**РАЗДЕЛ II. ФИНАНСЫ, ДЕНЕЖНОЕ ОБРАЩЕНИЕ И КРЕДИТ.
СПЕЦИАЛЬНОСТЬ 08.00.10****ВНЕДРЕНИЕ КИБЕР-БЕЗОПАСНОСТИ В БАНКОВСКОЙ СИСТЕМЕ:
НОВЕЙШИЕ ПОДХОДЫ И РАЗРАБОТКИ****THE INTRODUCTION OF CYBER SECURITY IN THE BANKING SYSTEM: THE
LATEST APPROACHES AND DEVELOPMENTS****ЗИНИША О.С.,
СОКОЛОВ Д.Г.,
ЗАКАРЬЯЕВ Р.А.****ZINISHA O.S.,
SOKOLOV D.G.,
ZAKARYAEV R.A.***ФГБОУ ВО "Кубанский ГАУ имени И.Т.
Трубилина"**Kuban State Agrarian University named after
I. T. Trubilin**zinisha@rambler.ru**doi: 10.18411/emiip-03-2019-09**idsp: sciencepub-emiip-03-2019-09***АННОТАЦИЯ**

В статье авторами рассматривается проблема кибербезопасности в банковской системе, обозначается актуальность проблемы, анализируются причины кибератак и их особенности, а также предлагаются методы повышения уровня защиты банковских систем.

КЛЮЧЕВЫЕ СЛОВА: банки, банковские системы, кибербезопасность, киберзащита, киберугрозы, технологии

ABSTRACT

The article discusses the problem of cyber security in the banking system, identifies the relevance of the problem, analyzes the causes of cyber-attacks and their features, and suggests effective methods for improving the level of protection of banking systems.

KEYWORDS: banks, banking systems, cyber security, cyber defense, cyber threats, technologies

В современном информационном обществе Интернет проникает во все сферы его жизни, включая экономику и банковские системы в частности, – уже сегодня существует множество вариантов его применения. Наиболее часто Интернет в них применяется для осуществления различных операций с финансами: купля, продажа, перевод. Интернет позволяет все это сделать со своего мобильного телефона, или с другого устройства, имеющего выход в сеть, не посещая банковское отделение.

Но, как и в случае с натуральными деньгами, в сфере виртуальных финансов существуют различные способы мошенничества. Развитие научно-технического прогресса, связанное с внедрением современных информационных технологий, привело к появлению новых преступлений, таких как незаконное вмешательство в работу электронно-вычислительных сетей, машин и систем, вымогательство компьютерной информации, и др. – преступления, получившие сегодня название «киберпреступность». Рост киберпреступности сегодня набирает обороты, ничуть не уступающие «традиционной» преступности.

Киберпреступность уже вполне заслуженно можно признать одной из главных проблем XXI-го века. Под этим термином подразумевается совершение преступлений в сфере «высоких» технологий. Понятие киберпреступлений также по своей сути весьма обширно, под него сегодня подпадает очень много правонарушений.

Киберпреступление – любое незаконное действие в сфере электронных технологий, совершенное с использованием компьютерных технологий, либо же против них [1]. Специальные службы научились расследовать «классические» преступления, где результат преступных действий «на лицо» и потерпевшая сторона находилась на момент совершения деяния в одном месте с виновником. Особенностью киберпреступлений считается тот факт, что порой сложно выявить состав самого преступления, не говоря уже про поиск виновных. Можно выделить несколько особенностей подобных преступлений: максимальная скрытность деяний, трансграничность, полная невозможность составления портрета преступника, несовершенство технологий борьбы.

Сфера электронного банкинга является сегодня лидером среди технологий дистанционного банковского обслуживания. Развитие системы электронных банков коренным образом изменило процесс взаимодействия организаций кредитно-финансовой сферы с клиентами, переместив его в киберпространство.

Сегодня в электронный банкинг входят следующие элементы:

- Интернет-банкинг – управление банковскими картами и счетами через интернет при помощи веб-браузера в режиме онлайн;
- Мобильный банкинг – управление банковскими картами и счетами при помощи персонального компьютера, смартфона, планшета;
- Торговый банкинг – использование банковских карт при осуществлении платежей, эквайринг;
- Терминалы и банкоматы банковского самообслуживания [6].

Внедрение системы электронного банкинга не только является одним из главных преимуществ кредитных организаций, но и позволяет значительно сократить операционные издержки банков. Переноса свою деятельность в киберпространство, банки вовсе не освобождаются от ответственности за качество предоставления финансовых услуг и должны в полной мере осознавать, что главной целью кибератак мошенников будут являться системы электронного банкинга с целью кражи денег, как со счетов клиентов, так и самих банков. От атак на отдельные компании хакеры перешли к атакам на целые отрасли. Первым номером в их списке целей и дальше будут стоять банки, биржи и другие финансовые институты. Этот факт поднимает вопрос обеспечения необходимого уровня кибербезопасности на новый уровень.

Одной из главных отличительных особенностей киберпреступлений является то, что они происходят удаленно и не требуют непосредственного присутствия грабителей в банке. К примеру, кибермошенники находят ранее необнаруженные уязвимости во внешнем периметре банка и пользуются ими при проведении кибератак. При этом, не обязательно самому разбираться в создании программ – преступнику достаточно приобрести на одном из форумов Даркнета (от англ. DarkNet – скрытая сеть, соединения в которой устанавливаются только между «доверенными» пользователями) специализированные программы для проведения атаки, а затем организовать обналичивание похищенных денег [2]. Основными объектами кибератак сегодня чаще всего становится сетевой периметр банка: системы банковских переводов, дистанционный банкинг, инфраструктура управления банкоматами, платежные шлюзы и процессинговые системы. Доступ к именно этим системам, приносит злоумышленникам гораздо больший доход, чем, например, массовый обман клиентов банков.

В целом, банки сегодня защищены лучше других организаций. Но вся защита не может ограничиваться лишь сетевым периметром: противостоять нарушителям, которые проникли во внутреннюю сеть банка, намного сложнее. Одним из актуальных способов для этого является рассылка фишинговых писем, содержащих вредоносное программное

обеспечение. После непосредственного проникновения в сеть, мошенники могут в считанные минуты перехватить контроль над инфраструктурой банка, используя для этого любые уязвимости и программное обеспечение.

Сегодня основополагающие причины киберугроз можно разделить на несколько групп:

1. Отсутствие необходимого законодательства и единых протоколов безопасности;
2. Отсутствие корпоративной культуры в сфере кибербезопасности внутри банка;
3. Недостаточность финансирования со стороны самих банков [5].

Единые стандарты кибербезопасности, введенные США и ЕС, в большинстве случаев являются эффективными. Сегодня банки Европы и Америки, будучи обязанными проводить свои внутренние стандарты безопасности в соответствии с предъявленными требованиями, обладают достаточно действенной системой противодействия большей части угроз. В России ситуация иная: банки вынуждены обеспечивать задачи риск-менеджмента самостоятельно, что не позволяет банкам наиболее полно выстраивать защитные системы [3].

Выстраивание локальных систем безопасности, с одной стороны, является крайне затратным мероприятием, с другой же – почти всегда малоэффективным. Сегодня ситуация обстоит так, что банки, даже имея значительный объем капитала, одновременно с этим не обладают значительными доступными средствами для поддержания уровня киберзащиты на должном уровне, предпочитая распределять их на другие статьи расходов. Однако, от эффективности защиты от различных внешних угроз зависит непосредственно как лицо и репутация банка, так и его доход. Сегодня постоянно разрабатывается целый комплекс мер для предупреждения кибератак и затруднения удаленного хищения денежных средств на уровне программного обеспечения.

Аппаратное программное обеспечение систем электронных банков достаточно хорошо защищено со стороны банка, но не на стороне клиента. Легче получить доступ к личному кабинету клиента, чем взламывать современные технические средства защиты. К двум основным факторам, сдерживающим развитие дистанционного банковского обслуживания (ДБО), относится отсутствие доверия клиентов из-за растущего количества кибератак и низкий уровень финансовой грамотности, куда входит информированность о возможностях современных технологий дистанционного банковского обслуживания и способах повышения интернет-защищенности в них.

Для решения этой проблемы, можно выделить ряд советов, которые значительно повысят уровень защищенности и доверия клиентов: своевременное обновление программного обеспечения и его тестирование, проверка доступности внешних сетевых портов, переход к наиболее надежным поставщикам IT-решений, а также тестирование сотрудников [4].

Повышение уровня финансовой грамотности населения – та задача, которая должна решаться комплексно, и не только со стороны банков. Во многих странах с основами кибербезопасности детей начинают знакомить с начальных классов, а в институтах этот предмет является обязательным. Однако, уровень финансовой и компьютерной грамотности общества всегда будет уступать скорости и уровню развития технологий мошенников. Поэтому разработчики программно-аппаратного обеспечения должны ориентироваться на всех пользователей и обеспечивать им максимальную доступность к средствам защиты от киберугроз.

Таким образом, киберпреступность – качественно новый виток к сфере преступности. Преступников почти невозможно идентифицировать и определить личность, поэтому нет возможности преследовать их по закону. Приведенные выше меры хоть и достаточно действенны, но не являются исчерпывающими. Из-за относительной

новизны таких преступлений, невозможно абсолютно обезопасить себя от кибератак: всегда находятся новые уязвимости и способы обойти защиту. Защитные системы сегодня постоянно совершенствуются, однако нельзя ограничиваться только этим – нужно разрабатывать новые подходы к обеспечению безопасности. Одним из таких подходов является подход оперативности и открытости. Необходимо объединение правительства, государственных и частных банков, предприятий, специализирующимся на информационной безопасности и граждан в вопросе открытости, доступности информации об угрозах и выработанных методиках борьбы с ними, для того чтобы совместными усилиями противостоять киберпреступности. Нельзя умалчивать о провале или победе над той или иной угрозой – вся подобная информация должна быть доступна незамедлительно. Только тогда можно говорить о создании реальной угрозы для преступного мира. Они развиваются быстро, поэтому необходимо развиваться быстрее, этим и обуславливается требование делиться знаниями в борьбе с киберугрозами.

1. Гамза, В. А. Безопасность банковской деятельности: Учебник для вузов.- 3-е изд., пер. и доп. / В.А. Гамза, И.Б. Ткачук, И.М. Жилкин. – М.: Юрайт, 2017. – 513 с.
2. Кибератаки на банки: тренды, уязвимости и роль регулятора // PlusWorld.ru [Электронный ресурс]. – Режим доступа: <https://www.plusworld.ru/professionals/kiberataki-na-banki-trendy-uyazvimosti-i-rol-regulyatora/> – (дата обращения 12.12.2018)
3. Кибербезопасность (2017-2018): цифры, факты, прогнозы // PositiveTechnologies [Электронный ресурс]. – Режим доступа: <https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/cybersecurity-2017-2018-rus.pdf> – (дата обращения 12.12.2018)
4. Кибербезопасность - 2017: типичные ошибки и советы по защите // Bankir.ru [Электронный ресурс]. – Режим доступа: <https://bankir.ru/publikacii/20171226/kiberbezopasnost-2017-tipichnye-oshibki-i-sovety-po-zashchite-10009378/> – (дата обращения 12.12.2018)
5. Кибербезопасность в банковской сфере // ICF.ua [Электронный ресурс]. – Режим доступа: <https://icf.ua/blog/view/kiberbezopasnost-v-bankovskoy-sfere> – (дата обращения 12.12.2018)
6. Кибербезопасность – Типовой учебный план // Nato.int [Электронный ресурс]. – Режим доступа: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_10/20171004_1610-cybersecurity-curriculum-rus.pdf – (дата обращения 12.12.2018)