УДК 336.71

БАНКОВСКИЙ БИЗНЕС В ЦИФРОВОЙ ЭКОНОМИКЕ: КИБЕРУГРОЗЫ

Н. С. КОСТКО, К. Б. ГАВРИЛОВА
Научный руководитель М. С. АЛЕКСАНДРЕНОК, канд. экон. наук, доц.
Белорусско-Российский университет
Могилев, Беларусь

Аннотация

В статье рассмотрены проблемы обеспечения защищенности банковского бизнеса и его клиентов от кибератак в условиях цифровизации мировой и национальных экономик.

Ключевые слова:

банковский бизнес, информационные технологии, ИТ-уязвимость, киберпреступность, кибератаки, защищенность систем дистанционного банковского обслуживания.

Развитие технологий в современном мире идет в ускоренном темпе. Но наряду с технологической эволюцией происходит и развитие киберпреступности, которая постоянно разрабатывает новые типы инструментов и методов, позволяющих хакерам проникать в наиболее сложные или контролируемые среды, наносить большой урон и оставаться незамеченными [1].

В банках, через которые ежедневно проходят сотни операций с использованием денежных средств, и которые широко используют информационные технологии (ИТ), растет число ИТ-уязвимостей и возможных финансовых и репутационных потерь. Основными объектами кибератак становятся системы межбанковских переводов, процессинговые системы, платежные шлюзы, дистанционный банкинг и инфраструктура управления банкоматами (АТМ).

Зачастую хакеры для проникновения в банки используют следующие виды уязвимостей: уязвимости веб-приложений, недостаточная сетевая безопасность, недостатки конфигурации серверов и недостатки управления учетными записями и паролями [2].

Наряду с дистанционным хищением денег из банковской системы свою популярность не потеряли, так называемые, физические атаки, которые подверглись некоторым модификациям, что обусловлено непрерывным развитием информационных технологий. К атакам такого рода можно отнести:

1) скимминг – установка специальных технических средств, причем не обязательно в картоприемник, для хищения данных, записанных на магнитную ленту платежной карты. PIN-код, как правило, похищается с помощью отдельного технического устройства – видеокамеры или фальшивой накладки на PIN-пад;

2) шимминг – установка в картоприемник специальных технических средств, предназначенных для хищения данных с EMV-чипа карты. Таким образом, похищается следующая информация: история платежей, информация, содержащаяся на Track 2 карты, срок действия;

3) Black Box – установка либо подключение технического устройства, взаимодействующего с компонентами банкомата (чаще всего с диспенсером) и отдающего последнему команду для выдачи денежных средств;

4) подмена процессинга – в этом случае банкомат отключается от процессинга кредитной организации и подключается к устройству, имитирующему его. Передовые устройства могут эмулировать нормальное состояние банкомата (обслуживание клиентов) для мониторинга программного обеспечения (ПО);

5) Transaction Reversal Fraud (TRF) – получение наличных денежных средств с одновременным воздействием на работу банкомата и процессингового центра, в результате чего отсутствует корректное завершение операции по выдаче наличных средств и не меняется баланс по карте (манипулирование карточным счетом) [3].

Схожее устройство банкоматов позволяет злоумышленникам использовать одно и то же вредоносное ПО в различных кампаниях по всему миру. Так, GreenDispenser, который использовали при атаках на банкоматы в Мексике, через некоторое время был обнаружен в странах Восточной Европы.

Полная статистика заражений по всему миру за ноябрь 2018 г. представлена в табл. 1 [4].

Табл. 1. Статистика заражений по миру за ноябрь 2018 г.

Страна	Процент заражений, %	Страна	Процент заражений, %
Таджикистан	47,24	Судан	32,95
Киргизия	42,94	Мьянма	32,94
Йемен	39,10	Казахстан	32,49
Узбекистан	38,01	Россия	32,15
Афганистан	37,58	Лаос	31,81
Сирия	35,18	Замбия	31,57
Беларусь	33,69	Руанда	31,33
Эфиопия	33,52		

Как уже отмечалось, одной из главных целей атак злоумышленников неизменно остается банковская отрасль. В ходе анализа защищенности систем дистанционного банковского обслуживания в Республике Беларусь в 2017 г. эксперты Positive Technologies почти в каждом втором банковском мобильном приложении находили хотя бы одну критическую уязвимость, которая позволяла бы злоумышленникам проводить мошеннические опе-

рации. Лишь 8 % исследованных мобильных банковских приложений обладали приемлемым уровнем безопасности. Наиболее распространенная проблема защищенности онлайн-банков – доступ к сведениям, составляющим банковскую тайну клиентов [5].

Анализ защищенности онлайн-банков показал в 2017 г. рост среднего количества уязвимостей на 16 % по сравнению с 2016 г. Объекты, которые подверглись кибератакам в 2017 г., изображены на рисунке 1 [6].

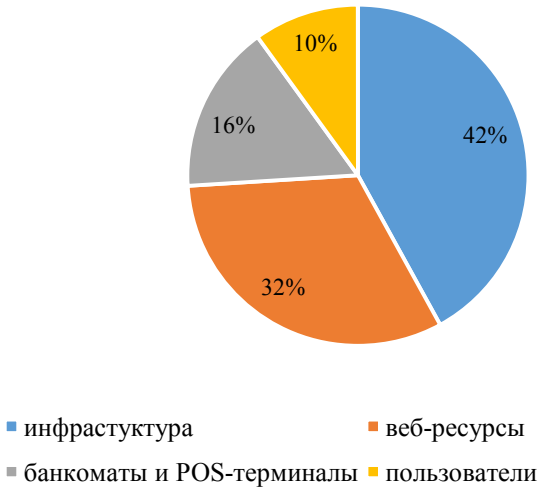

Рис. 1. Объекты кибератак

В половине атак на банки в 2017 г. было задействовано вредоносное ПО, причем существенна доля атакованных POS-терминалов и банкоматов. По сравнению с результатами 2016 г. отмечается значительный рост этой категории атак. Именно при помощи вредоносного ПО злоумышленники пытались или получить доступ непосредственно к банкоматам и управлять выдачей денег из них, или скомпрометировать внутренние ресурсы банка.

Мотивы атак изображены на рис. 2 [6].

Рис. 2. Мотивы кибератак

С целью проникновения в банковскую систему кибепреступники используют различные методы атак, которые представлены на рис. 3 [6].

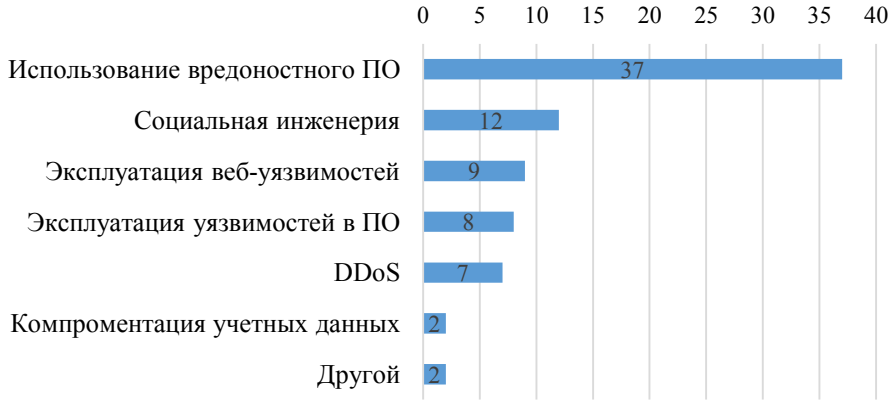

Рис. 3. Методы кибератак

Следует обратить внимание на действия группировки Cobalt. Целью этих хакеров обычно является попадание в локальную сеть банка. Как правило, для этого они используют фишинговые рассылки сотрудникам банка. Чтобы пройти спам-фильтры компании и увеличить вероятность прочтения письма, они регистрируют домены, похожие на доверенные (например, visa-pay.com, swift-alliance.com), или компрометируют инфраструктуру контрагентов и отправляют от их имени письма, содержащие вредоносные вложения. Проникнув в локальную вычислительную сеть банка (ЛВС), злоумышленники исследуют ее в поисках компьютеров сотрудников, отвечающих за работу банкоматов, загружают через них на АТМ вредоносное ПО и получают доступ к удаленному управлению банкоматами.

Сегодня в мире нет единых правил борьбы с киберугрозами, но можно выделить следующие приемы по предотвращению кибератак в банковской сфере:

– разработка международных соглашений для введения рекомендуемых и принятых норм в конструировании, управлении и использовании цифровых сетей;

– создание единой информационной платформы для обмена значимыми данными, способствующими предотвращению мошенничества и сокращению кибератак [7].

Для обеспечения кибербезопасности в Республике Беларусь создан Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (FinCERTby). Одной из основных целей его функционирования является организация информационного взаимодействия Национального банка с участниками рынка финансовых услуг (банки, небанковские кредитно-финансовые организации, компании-интеграторы, разработчики программного обеспечения, в т. ч. средств защиты информации, провайдеры и операторы связи), правоохранительными и иными государственными органами и организациями. Данное взаимодействие направлено

на обмен информацией о потенциальных компьютерных атаках в кредитно-финансовой сфере, актуальных угрозах информационной безопасности и уязвимостях программного обеспечения, используемого участниками рынка финансовых услуг.

Основными направлениями развития FinCERTby являются следующие:

– наращивание компетенций (внедрение новых сервисов и технологий, обучение, повышение квалификации работников FinCERTby и т. д.);

– автоматизация процессов (создание и внедрение автоматизированной системы обработки инцидентов);

– развитие взаимодействия (подписание соглашений со всеми странами – участницами ЕАЭС, установление связей с международными платежными структурами, объединениями команд по реагированию и другими организациями);

– образовательная деятельность (участие в мероприятиях по повышению киберграмотности, создание интернет-портала);

– совершенствование нормативной правовой базы;

– реализация контрольных функций [8].

Стоит также упомянуть, что Республика Беларусь заключила соглашения о взаимодействии с Центральным банком России и Национальным банком Казахстана, что позволит работать более эффективно в области кибербезопасности.

В заключение можно отметить, что киберпреступность в банковской сфере является серьезной проблемой для всех стран мира. В связи с этим все экономическое сообщество должно объединить свои усилия для разработки более совершенных систем защиты от кибератак, что позволит снизить потери от действий злоумышленников.

СПИСОК ЛИТЕРАТУРЫ

1. Кибератаки в банковском секторе – подход к обеспечению безопасности ИТ-инфраструктур коммерческих банков [Электронный ресурс]. – Режим доступа: https://modern-j.ru/domains_data/files/30/TUMERKIN%20I.Sh.%201%20(SOVREMENNAYa%20NAUKA).pdf. – Дата доступа: 23.11.2018.

2. Кибератаки на банки: тренды, уязвимости и роль регулятора // Журнал плас [Электронный ресурс]. – Режим доступа: https://www.plusworld.ru/professionals/kiberataki-na-banki-trendy-uyazvimosti-i-rol-regulyatora. – Дата доступа: 23.11.2018.

3. Киберугрозы и способы защиты финансовой безопасности 2017 г. // Индустриальные новости [Электронный ресурс]. – Режим доступа: https://ria-in.ru/it-industriya/kiberugrozy-i-sposoby-zashchity-finansovoj-bezopasnosti-2017. – Дата доступа: 23.11.2018.

4. Интерактивная карта киберугроз // Лаборатория Касперского [Электронный ресурс]. – Режим доступа: https://cybermap.kaspersky.com/ru/stats#country=39&type=oas&period=m. – Дата доступа: 29.11.2018.

5. Статистика о кибератаках, киберугрозах, уязвимостях ICO // Новости безопасности Беларуси и СНГ [Электронный ресурс]. – Режим доступа: https://aercom.by/statistika-o-kiberatakax-kiberugrozax-uyazvimostyax-ico-i-blokchejn-ot-positive-technologies/. – Дата доступа: 29.11.2018.

6. Актуальные киберугрозы – 2017. Тренды и прогнозы [Электронный ресурс]. – Режим доступа: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-threatscape-2017-rus.pdf.– Дата доступа: 29.11.2018.

7. Как отразить глобальные киберугрозы // Независимая газета [Электронный ресурс]. – Режим доступа: http://www.ng.ru/economics/2018-06-26/4_7253_sberb.html. – Дата доступа: 27.11.2018.

8. **Плешкевич, В. М.** О ходе реализации стратегического проекта Национального банка «Создание системы мониторинга и противодействия компьютерным атакам в кредитно-финансовой сфере (FinCERT)» / В. М. Плешкевич // Банковский вестник. – 2018. – № 10/663. – С. 15–16.