угрозам как со стороны виртуального, так и со стороны реального мира [5].

Именно поэтому требуется разработать систему контроля доступа, где передача конфиденциальной информации в корпоративной сети будет осуществляться на основе различных методов шифрования. Сейчас крупные компании создают свою комплексную систему защиты, которая позволяет защитить организацию от потери конфиденциальной информации и предотвратить саботаж. Как показывает практика, девять из десяти диверсий совершаются людьми, которые связаны с IT инфраструктурой, в связи с чем для предотвращения атак необходимо создавать и использовать новые, более сложные алгоритмы шифрования.

Также, на наш взгляд, с целью сокращения роста преступности следует более активно проводить разъяснительную работу как со стороны правоохранительных органов, так и со стороны иных органов государственной власти с различными группами населения о наиболее распространенных схемах мошенничества с использованием мобильной связи и информационно-телекоммуникационной сети «Интернет».

Список литературы:

1. Потери_организаций_от_киберпреступности. // TAdviser — портал выбора технологий и поставщиков. URL: https://www.tadviser.ru/index.php/Статья:Потери_-организаций_от_киберпреступности (дата обращения: 17.02.2022).

2. Скамеры — новое название, старые схемы // Финансовая грамотность населения. Проект Министерства финансов Ставропольского края. URL: https://fingram26.ru/articles/riski-i-finansovaya-bezopasnost/6981/ (дата обращения: 17.02.2022).

3. На Международном Конгрессе по кибербезопасности (ICC) в Москве обсудят методы предотвращения ущерба от кибератак // Официальный сайт ICC. URL: https://2019.icc.moscow/ru/news/methods-for-preventing-damage-caused-by-cyberattacks-to-be-discussed-at-icc-in-moscow/ (дата обращения: 17.02.2022).

4. Бородкина Т. Н., Павлюк А. В. Киберпреступления: понятие, содержание и меры противодействия // Социально-политические науки. 2018. № 1. С. 135–137.

5. Прудковский Н. С. Обмен секретным ключом по открытому каналу связи // Современные инновации. 2017. № 1 (15). С. 44–46.

References:

1. Losses_of_organizations_from_cybercrime. // TAdviser — technology and vendor selection portal. URL: https://www.tadviser.ru/index.php/ Article: Losses_of_-organizations_from_cybercrime (access date: February 17, 2022).

2. Scammers — new name, old schemes // Financial literacy of the population. Project of the Ministry of Finance of the Stavropol Territory. URL: https://fingram26.ru/articles/riski-i-finansovaya-bezopasnost/6981/ (access date: February 17, 2022).

3. Methods for preventing damage from cyber attacks will be discussed at the International Cybersecurity Congress (ICC) in Moscow // Official website of the ICC. URL: https://2019.icc.moscow/ru/news/methods-for-preventing-damage-caused-by-cyberattacks-to-be-discussed-at-icc-in-moscow/ (access date: February 17, 2022).

4. Borodkina T. N., Pavlyuk A. V. Cybercrime: concept, content and countermeasures // Socio-political sciences. 2018. No. 1. Pp. 135–137.

5. Prudkovskiy N. S. Secret key exchange over an open communication channel // Modern innovations. 2017. No. 1 (15). Pp. 44–46.