КИБЕРПРЕСТУПЛЕНИЯ В ИНДУСТРИИ ФИНАНСОВЫХ УСЛУГ

© 2018 **Косолапов Юрий Вячеславович**
кандидат химических наук, доцент кафедры таможенного права и организации таможенного дела
Юридический институт Российского университета транспорта, г. Москва
© 2018 **Костромина Елена Александровна**
кандидат филологических наук, доцент кафедры менеджмента и маркетинга
Московский университет имени С.Ю. Витте, г. Москва
© 2018 **Сивова Анна Александровна**
кандидат филологических наук
старший научный сотрудник НИЦ-2 ФКУ НИИ ФСИН России, г. Москва
E-mail: pan_kosolapov@mail.ru, ea_kostromina@mail.ru, sivovaanna@mail.ru

В статье раскрыты некоторые общие аспекты киберпреступности в индустрии финансовых услуг, дифференцированы виды и угрозы существующей системы защиты информации от киберпреступности. Теоретическое и практическое изучение данного вопроса позволило авторам выявить необходимость существенных изменений в организации международной деятельности по борьбе с киберпреступностью. Современные исследования в этой области организованной преступности, доказывают, что количество уголовных преступлений против безопасности информации растет вместе с развитием информационных технологий.

Ключевые слова: IT-сфера, киберпреступление, кибербезопасность, кибератака, киберпреступность, информационные технологии, финансовые услуги.

Глобальное распространение киберпреступности считается одной из главных угроз для национальной безопасности в XXI веке. Киберпреступления представляют огромную проблему для мирового сообщества. Поскольку Интернет является целью и проводником такой деятельности, а информационные и коммуникационные (инфокоммуникационные) правоотношения в Интернете обладают транснациональными характеристиками, борьба с киберпреступностью требует хорошо скоординированных международных усилий. Киберпреступность стала новой формой постоянной угрозы, учитывая, что кибератака может уничтожить страну без непосредственного нахождения на ее территории.

Проблемы текущих и будущих угроз, связанных с этим видом экономических преступлений, актуальны во всем мире. Государства в принципе имеют внутренний потенциал и источники по борьбе с данным видом правонарушений, но они недостаточны, чтобы противостоять кибератакам крупных размеров. Отметим, что киберпреступность — это явление, которое затрагивает различные сферы жизнедеятельности, такие как телекоммуникации, информационные технологии, криминология, финансовые технологии, экономика и правосудие. Именно поэтому киберпреступность рассматривается как сложное явление, и единственный способ противостоять ей — осуществлять решение этой проблемы через глобальный подход. На наш взгляд, необходимо международное сотрудничество между экспертами в вышеуказанных областях, чтобы избежать частных решений, частично нивелирующих проблему.

Нестабильная ситуация в сфере международных отношений, сложившаяся на современном этапе развития мирового сообщества, может привести к тяжелым и серьезным последствиям в сфере кибербезопасности. Правительства разных стран стремятся получить доступ к большим объемам информации, спецслужбы заинтересованы в получении сведений, которые могут принести пользу финансовой сфере своих стран. Такая глобальная тенденция может препятствовать инициативам по межгосударственному обмену данными.

В настоящее время наблюдается рост объема, масштаба и стоимости киберпреступлений, количество которых достигло небывалого уровня. Некоторые государства, входящие в Европейский союз, говорят о том, что случаи преступлений в сфере кибербезопасности, возможно, уже превосходят численность традиционных преступлений [3].

Кибератаки, действительно, способны оказывать большое влияние на бизнес компаний, например, приводить к ухудшению финансовых

показателей, краже интеллектуальной собственности, что в итоге приведет к потере конкурентного преимущества и т.д. Все это становится возможным из-за возможности киберпреступников получить доступ к необходимой информации.

Для бизнеса самыми критичными являются потери от кибератак на финансы компаний. По сведениям Europol, можно выделить основные тенденции киберпреступлений в финансовой сфере:

• «Преступление-в-качестве-услуги»: «подпольные цифровые услуги» подкрепляются моделью «преступление-в-качестве-услуги», которая становится все более популярной и востребованной. Она объединяет между собой специализированных поставщиков хакерских утилит и организованные преступные группировки.

• «Программы-вымогатели»: вымогательство и банковские «трояны» остаются главными угрозами среди вредоносного программного обеспечения.

• Преступное использование данных: сведения остаются ключевым товаром для киберпреступников. Во многих случаях они используются для получения немедленной финансовой выгоды, но все чаще применяются для реализации более сложных схем мошенничества, зашифровываются с целью получения выкупа, либо используются непосредственно для вымогательства.

• Платежное мошенничество: EMV (чип и PIN-код), геоблокировка и другие промышленные меры безопасности продолжают помогать в эффективной борьбе с карточным мошенничеством, но, тем не менее, растет и число атак, направленных против банкоматов. Организованные преступные группы начинают компрометировать платежи, связанные с использованием бесконтактных карт (NFC).

• Социальная инженерия: правоохранительными органами был зарегистрирован рост числа фишингатак, направленных на цели, имеющие высокую значимость. Главной угрозой стали атаки против руководящих сотрудников предприятий и организаций [5].

Начиная с 2016 года, наблюдается увеличение количества целевых атак на организации кредитно-финансовой сферы. Основной тренд последних лет — использование для компрометации информационных систем и сетей инструментов, предназначенных для проведения тестирования на проникновение. Прежде всего таких, как Metasploit Framework и основанных на Metasploit — Cobalt Strike, Armitage, Empire.

В то же время, анализируя способы совершения различных атак, можно обоснованно предполагать наличие иных преступных групп, использующих похожие инструменты.

Типовая схема целевой атаки на кредитную организацию выглядит следующим образом:

1. Производится массовая рассылка электронных писем, содержащих вредоносные вложения, на адреса организаций кредитно-финансовой сферы.

2. В случае запуска вредоносного вложения из письма на компьютере получателя, проявившего неосторожность, происходит скрытное внедрение программ, чаще всего — загрузчика.

3. После скачивания загрузчика на компьютере устанавливается компонент Beacon — основной инструмент из набора Cobalt Strike. Атакующий получает возможность удаленного доступа к зараженному компьютеру.

4. Атакующий проводит исследование доступных с зараженного компьютера сегментов сети и пытается установить доступ к контроллеру домена сети с целью последующего получения паролей администраторов. Для получения пароля могут быть использованы возможности специальных инструментов (Mimikatz и другие).

5. После получения доступа к контроллеру домена и администраторских паролей атакующий проводит поиск в сети интересующих серверов и компьютеров. Прежде всего ищется компьютер или сервер, с которого есть доступ в подсеть, где находятся банкоматы или иные сегменты сети, например в сегмент процессинга платежных карт.

6. На банкоматах устанавливается программное обеспечение, взаимодействующее, предположительно, через программный интерфейс XFS и обеспечивающее выдачу денежных средств по команде, подаваемой удаленно. После получения контроля над банкоматами к процессу привлекаются соучастники, занимающиеся получением денежных средств. Их задача — обеспечить присутствие около банкоматов в условленное время для получения денег. После успешной выдачи денежных средств программное обеспечение с банкоматов, как правило, удаляется.

7. В случае получения доступа к процессингу платежных карт привлекаются соучастники,

занимающиеся оформлением на подставных лиц платежных карт атакованной организации. Данные карты консолидируются в руках лиц, занимающихся получением денежных средств. Их задача — обеспечить снятие денежных средств в банкоматах непосредственно после того, как балансы и лимиты карт будут повышены в системе процессинга. В процессе получения денег соучастниками оператор может при необходимости продолжать поднимать лимиты по снятию или балансы карт.

8. В случае получения доступа к компьютерным средствам сегмента платежной системы Банка или системы переводов SWIFT производятся платежи на заранее подготовленные счета, с которых денежные средства далее переводятся и обналичиваются по стандартным для компьютерной преступности схемам [2].

В 2017 году отмечено большое количество атак на юридические лица — клиентов кредитных организаций, использующих бухгалтерские системы. Основная характерная особенность атак — автоматическая подмена платежных поручений на этапе их передачи из бухгалтерской системы в систему дистанционного банковского обслуживания.

Несмотря на простую схему атак, суммарный ущерб от нее превысил 200 млн. рублей [2].

Также на протяжении всего 2017 г. отмечался повышенный интерес преступников к атакам на банкоматы с использованием физического подключения к внутренним устройствам банкомата и удаленного управления диспенсером.

Делая выводы из анализа видов и природы киберпреступлений, можно говорить о том, что компьютерные системы сами по себе предоставляют новые возможности для нарушения закона путем создания неограниченного потенциала для совершения различных видов преступлений. Киберпреступность в индустрии финансовых услуг является постоянной международной угрозой и имеет возможность действовать за пределами национальных границ, таким образом, делая эту форму организованной преступности глобальной проблемой. Киберпреступники могут появляться в различных формах, в зависимости от того, как совершается преступление, а также от умысла лиц, совершивших эти преступления, в том числе в интернете. При этом основными причинами, которые способствуют совершению такого рода преступлений, являются глобализация технологий и революционное развитие информационных и коммуникационных технологий (ИКТ).

Результаты исследований компании Ernst & Young в области информационной безопасности позволили определить степень готовности компаний мирового уровня противостоять кибератакам и недостаточность инвестиций в развитие направлений по борьбе с киберпреступлениями, отсутствие планов устранения негативных последствий таких атак [9]. В опросе приняли участие 1735 компаний из разных стран и отраслей индустрии. Согласно исследованию, половина опрошенных (50%) способны, по их мнению, обнаружить тщательно подготовленные кибератаки — наибольший уровень уверенности с 2013 года — за счет инвестиций в средства обнаружения киберугроз для прогнозирования последствий атаки, а также за счет создания механизмов непрерывного мониторинга, работы операционных центров информационной безопасности (Security Operation Center, SOC) и механизмов активной защиты. Несмотря на упомянутые инвестиции, 86% респондентов признают, что их служба кибербезопасности не соответствует в полной мере потребностям организации.

Если обратиться к оценке уровня кибербезопасности России и зарубежных стран, то необходимо отметить, что российские компании сравнялись с американскими. Стратегию по кибербезопасности имеют 60% российских компаний. Таким образом, в данной сфере Россия обошла Германию (45%), Францию (51%), Италию (55%) и сравнялась с США (также 60%) [9].

По данным отчета консалтинговой компании PricewaterhouseCoopers (PwC) наиболее защищенными от кибератак странами являются Малайзия (74%), Япония (72%) и Индонезия (70%) [9]. Основное отличие российских компаний от зарубежных состоит в том, что не все из них выбирают и используют на практике международные стандарты кибербезопасности и, как следствие, отдельные аспекты защиты от киберугроз часто упускаются. В то же время за границей данные стандарты зачастую являются обязательными.

Согласно данному отчету наиболее серьезными киберугрозами в отечественных компаниях считают нарушение конфиденциальности данных (48%), нарушение нормального хода деятельности компании (47%), снижение качества продукции (27%) и создание угрозы для жизни

(21%). Большинство сотрудников опрошенных российских компаний назвали фишинговые атаки основными причинами киберинцидентов. На втором месте оказалось использование мобильных устройств — на данную проблему указали более четверти респондентов. Как отметили эксперты, больше всего средств на защиту от киберугроз тратит государственный сектор. Госструктуры в больших объемах закупают программные и аппаратные средства защиты и реализуют крупные IT-проекты. В то же время банки лидируют в данном вопросе по показателю эффективности защиты от киберинцидентов.

Однако кибератаки не только развиваются, они становятся более изощренными. В 2017 году, по данным компании по разработке программного обеспечения в области информационной безопасности и защиты информации «Symantec», 978 миллионов человек в 20 странах пострадали от киберпреступности, т.е. 44% потребителей. Среди наиболее распространенных правонарушений данного вида выделяют: заражение технических устройств вирусом или другая угроза безопасности (53%), мошенничество с дебетовыми или кредитными картами (38%), незаконное использование паролей учетной записи (34%), несанкционированный доступ или взлом электронной почты или аккаунтов в социальных сетях (34%), покупки в интернете несуществующих товаров и услуг (33%), вход в мошеннические электронную почту или использование конфиденциальной (личной/финансовой) информации в ответ на мошенническую электронную почту (32%) [9].

В результате потребители, которые стали жертвами киберпреступности, в мире потеряли $172 млрд.— в среднем по $142 каждая жертва, круглосуточно во всем мире (или почти трех полных рабочих дней) происходит ликвидация последствий данного вида правонарушений [3].

В ходе исследования, проведенного в рамках данной работы, сделаны следующие выводы: усовершенствование технологических разработок, связанных с расширением информационных технологий и автоматизацией деятельности во всех сферах жизнедеятельности, в том числе индустрии финансовых услуг, имеет, несомненно, первостепенное значение. С другой стороны, прогресс в IT-технологиях повлек за собой умышленное злоупотребление этими технологическими достижениями, создавая целый ряд проблем и рисков для отдельных лиц и групп, стран, а также для мирового общества в целом. Следовательно, глобальный характер компьютерной преступности требует улучшения сотрудничества и кодифицированых действий всех государств для эффективной борьбы с киберпреступностью.

Изучение проблемы киберпреступности в индустрии финансовых услуг, состояния готовности компаний мирового уровня противостоять кибератакам позволило сформулировать конкретные предложения по совершенствованию механизма противодействия киберугрозам:

• в целях повышения эффективности в борьбе с киберпреступностью необходима дальнейшая разработка и внесение изменений в законодательство различных стран в сфере киберправонарушений в соответствии с международным законодательством;

• предлагается увеличить число экспертов в органах безопасности и специализированных подразделениях, занимающихся киберпреступностью;

• принять меры по усилению межведомственного сотрудничества между различными структурами информационных технологий для сенсибилизации групп интересов и предотвращения риска возникновения кибератак. Сотрудничество должно быть не только на уровне национальной безопасности, но также с международными органами безопасности;

• повысить уровень осведомленности общественности о необходимости надлежащего использования ресурсов в информационных технологиях в связи с киберпреступлениями;

• создать глобальную систему безопасности информации, позволившую с учетом технических, эксплуатационных, организационных, экономических, судебных, нормативных и человеческих факторов разработать национальную и международную стратегию информационной безопасности.

Библиографический список

1. *Козаченко И.Я., Курченко В.Н., Злоченко Я.М.* Проблемы причины и причинной связи в институтах общей и особенной частей отечественного уголовного права: вопросы теории, оперативно-следственной и судебной практики. СПб., 2003. 791 с.

2. Основные типы атак в кредитно-финансовой сфере в 2017 году. Материал подготовлен Центром мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ Банка России) Главного управления безопасности и защиты информации Банка России. 2018 // URL: http://www.cbr.ru/StaticHtml/File/14435/gubzi_17.pdf (дата обращения 02.04.2018).
3. Отчет Центра безопасности «Symantec» // URL: https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en.pdf (дата обращения 08.02.2018).
4. Отчет центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере главного управления безопасности и защиты информации банка России. Настоящий отчет подготовлен Центром мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ Банка России) Главного управления безопасности и защиты информации Банка России. 2017 // URL: http://www.cbr.ru/StaticHtml/File/14435/GUBZI-4.pdf (дата обращения 02.04.2018).
5. Официальный сайт Europol // URL: https://www.europol.europa.eu/ (дата обращения 02.04.2018).
6. Прокуроры отмечают шестикратный рост количества киберпреступлений // Информационно-правовой портал «Гарант.РУ» // URL: http://www.garant.ru/news/1131347/#ixzz56JZ4rn8G (дата обращения 08.02.2018).
7. Подписан закон о запрете анонимайзеров // Информационно-правовой портал «Гарант.РУ» // URL: http://www.garant.ru/news/1125883/#ixzz56JZRlxIf (дата обращения 08.02.2018)..
8. Проблемы кибербезопасности в России и пути их решения. Информационно-правовой портал «Гарант.РУ» // URL: http://www.garant.ru/article/520694/ (дата обращения 08.02.2018).
9. TAdviser. Государство. Бизнес. IT [Электрон. ресурс] // URL: http://www.tadviser.ru/index.php/ (дата обращения 30.03.2018).

Поступила в редакцию 22..03.2018 г