КИБЕРАТАКИ НА БАНКОВСКИЙ СЕКТОР

С. Ю. Воробьёв, Д. А. Жук

Региональная дирекция ОАО «Белагропромбанк» по Минской области,
г. Минск, Беларусь

В. А. Русак

УО «Академия Министерства внутренних дел Республики Беларусь»,
г. Минск, Беларусь

В. А. Шкред

Загородный отдел милиции РУВД г. Борисова
УВД Минского областного исполнительного комитета,
г. Минск, Беларусь

В статье рассматривается опасность киберпреступлений в банковской сфере, приведен пример типовой таргетированной кибератаки на банковское учреждение. Выделены особенности, присущие правонарушениям, совершаемых в банковской сфере с применением информационных технологий, и условия, им способствующие. Даны рекомендации, выполнение которых позволит предотвратить значительное количество киберпреступлений.

Ключевые слова: кибератака; киберпреступность; информационные технологи; банк; киберугроза.

В эпоху стремительного развития технологий практически все сферы жизнедеятельности человека подверглись цифровой трансформации [1]. Кражи данных платежных карт (банковских счетов) или данных доступа к системе Интернет-банкинга с целью завладения средствами клиентов банка, кража персональных данных и коммерческой информации из частных компьютеров или серверов, умышленное повреждение информационных систем или средств коммуникаций с целью создания убытков компаниям – это далеко не полный перечень подобных угроз, связанных с бурным развитием информационных технологий. Все это приводит к появлению такого вида правонарушений, как киберпреступность [2].

Опасность киберпреступлений для организаций и компаний, работающих в финансовой сфере, состоит в том, что цифровые технологии развиваются крайне стремительно и злоумышленники изобретают новые способы обхода систем безопасности, к которым текущие системы защиты не готовы

[3]. Киберпреступления, как и другие виды преступлений, является работой одного или нескольких правонарушителей, как правило с колоссальными знаниями в области цифровых технологий, которые используют для достижения корыстных целей [4]. Наиболее привлекательна для преступников банковская сфера, ведь она осуществляет ежедневно огромное количество транзакций и осуществляет оборот огромного количества денежных средств. В условиях постоянного развития информационных технологий у мошенников появляются все новые и новые способы достижения своих преступных целей. С каждым днем количество таргетированных кибератак на банковские учреждения не только не сокращается, а становится все более изощренным.

Опасность для банковской сферы представляют кибератаки на платежную инфраструктуру, при которых банки несут значительные финансовые потери. Злоумышленники также атакуют системы дистанционного банковского обслуживания.

Так, банковская система Республики Беларусь по-прежнему остается в поле зрения злоумышленников и международных преступных группировок. В последние несколько лет постоянно выявлялись факты мошенничества с использованием электронных платежных средств, имели места хакерские атаки на банки Республики Беларусь, в результате которых злоумышленниками похищались значительные денежные средства. Сотрудниками правоохранительных органов на территории республики Беларусь задерживались участники международных преступных группировок Cobalt, Andromeda и др. [5].

Возможность баснословных прибылей в случае успеха и достаточно невысокий уровень риска быть обнаруженными благоприятствуют росту киберпреступлений. Злоумышленники, как хамелеоны, приспосабливаются к изменениям обстановки в сфере информационной безопасности, тщательно отслеживают появление новых уязвимостей в программном обеспечении и появление брешей в информационных системах банков и финансовых организаций.

Выбор целей киберпреступников обусловлен технической подготовкой, имеющимся в наличии инструментарием и знаниями о внутренних процессах банка [6]. При этом, как правило, основным фактором таргетированной атаки на финансовую организацию является слабая защита информационных систем.

Типовая схема таргетированной кибератаки на банковское учреждение состоит из следующих этапов:

- осуществляется массовая рассылка писем на e-mail адреса работников банка, в которых содержится вредоносное программное обеспечение;

- при открытии письма работником банка происходит процесс внедрения вредоносного программного обеспечения, после чего злоумышленник получает доступ к зараженному компьютеру;

- атакующий проводит исследование доступных с зараженного компьютера сегментов локальной сети банка и устанавливает доступ к контроллеру домена с целью получения паролей администраторов;

- после получения доступа к контроллеру домена и паролей администратора сети киберпреступник проводит в сети финансового учреждения представляющий интерес рабочих станций и серверов;

- на банкоматах устанавливается вредоносное программное обеспечение обеспечивающее выдачу финансовой наличности посредством удаленной команды. Далее после установления контроля над банкоматом к процессу подключаются соучастники, занимающиеся получением денежных средств. Их задача – непосредственное присутствие у подконтрольного банкомата в условленное время для получения денег. После успешного изъятия наличности вредоносное программное обеспечение, как правило, с банкоматов деинсталлируется [7].

Также необходимо упомянуть и такой деятельности злоумышленников, как социальная инженерия – одну из главных угроз кибербезопасности. Социальная инженерия – это методы психологической манипуляции человеком, направленные на то, чтобы заставить жертву выполнить определенные действия в пользу атакующего [8]. Необходимо помнить, что работник организации, как пользователь, является одним из звеньев информационной системы организации, так как обладает определенными привилегиями, осуществляет различные операции в процессе выполнения трудовых операций. Также необходимо отчетливо представлять, что степень защищенности информационной системы в организации измеряется защищенностью ее самого слабого звена [9]. Потенциально этим звеном как раз и может является пользователь (например, разочарованный заработной платой системный администратор или повздоривший с руководителем работник отдела кадров). Массу полезной информации для осуществления таргетированной кибератаки злоумышленник может получить из общения с сотрудниками банковской организации и из открытых источников, при этом не прибегая к помощи вредоносного программного обеспечения и иных технических средств [10]. Такую возможность предоставляют социальные сети, сайты банков, сайты закупок и т. п.

Так, представляется возможным выделить ряд особенностей, присущих правонарушениям в банковской сфере с применением информационных технологий:

- применение компьютерной техники;

- высокая латентность последних;

- умышленная, корыстная направленность последних;

- высокая степень организованности [11].

К условиям, способствующим киберпреступлениям в банковской сфере можно отнести:

- недостаточная защита от восстановления учетных данных из памяти операционной системы;

- использование словарных паролей;

- хранение чувствительных данных в открытом (незашифрованном) виде;

- внедрение операторов SQL;

- использование устаревшего (необновленного) программного обеспечения [12].

В связи с тем, что банковские и иные финансовые учреждения принимают меры для защиты своей инфраструктуры, финансов и транзакций клиентов, киберпреступники постоянно повышают свою квалификацию.

Банковскому сектору необходимо на системной основе поддерживать в надлежащем состоянии и модернизировать систему информационной безопасности, тесно и плодотворно сотрудничать с организациями, осуществляющими разработку специализированного программного обеспечения, защищающего электронные устройства от воздействия киберпреступников.

Для успешного предотвращения кибератак на банковские учреждения необходимо выполнение финансовыми учреждениями следующих мер:

- использование соответствующих аппаратных, программных и программно-аппаратных комплексов средств защиты информации;

- постоянный мониторинг событий безопасности ;

- повышение квалификации работников, отвечающих за информационную безопасность;

- обучение работников банков основам информационной безопасности;

- поддержание здорового климата в коллективе (довольный работник с меньшей долей вероятности осознанно навредит организации, в которой работает);

- информирование и обучение клиентов банков финансовой и цифровой грамотности;

- разработка пакета нормативной документации, регламентирующей сферу информационной безопасности в банке (политика безопасности, регламент управления инцидентами, формализация принципов приоритезации событий информационной безопасности, политика расследования инцидентов информационной безопасности и др.);

- блокирование подключения к беспроводным сетям на территории банка;

- создание команды по расследованию инцидентов информационной безопасности;

- скрупулезный подбор персонала в банковские организации с учетом их профессиональных, нравственных и моральных качеств;

- взаимодействие и обмен информацией о кибератаках между банками и правоохранительными органами.

Библиографические ссылки

1. Гамко, С. Л. Следственная деятельность в условиях изменения «ландшафта» киберпреступности: безопасность конфиденциальных данных и профилактика / С. Л. Гамко // Предварительное расследование. - 2019. - № 1 (5). - С. 76–79.

2. Орлов, А. Киберпреступления в банковской сфере [Электронный ресурс] / А. Орлов // Научно-практический электронный журнал Аллея Науки. - 2018. - № 11 (27). - Режим доступа:https : www.alleyscience.ru/domains_data/files/20V%20BANKOVSKOY%20SFERE.pdf. - Дата доступа : 14.03.2020.

3. Дементьева, М. А. Киберпреступления в банковской сфере Российской Федерации: способы выявления и противодействия / А. М. Дементьева, В. В. Лихачева, Т. Г. Козырев // Экономические отношения. - 2019. - Т. 9. – № 2. - С. 1009–1019.

4. «Компания Avast о типах киберугроз» [Электронный ресурс]. - Режим доступа : http://www.avast.ru/c-malware. - Дата доступа : 10.03.2020.

5. Плешкевич, В. М. О ходе реализации стратегического проекта Национального банка «Созданием системы мониторинга и противодействия компьютерным атакам в кредитно-финансовой сфере (FinCERT)» / В. М. Плешкевич // Банковский вестник. - 2019. - № 10 (663). - С. 15-16.

6. Панков, А. Атака на банки / А. Панков // Веснік сувязі. - 2018. - № 4(150). - С. 40-45.

7. Косолапов, Ю. В. Киберпреступления в сфере финансовых услуг / Ю. В. Косолапов, Е. А. Костромина, А. А. Сивова // Вопросы экономики и права. - 2018. - № 4 (118). - С. 25-29.

8. Скабцов, Н. В. Аудит безопасности информационных систем / Н. В. Скабцов. – СПб.: Питер, 2018. - 272 с.

9. Олифер, В. Компьютерные сети. Принципы, технологии, протоколы : Учебник для вузов. / В. Олифер, Н. Олифер. - 5-е изд. - СПб. : Питер, 2017. – 992 с.

10. Бирюков, А. А. Информационная безопасность: защита и нападение / А. А. Бирюков. - М. : ДМК Пресс, 2017. - 434 с.

11. Чеботарева, А. А. Компьютерная преступность в банковской сфере:основные направления уголовно-правовой политики в Российской Федера-

ции / А. А. Чеботарева // Криминологический журнал Байкальского государственного университета экономики и права. - 2014. - № 3. - С. 140–144.

12. Левшук, О. И. Киберпреступность как масштабная угроза мировому сообществу / О. И Левшук // Юстиция Беларуси. - 2020. - № 1(214). - С. 20-24.

РАЗРАБОТКА СИСТЕМЫ ПОКАЗАТЕЛЕЙ ОЦЕНКИ УРОВНЯ ИНФОРМАТИЗАЦИИ РЕГИОНА

Е. С. Высочанская

магистрант кафедры прикладной информатики в экономике,
Рыбницкий филиал ПГУ им. Т. Г. Шевченко,
г. Рыбница, Молдова (Приднестровье)

tania00803ksa@mail.ru

Л. К. Скодорова

магистрант кафедры прикладной информатики в экономике,
Рыбницкий филиал ПГУ им. Т. Г. Шевченко,
г. Рыбница, Молдова (Приднестровье)

skodorova@rambler.ru

Актуальность цифровой трансформации в секторах экономики и бизнесе, подтверждает необходимость оценки процессов цифровизации.

Ключевые слова: оценка уровня информатизации; регион; цифровая экономика.

Значительное влияние на инфраструктуру экономике оказывают цифровые технологии. В международной конкуренции эти тенденции стали ключевыми. Поэтому особую актуальность приобретает контроль и стимулирование этих процессов со стороны государства. Недостатком раннее проводимых исследований на тему *«Оценка уровня информатизации»* является ограниченность сферы исследования формальными показателями оценки. Отсутствуют сведения о попытках оценить информационную прозрачность комплексно, отталкиваясь от информации открытых источников, в то же время как в статьи 28 и 29 Конституции Приднестровской Молдавской Республики гарантируют право на получение достоверной информации о деятельности государственных органов. Из этого следует, что открытые источники информации должны