Якуба Никита Сергеевич
студент
Шандарин Даниил Михайлович
студент
Турсунмухамедов Искандер Гайратович
канд. экон. наук, доцент
Калужский филиал
ФГОБУ ВО «Финансовый университет
при Правительстве Российской Федерации»
г. Калуга, Калужская область

ХАРАКТЕР И ПОСЛЕДСТВИЯ КИБЕРПРЕСТУПНОСТИ В БАНКОВСКОЙ СФЕРЕ

Аннотация*: в работе рассматриваются все масштабы и последствия киберпреступности в банковской и финансовой сфере. Авторы раскрывают качественные особенности данного вида преступности. В процессе подготовки исследования авторы использовали учебную и учебно-методическую литературу, а также официальные ресурсы сети Internet.*

Ключевые слова*: киберпреступность, вирусные программы, фишинг, скимминг, социальная инженерия, ИКТ, хищение.*

На сегодняшний день массово внедряют во все сферы социально-экономической жизни новейшие информационно-коммуникативные технологии. Финансовая и кредитно-банковская сферы также не являются исключением из правил. Внедрение подобных технологий в эти сферы достаточно сильно меняет характер деятельности кредитных учреждений, а также организаций.

Масштабированное внедрение ИКТ в финансовую и кредитно-банковскую сферы, несомненно, способствует увеличению результативности проведения любых банковских операций, а также снижению различных всевозможных затрат на их осуществление. Но сегодня все чаще стала возникать проблема обеспече-

ния безопасности проведения подобных операций при помощи ИКТ. Сейчас проблема кибербезопасности в банковской сфере является одной из самых обсуждаемых. А дело все в том, что после образования подобных технологий новый вид мошенничества также получил распространение и получил название «киберпреступность». Особенности киберпреступности в банковской сфере:

– все совершенные преступления уникальны;

– преступления совершаются в автоматизированном режиме;

– большая степень латентности, обеспеченная механизмами шифрования и кодирования;

– дистанционность положения преступников, а также потерпевших и прочее [1, с. 70].

Данные особенности в большей степени показывают сущность киберпреступности. Что же касается ее классификаций, выделяют несколько видов подобных преступлений.

1. Первая группа:

– незаконное вмешательство в компьютерную систему;

– несанкционированный доступ и др.

2. Вторая группа:

– изменения каких-либо данных;

– блокировка каких-либо данных;

– подлог и др.

3. Третья группа:

– нарушение авторских прав.

4. Четвертая группа:

– кибертерроризм [2, с. 112].

Также выделяют конкретные виды киберпреступлений:

– применение троянских программ либо захват одноразового кода, приходящего по SMS, и дальнейшая передача его преступникам;

– скимминг – установка устройства, которое считывает данные с карты во время ее использования в банкомате;

– фишинг – копия сайта, на котором потерпевший вводит данные с карты, после чего все данные попадают в руки преступников;

– популярный на сегодня вид киберпреступлений – социальная инженерия. На телефон потерпевшего могут приходить SMS с просьбой об оказании денежной помощи [1, с. 71].

После внедрения информационно-коммуникативных технологий в банковскую сферу прежние ограбления банков, в которых людям приходилось брать оружие в руки ради наживы, брать других людей в заложники и прочее, ушли на второй план. Сначала многие были уверены, что благодаря ИКТ хищение денежных средств станет невозможным, но, к сожалению, это даже в какой-то степени упростило задачу умелым преступникам. Так, в 2017–2019 гг. в мировой банковской системе значительно увеличились хакерские атаки на банковские сервисы и услуги, оказываемые через Интернет. Потери от киберпреступлений на 2018 год составили почти 2 трлн долларов.

В 2015 году банки России и еще сотни банков по всему миру подверглись глобальной хакерской атаке. Банки России потеряли около 300 млн долларов. Группа хакеров смогла внедрить вредоносное программное обеспечение в систему банковских учреждений около 30 государств, после чего в течении 2 лет спокойно совершались хищения денежных средств на их счета в США и Китае. В 2016 году электронная информационная система SWIFT также стала очень часто подвергаться атакам хакеров, злоумышленники смогли украсть 81 млн долларов из ЦБ Бангладеша [5, с. 46].

По данным ЦБ России, общий объем хищений из-за хакерских атак на сегодняшний день составляет примерно 2 млрд рублей, хотя многие считают эти данные слишком заниженными. В начале 2017 года была задержана группа хакеров их Московской области сотрудниками МВД России. Хакеры похитили около 100 млн рублей с банковских счетов многих городов России, используя различные вирусные программы с помощью спам-рассылки для управления банковскими счетами юридических лиц.

К сожалению, киберпреступность на данный момент не ограничивается лишь обычным хищением денежных средств, объектами хищения также могут служить информационные данные о банковских клиентах. Эта информация с каждым годом приобретает товарную форму и становится объектом купли-продажи и подвергается влиянию спроса и предложения. Даже в этой сфера масштабы киберпреступности достаточно внушительны. В 2015 году была совершена хакерская атака на налоговую службу США, из ее базы было похищена информация примерно о 100 тыс. налогоплательщиков. Хакеры представились обычными налогоплательщиками и получили компенсацию в размере 50 млн долларов [2, с. 137].

В 2014 году один из самых крупнейших по активам банк США «Морган Чейз» был подвергнут масштабной хакерской атаке, по результатам которой злоумышленники получили доступ к 80 млн клиентским учетным записям и к 7 млн данных малого бизнеса.

Зачастую краденая информация может стать инструментом для вымогательства. Так, например, у копании «Apple» хакерская организация под названием «Турецкая киберпреступная семья» похитила около 560 млн учетных записей пользователей, а позже потребовала за эту информацию выкуп в размере 75 тыс. долларов.

Исходя из динамики хищений информационных данных, Россия занимает второе место после США по количеству случаев подобного рода киберпреступлений. Более 90% утечек информационных данных связано с кражей платежной информации, а также персональных данных.

Также хакерские атаки нередко используются не просто для хищения чего-либо в личных целях, а для ослабления рыночных позиций какого-либо кредитного учреждения [4, с. 24].

Полностью избавиться от киберпреступности невозможно, так как данный вид деятельности имеет высокую доходность. Так, по данным ЦБ России, до-

ходы хакеров составляют примерно около 2,5 млрд руб. Разработчики вредоносных программ только за одну такую программу получают около 50 тыс. долларов.

Исходя из этого, основная задача каждого государства заключается в том, чтобы сделать этот процесс более контролируемым. Прежде всего необходимо совершенствовать законодательство, которое будет регулировать использование ИКТ, потому что даже, например, в нашем отечественном законодательстве нет четко сформулированного определения киберпреступности, также не предусмотрена никакая ответственность за утечку информации. Хотя и действует закон о защите персональных данных, но ответственность предусмотрена лишь за несоблюдение обычных формальных требований, утечка данных не является преступлением, если не нарушены какие-либо другие законы [5, с. 45].

Также на сегодняшний день обеспечение защиты банковских электронных систем выглядит совершенно пессимистично. Это вполне легко объясняется, хакерские методы в данной сфере постоянно совершенствуются, методов обойти любую систему существует уже слишком много, поэтому даже пользователи вынуждены прилагать собственные усилия, чтобы совершенствовать систему защиты своих данных и средств.

Хакеры совсем недавно разработали метод бесконтактного хищения денежных средств из банкоматов при помощи вируса, при введении которого банкомат выдает только купюры номиналом 1000 или 5000 рублей. Исходя из этого, можно сказать, что на сегодняшний день банковская сфера все время находится в состоянии нервного напряжения и время ее существования, а также процветания уже постепенно уходит [4, с. 22].

Чтобы российский банк смог создать мощную и надежную защиту от подобных атак, ему необходимы огромные инвестиции, которыми, к сожалению, почти ни один банк не обладает. Все очевиднее становится надобность в создании какого-либо единого центра обеспечения безопасности российских банков, а также установление определенных, а главное единых стандартов подобной без-

опасности для всей финансовой и банковской системы. Также многие исследователи предлагают объединить усилия через развитие ГПЧ (государственно-частного партнерства) в сфере борьбы с киберпреступностью. Данный метод является вполне рациональным, эффективным и своевременным.

Также в системе борьбы с киберпреступлениями в Российской Федерации важную роль играет обучение населения финансовой грамотности. Финансово грамотные люди должны знать о том, что никому нельзя сообщать свои личные данные, например, пароли, номера карт, единоразовые ПИН-коды и прочее [3, с. 124].

Таким образом, исходя из всего вышесказанного, хотелось бы отметить, что киберпреступность достаточно значимая и актуальная тема на сегодняшний день. Из-за стремительного развития высоких технологий этот вид преступности с каждым годом увеличивает свои обороты, подвергая нас всех опасности. Сегодня почти все наши данные содержатся в электронном виде, и, как оказывается, заполучить и воспользоваться ими не так-то уж и сложно, ведь любую систему знающему и разбирающемуся в этом человеку можно всегда обойти. Поэтому каждый человек не должен к этому равнодушно относится, ведь на кону его личная безопасность. Все люди должны быть финансово грамотными и прилагать любые усилия для самозащиты.

Список литературы

1. Уголовный кодекс Российской Федерации. – М.: Проспект; КноРус, 2015. – 240 с.

2. Агеева Н.А. Деньги, кредит, банки: учебное пособие / Н.А. Агеева. – М.: РИОР, Инфра-М, 2018. – 160 с.

3. Андрюшин С.А. Банковские системы / С.А. Андрюшин. – М.: Альфа-М; Инфра-М, 2016. – 243 с.

4. Головлев П. Киберпреступность в банковской сфере и способы защиты / П. Головлев // Информационная безопасность. – 2012. – №5. – С. 21–27.

5. Чекунов И.Г. Современное состояние киберпреступности в России / И.Г. Чекунов, Р.Н. Шумов // Российский следователь. – 2016. – №10. – С. 44–47.