УДК 336.77: 332.2

БАНКОВСКИЕ ЭЛЕКТРОННЫЕ УСЛУГИ В УКРАИНЕ: ПРОТИВОДЕЙСТВИЕ МОШЕННИЧЕСТВУ

Шевчук Татьяна Витальевна, к.э.н., доцент,
Львовский институт ГВУЗ «Университет банковского дела»
Shevchuk Tetyana, PhD, Higher State Education Institution «Banking University»,
shev_tana@ukr.net

Аннотация. Рассмотрены значение безопасности и необходимость защиты информации при дистанционном банковском обслуживании. Проведен анализ основных видов киберпреступности в банковской системе. Предложены меры безопасности систем дистанционного обслуживания.

Ключевые слова: дистанционное банковское обслуживание, мобильный банкинг, интернет–банкинг, киберпреступность.

Развитие информационных и телекоммуникационных технологий привело к тому, что современное общество в огромной степени зависит от управления различными процессами с помощью компьютерной техники путем электронной обработки, хранения и передачи информации. А это, в свою очередь, способствовало появлению новых видов преступлений, связанных, в частности, с незаконным вмешательством в работу систем и компьютерных сетей, похищением и несанкционированным изменением данных, присвоением средств.

Применение новых информационных и телекоммуникационных технологий в банковской системе Украины позволяет осуществить комплексную автоматизацию деятельности банковских учреждений, сократить время выполнения расчетных операций, расши-

рять ассортимент банковских услуг и повышать их качество, предлагать клиентам различные механизмы дистанционного банковского обслуживания (ДБО).

Статья посвященная вопросам безопасности и кибербезопасности, которые были и остаются всегда очень актуальны в различных сферах человеческой деятельности во всем мире. Украина – не исключение, поскольку вредоносные программы, введенные в сети государственных и коммерческих структур, банков, конкурирующих фирм и различных субъектов с каждым годом наносят все больший вред. В контексте наших рассуждений привлекают внимание работы ряда ученых. В частности, исследованием способов совершения преступлений против банковской системы занимались: Х. Засадна, А. Клочко, А. Бабенко, В. Степаненко, А. Поспелов и другие.

За последние годы система ДБО превратилась из вспомогательного в основной инструмент предоставления услуг. К такому результату привели некоторые факторы, в частности: общее распространение онлайн технологий, предоставляющих пользователям максимальную мобильность и удобство; предоставление всех доступных операций «в сеть», что позволяет существенно снизить затраты на обслуживание клиентов в отделениях банка. Положительный как для клиента, так и для банка результат закономерно способствовал тому, что дистанционное обслуживание сегодня у банков в приоритете.

Однако, наряду с преимуществами, которые предоставляют новые технологии, появляются новые риски и угрозы. Поэтому, учитывая стремительное развитие высокотехнологичных банковских продуктов нового поколения, банкам необходимо обращать особое внимание на обеспечение информационно–технологической безопасности при предоставлении услуг клиентам, в частности, по переводу средств с помощью систем дистанционного обслуживания.

Чем популярнее системы, обеспечивающие клиенту удаленный доступ в банк – тем большее внимание уделяют этим системам мошенники путем распространение компьютерных вирусов, мошенничества с пластиковыми платежными карточками, кражи средств с банковских счетов, похищение компьютерной информации и нарушение правил эксплуатации автоматизированных электронно вычислительных систем. Особенно это касается мобильного банкинга и интернет–банкинга. Убытки от несанкционированного доступа при использовании ДБО официально никто не подсчитывал, банки с неохотой делятся информацией об этих конфликтах. По данным НБУ, в 2012 году количество противоправных операций по платежными карточками украинских банков выросла до 7,6 тыс. по сравнению с 2,9 тыс. годом ранее. Объем неправомерно списанных средств увеличился почти в полтора раза – с 6,3 млн до 9,1 млн грн. И это только официальная статистика, к тому же за 2012 год [2, с.84].

Проблема компьютерной преступности привлекла внимание криминалистов ведущих зарубежных стран с момента широкого внедрения компьютерной техники, вызвало ряд негативных последствий и обострило ситуацию с защитой информации, содержащейся в базах данных компьютеров и компьютерных систем.

Согласно оценкам Комиссии по внутренним делам Палаты общин парламента Великобритании, потери мировой экономики от преступлений, совершенных с помощью Интернета, достигли суммы в 388 млрд долл. в год. Ежедневно системы информационной безопасности по всему миру отражают около 247 000 атак. В среднем каждый успешный взлом дает хакерам доступ к личным данным 604 интернет–пользователей. По данным американского телеком–оператора Verizon, 75% хакерских атак осуществляются с целью обогащения. Среди громких атак в мире на финансовые структуры за последние годы можно считать взлом сайтов MasterCard, Visa и Paypal группой Anonymous, когда те отказались принимать платежи для сайта WikiLeaks. Убытки от атаки составили 5,5 млн. долл. Для противостояния кибермошенникам в разных странах создаются спецподразделения. Их полномочия постоянно расширяют, а технические возможности усиливают [3].

Что касается Украины, то с ростом объемов безналичных расчетов растет и количество пострадавших от кибермошенников. По данным МВД Украины в 2012 г. правоохранительными органами установлено 139 фактов вмешательства в работу систем дистанционного банковского обслуживания с целью кражи средств. В результате этих операций со счетов юридических лиц–клиентов банков списано 116 млн грн. Динамика свидетель-

ствует о росте таких преступлений, поскольку в 2013 году зафиксировано 270 попыток несанкционированного списания средств со счетов клиентов на сумма 108 млн грн. и 115 тыс. долл. Правоохранительные органы Украины обнаружили в 2013 более 100 скиммеров (приспособлений, которые считывают информацию с карт); в 2011 г. таких скиммеров было выявлено 45, в 2012 – 73 [5].

По состоянию на 10 января 2014 в межбанковском «черном» списке получателей несанкционированных платежей находился 591 контрагент, данные о которых используются в локальных стоп–листах банков. Благодаря этому списку банки имеют возможность не только останавливать отправку несанкционированных платежей в пользу этих получателей и задерживать зачисления их входных платежей, но и отслеживать открытие такими контрагентами новых счетов и предупреждать получения ими новых несанкционированных платежей [4].

Дистанционное обслуживание через Интернет в настоящее время наиболее перспективно и эффективно для клиентов, как юридических, так и физических лиц. Ведь ДБО доступен почти всем и стоимость его использования очень низкая. Использование Интернет является главным источником угроз для систем ДБО, что обусловлено невозможностью осуществления контроля этой сети со стороны банков. Основными способами киберпреступности в банковской сфере являются [1, с. 289] :

• сетевые атаки через Интернет, ориентированные на финансовые мошенничества и несанкционированный доступ к конфиденциальной информации;

• фишинговые атаки – один из самых распространенных в мире видов киберпреступлений, с помощью которого чаще всего похищают аккаунты и банковскую информацию;

• блокирование дистанционного выполнения банковских операций;

• скимминг – вид киберугроз, который не имеет отношения к программам, или Интернета. Речь идет о краже данных с кредитных карточек через скимминговое устройство, которое устанавливается на банкомате;

• вирусное заражение компьютерных систем.

Эксперты отмечают тревожную тенденцию, а именно, за последние годы киберпреступность стала более организованной и начала иметь форму бизнеса. Банкиры обратили внимание, что киберпреступники немного ослабили интерес к карточному сектору и переключились на онлайн–системы ДБО, в частности системы клиент–банк.

Дополнительно банкиры обеспокоены тем, что в 2013 г. зафиксированы случаи массового применения против банков (одновременно 10 и более банков) распределенных кибератак на внешние сервисы типа «отказ в обслуживании» (DDoSатаки). По данным Лаборатории Касперского, 12% от всех атак приходится на Украину. Она вошла в тройку лидеров по DDoS–атакам.

Сегодня типичная цель DDoS–атаки – скрыть попытку хищения средств с sиспользованием ДБО. В результате атаки банковский сервер становится недоступен, что делает невозможным своевременное выявление клиентом факта хищения. DDoS–атака может привести к недоступности Интернет–каналов для связи с филиалами и банкоматами.

Отдельного внимания заслуживают клиенты мобильных средств, которые активно внедряются в последнее время. Украина присоединилась к глобальной образовательной кампании по борьбе с мошенничеством с использованием вредоносного программного обеспечения (ПО) на мобильных устройствах. Благодаря специально разработанным информационным материалам украинцы смогут узнать о мерах безопасности для защиты от мошенников, действующих через мобильные устройства и разработки. Инициативу традиционно взял на себя Европейский центр по борьбе с киберпреступностью Европола. В Украине кампанию поддержала Украинская межбанковская ассоциация членов платежных систем ЕМА в рамках реализации Национальной программы содействия безопасности электронных платежей и карточных расчетов Safe Card.

Регуляторов в области информационной безопасности в нашей стране три: Национальный банк Украини, Управления по борьбе с киберпреступностью МВД Украины, Служба безопасности Украини.

Вместе с регуляторами рынка Украинская межбанковская ассоциация членов платежных систем ЕМА (создана в 1999 году) формирует законодательную и нормативную ос-

нову работы платежного рынка. В течение 15 лет создано и администрируется единственная в Украине межотраслевая онлайн–система обмена информацией о платежных и кредитных кибершайхраствах, налажено сотрудничество с правоохранительными органами. С 1 октября 2016 по 30 сентября 2017 Ассоциация ЕМА является координатором Национальной программы содействия безопасности электронных платежей и карточных расчетов Safe Card. Программа предусматривает комплекс мероприятий Ассоциации ЕМА, медиа, участников платежного рынка и государственных органов по таким направлениям противодействия: повышение осведомленности граждан Украины об эффективных способах защиты собственной информации и правила безопасного использования платежных карточек, электронных платежей и банкоматов; совершенствование уголовного законодательства Украины в сфере неправомерного обращения средств платежа и приведение его в соответствие мировым стандартам с учетом актуальных видов карточных и платежных преступлений; совершенствование системы оперативного получения и проверки правоохранительными органами информации о преступлениях с платежными карточками, электронными платежами и в банкоматах; совершенствование взаимодействия между банками, патрульной полицией, киберполиции при расследовании и противодействии преступлениям с электронными платежами.

Также Национальное антикоррупционное бюро Украины (НАБУ) инициирует создание единой информационной базы данных банков с целью обмена антимошеннической информацией, хранителем и держателем которой планируется сделать НБУ так как именно регулятор реализует государственную политику по обеспечению информационной безопасности банков. Основными принципами работы базы являются: доступ всех банков к информации; обезличенность информации в системе; сотрудничество НБУ с МВД и другими государственными структурами в сфере эффективных превентивных мер; защита информации на государственном уровне.

С целью обеспечения кибербезопасности в различных сферах деятельности государством разработан ряд документов. Основными документами по информационной безопасности банка являются Закон Украины «О внесении изменений в Закон Украины "Об основах национальной безопасности Украины»» (от 18.09.2012 г. № 5286–VI); Письмо НБУ Об усилении защиты информации при осуществлении перевода средств от 24.12.2013 № 25–111 / 29563; Проект специального (базового) Закона "Об основных принципах обеспечения кибербезопасности Украины". Таким образом, для нормального функционирования банковской Интернет–системы должны быть созданы и введены в действие законы и подзаконные акты, регламентирующие правила работы с системой и информацией, которая обрабатывается, накапливается и хранится в системе.

По нашему мнению, сотрудничество банков с клиентами по вопросам защиты информации относительно перевода средств на всех этапах ее формирования, обработки, передачи и хранения, своевременное информирование клиентов о новых средствах защиты информации, проведение соответствующих организационных мероприятий и т.д. позволят минимизировать риски несанкционированного доступа к счетам клиентов и обеспечат надлежащий уровень безопасности при осуществлении перевода средств с помощью систем дистанционного обслуживания.

Список использованных источников:

1. Засадная Х. Е. Услуги мобильного банкинга и их защита [Текст] // Вестник Университета банковского дела НБУ (г. Киев). – № 3 (18). – 2013. – С.288–291.

2. Клочко В. М. Мошенничество с использованием банковских платежных карточек [Текст] / В. Клочко // Юридический научный електронный журнал. – 2016. – № 1. – С. 82–86.

3. Киберпреступность: Украинские банки на линии удара [Електронный ресурс] / – Режим доступа: https://www.ukrinform.ua/rubric–presshall/1581644–anons_1886393.html

4. Осторожно – кибермошенники! [Електронный ресурс] / – Режим доступа: http://anticyber.com.ua/article_detail.php?id=196

5. Платежи, карточки и инновационные технологии 2014 [Електронный ресурс] / – Режим доступа: http://ema.com.ua/wp–content/uploads/2013/10/ema_infosecurity_report_conference_announce_15_10_2013.pdf