ЛИТЕРАТУРА

1. Компания Cisco [Электронный ресурс]. – Режим доступа: http://www. cisco. com/web/RU/ news/releases/ txt/2012/060112a. html
2. Vistum a wireless network scanner for vista [Электронный ресурс]. – Режим доступа: http://www. vistumbler. net/
3. ACM Siggcomm Citywide Mobile Internet Access Using Dense Urban WiFi Coverage [Электронный ресурс]. – Режим доступа: http://conferences. sigcomm. org/co-next/2012/eproceedings /urbane/p31. pdf
4. Telecom daily новости IT и телекоммуникаций [Электронный ресурс]. – Режим доступа: http://www. tdaily. ru/news/all/103/27360
5. Проект национальная деловая сеть [Электронный ресурс]. – Режим доступа: http://i-business. ru/ blogs/24791

Л. Гура,
студентка 5 курса факультета
Компьютерных наук и инновационных технологий,
Международный гуманитарный университет

БЕЗОПАСНОСТЬ БАНКОВСКИХ ИНФОРМАЦИОННЫХ СИСТЕМ

Сегодня невозможно представить функционирование банковских учреждений без использования современных информационных технологий и, в частности глобальных компьютерных сетей, в том числе и Internet. Это объясняется тем, что онлайновые банковские услуги позволяют проводить финансовые операции без посредников, что приводит к снижению комиссионных и ускорение оборота финансовых активов. Финансовые институты стремятся снизить огромные затраты по содержанию своих филиалов и отделений, а также расходы по обязательным платежным перечислениям, одновременно они пытаются повысить и прибыль отдельных кредитных учреждений. Если в 1997 году только 5 % финансовых учреждений предоставляли доступ через Internet, то в 1998 их было 18 %, а в 2010 – 65 %. В Европе 75 % банков предоставляют услуги в онлайн режиме. По оценкам компании Garther объемы коммерческих трансакций в Европе возрастут за ближайшие четыре года с $53 млрд. до $1 200 млрд. Огромное многообразие электронных банковских продуктов и услуг касается, в первую очередь, такой важной сферы, как национальный и международный платежный оборот. Система электронных расчетов сводит к минимуму банковские операции (расчеты, платежные поручения, информационное обеспечение) по обслуживанию клиентов в кассах. Наряду с этим все шире используются банкоматы, с помощью которых клиентам выдается не только наличные, но и предоставляется возможность положить средства на счет, сделать операции по сберегательной книжке клиента и т. д., то есть система расчетов наличными изменяется системой безналичных расчетов и платежей.

В настоящее время сеть Internet уже является информационной системой для оперативного осуществления банковских операций. Вместе с тем открытость сети для платежей и использования ее как канала сбыта вызывает у пользователей разного рода сомнения относительно безопасности. Ежедневно в мире $2000 млрд. пересчитываются с использованием электронных средств связи. По данным Бюро технологической оценки США 0,05–0,1 % всех переводов относятся к отмыванию «грязных» денег. Годовые убытки от мошеннических действий с пластиковыми картами составляют менее половины одного процента от общего денежного оборота – примерно $1,3 миллиарда. Хотя убытки составляют и небольшой процент от общего объема, но сама сумма является впечатляющей. Постоянное увеличение этой цифры свидетельствует о существовании уголовной подпольной индустрии, связанной с незаконным использованием пластиковых

карт. В исследовании, опубликованном американской фирмой Clear Commerce, Украина называется очагом кибермошенничества – здесь происходит большинство мошеннических операций с кредитными карточками. Выводы исследования свидетельствуют, что 20 % всех заказов, которые поступают из Украины, являются мошенническими – «заказчики» используют украденную информацию с кредитных карточек

Итак, одновременно с расширением сети пользователей банковских учреждений и упрощением процедуры доступа к ним увеличивается количество угроз к компьютерным системам, так и к финансовым организациям в целом. Распространение так называемой компьютерной преступности в банковско-кредитной сфере объясняется очень просто – ведь именно в данной сфере находятся огромные финансовые средства, которые в первую очередь интересуют преступников.

Сразу следует отметить, что правоохранительным органам становятся известны далеко не все случаи похищения денег путем использования банковских компьютерных систем. Это можно объяснить несколькими обстоятельствами. Среди них и нежелание руководства организаций предоставлять соответствующую информацию из-за опасения «компрометации» финансовых учреждений и возможности выявления дополнительных правонарушений при проведении следственных действий. Например, в одном из коммерческих банков ведущий бухгалтер отдела валютных операций провела на счета своих знакомых $123 тыс. Сотрудники банка долгое время не сообщали правоохранительным органам в надежде «разобраться своими силами», но в конце концов были вынуждены это сделать когда ситуация вышла из-под контроля [1].

К сожалению, значительную часть среди субъектов несанкционирован-ного доступа к компьютерным банковским системам составляет персонал, который хорошо знаком с технологией обработки информации. Объясняется это также тем, что с точки зрения психологических особенностей, персонал – явление сложное, каждый из сотрудников всегда индивидуален, трудно предсказуем и мотивации его поведения часто противоречивы. К числу правонарушителей иногда попадают и лица, которые сами должны отвечать за информационную безопасность в учреждении. Так старший инженер-программист Симферопольского отделения банка «Украина» на протяжении трех лет совершал хищение средств на значительную сумму. На него возлагалась обязанность по учету изготовленных, выданных, испорченных и таких, принадлежавших уничтожению магнитных карт. Поэтому он вполне владел информацией о принципе работы автоматизированной системы, имел широкий круг полномочий по сопровождению и обслуживанию. Кроме того, он был сотрудником финансовой безопасности банка, ведь владел информацией о движении средств физических и юридических лиц.

Кстати, в отделении банка в конце каждого операционного дня сводился баланс, неоднократно проходили ревизии, но хищения не оказывалось. Расследуя уголовное дело, специалисты особое внимание уделили поиску в памяти компьютера данных, свидетельствующих об использовании счетов вкладчиков. Как позже рассказал правонарушитель, он хотел, используя инфляцию гривны, вернуть похищенные деньги позже. Но в период трех лет инфляция была незначительной, и возместить похищенные суммы ему оказалось не по «карману». Под давлением неопровержимых доказательств, инжннер-программист признал свою вину и был осужден судом по ряду статей Уголовного кодекса Украины с наложением значительного штрафа и возмещением причиненного ущерба. Приговор вступил в законную силу [2].

Широко известным стало так называемое «винницкое» дело. Организованная преступная группировка (ОПГ) произвела кражу государственных средств из Винницкого

ОУ НБУ Украины в сумме 80,4 млн. грн. Один из членов ОПГ, работая в должности техника сектора обработки задач региональной расчетной палаты центра информатизации и платежных систем областного управления НБУ, используя свое служебное положение, периодически делал несанкционированный доступ в локальную сеть. Ему удалось скопировать цифровые подписи платежных документов. Одновременно, используя доступ со своего рабочего места до расчетных счетов банка путем визуального просмотра на мониторе компьютера, преступник установил, что на специальном счете Винницкого ОУ НБУ находится крупная сумма денег. Воспользовавшись полученной информацией, техник сформировал 9 пачек платежных документов, подписав их с помощью ранее скопированной электронной цифровой подписи и направил в систему электронных платежей, незаконно переведя сумму со специального счета. Далее деньги были переведены по 15 платежным поручениям на различные коммерческие структуры. В результате проведения соответствующих мероприятий, деньги были возвращены государству.

Крупный международный резонанс получило дело жителя Санкт-Петербурга В. Левина, который в начале 1994 года приобрел за смешную сумму в 100 долларов у профессионального хакера информацию, как проникнуть в одно из подразделений Internet, получив при этом определенные права и привилегии. Хакер, который продал информацию, не ставил своей целью грабить банки – благодаря незаконно приобретенным привилегиям он пользовался коммерческими службами сети Internet таким образом, что счет за услуги выставлялись другому абоненту.

В июле 1994 года он вместе со своим напарником – одним из совладельцев фирмы «Сатурн» – впервые проник в компьютерный центр Ситибанка и перевел с него деньги в калифорнийское отделение Bank of America на счета своих друзей. Левин пошел дальше своего «учителя» – он проник в компьютерную систему Ситибанк и начал спокойно воровать деньги.

В августе 1994 года Владимир Левин в очередной раз обошел сложную систему защиты банковской сети Ситибанка и перевел 2,78 млн. долларов на счета нескольких компаний в Израиле и Калифорнии. Как утверждают руководители Ситибанка, ему удалось похитить лишь 400 тыс. долларов, поскольку сработала защита и счета оказались заблокированными. Сразу после инцидента служба безопасности Ситибанка совместно с правоохранительными органами начали работу по выявлению нарушителя. Однако в течение полугода американские спецслужбы (в том числе ФБР) не могли его допросить – арестовать Левина было возможно лишь за пределами России. Специалисты американских спецслужб обманывали Левина, позволяя ему перебрасывать несуществующие деньги со счетов Ситибанка (на жаргоне хакеров такая операция называется «Дамми»).

В своем интервью San Francisco Chronicle агент ФБР Стивен Гарфинк заявил, что В. Левин совершил более 40 сделок на общую сумму $10 млн. Надо отметить, что $2,78 млн. – это средства, которые реально были переведены из Ситибанка [3].

Только приведенные примеры указывают, что защита информации в банковских учреждениях требует должного внимания и постоянного совершенствования. Как известно, она включает три основные составляющие: правовую, организационную и техническую защиту информации.

На протяжении последнего времени был принят ряд нормативно-правовых актов, в том числе и международных, которые непосредственно касаются защиты информации.

Прежде всего, следует упомянуть новый Уголовный кодекс Украины, который вступил в силу в сентябре 2001 года, где компьютерным преступлениям посвящен раз-

дел XVI «Преступления в сфере использования электронно-вычислительных машин (компьютеров), систем и компьютерных сетей», состоящий из:

• ст. 361. Незаконное вмешательство в работу электронно-вычислительных машин (компьютеров), систем и компьютерных сетей;

• ст. 362. Использование, присвоение, вымогательство компьютерной информации или завладение ею путем мошенничества или злоупотребления служебным положением;

• ст. 363. Нарушение правил эксплуатации автоматизированных электронно-вычислительных систем.

Важным событием в борьбе с транснациональными компьютерными преступлениями стало подписание нашим государством, вместе с 30 другими странами, 23 ноября 2001 года Европейской конвенции о киберпреступности, в которой достаточно четко определены виды компьютерной преступности и пути взаимодействия правительств по борьбе с ней.

6 декабря 2001 Президент Украины подписал Указ № 1193/2001, который предусматривает внесение изменений в законодательство, регулирующее вопросы борьбы с киберпреступлениями.

С целью организации противодействия «компьютерного терроризма», в том числе и распространения через глобальные и национальные сети, связи идеологии терроризма, пропаганды насилия, войны и геноцида, Постановлением Кабинета Министров Украины от 14 декабря 2001 г. № 1694 запланировано разработать с учетом рекомендаций Парламентской ассамблеи Совета Европы по борьбе с терроризмом проекты Законов Украины «О мониторинге телекоммуникаций», «О защите информации в сетях передачи данных», «О регулировании украинского сегмента сети Интернет» [4].

По организационному аспекту противодействия компьютерным преступлениям, следует отметить создание в 2001 году Управления по борьбе с преступлениями в сфере высоких технологий при МВД Украины. За время функционирования, подразделением возбуждено 40 уголовных дел (для сравнения к созданию такого подразделения в 2000 году было возбуждено 7 уголовных дел по ст. 198-1 Уголовного кодекса Украины, который действовал раньше).

Неотложной задачей на сегодня является создание Межведомственного центра по борьбе с компьютерными преступлениями, что предусмотрено Указом Президента Украины О решении Совета национальной безопасности и обороны Украины от 31 октября 2001 года «О мерах по совершенствованию государственной информационной политики и обеспечению информационной безопасности Украины». На базе МЦБКЗ следует организовать контактный пункт для получения сообщений о киберпреступлениях и оперативной помощи жертвам, лабораторию для проведения компьютерных экспертиз. Центр может стать местом для организации семинаров, практикумов в системе подготовки специалистов по защите информации. Если сегодня на создание и функционирование МЦБКЗ не выделить достаточных финансово-материальных ресурсов – завтра потери экономики государства от компьютерной преступности будут намного больше.

По технической защите информации, то одним из перспективных направлений здесь является использование криптографических систем, развитие которых предусмотрено Указом Президента № 1193 от 6 декабря 2001 года. Однако на пути использования отечественных разработок существует несколько препятствий. Во-первых, это отсутствие Закона об электронно-цифровой подписи, что ставит под сомнение законность использования таких систем. Во-вторых, – лицензирование работы по разработ-

ке криптосистем и проведение их сертификации требует значительных средств, что не может не отметиться на стоимости конечного продукта и под силу далеко не всем организациям. А потому, по-моему мнению, нужна соответствующая программа для поддержки отечественных разработок, предоставления грантов и т. д.

Комплексное решение указанных проблем позволит получить преимущества, которые предоставляет электронный банкинг при высоком уровне безопасности банковских информационных систем.

ЛИТЕРАТУРА

1. Пособие для следователя. Расследование преступлений повышенной общественной опасности [под ред. Н. А. Селиванова]. – М. : Лига Разум. – 1999. – С. 420.

2. Курило Н. Віртуальний злочинець? Розкритий і знешкоджений! / Н. Курило // Крок. – 2001. – № 19.

3. Комп'ютерна злочинність : навчальний посібник. – Київ : Атік. – С. 89.

4. Про затвердження Програми реалізації положень Варшавської конференції щодо спільної боротьби проти тероризму : Постанова КМ України від 14 грудня 2001 р. № 1694.

5. Зубок М. І. Безпека банківської діяльності : навч. посіб. / М. І. Зубок. – К. : КНЕУ, 2002. – 190 с.

6. Протидія злочинам, які вчиняються з використанням комп'ютерних мереж : тези доповідей Міжнародної науково-практичної конференції (м. Севастополь, 1–2 жовтня 2010 року) / Державний вищий навчальний заклад «Українська академія банківської справи НБУ». – Суми : ДВНЗ «УАБС НБУ», 2010.

Е. Матович,
студент 5 курса факультета
Компьютерных наук и инновационных технологий,
Международный гуманитарный университет;
руководитель – д-р. техн. наук, проф. С. А. Михайлов

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ И ДОСТОВЕРНОСТИ ПЕРЕДАЧИ ИНФОРМАЦИИ В СИСТЕМАХ РАДИОДОСТУПА В СТАНДАРТЕ WiMax

Ввиду растущей интеграции телекоммуникаций и компьютерной техники, на сегодня в номенклатуре средств абонентского доступа главное место занимают технологии широкополосного радиодоступа. Новейшие технологии широкополосного радиодоступа призваны решать целый комплекс заданий из обеспечения персонализации, мобильности и мультимедийности средств связи.

Wireless Fidelity (WiFi) – технология на базе стандарта IEEE 802.11b и IEEE 802.11a, работающая в режимах – «клиент-сервер» и «точка-точка». С целью сдерживания неконтролируемого роста промышленного рынка средств широкополосного радиодоступа, уменьшения расходов, разработки эффективных механизмов взаимодействия разных радиотехнологий, упрощения развертывания сетей и расширения ассортимента услуг, были разработаны и другие модификации стандарта IEEE 802.11.

Комплекс общетехнических подходов относительно последующего повышения показателей спектральной эффективности и пропускной способности радиотехнологии WiFi 802.11b с ортогональным частотным разделением каналов (OFDM) характеризуется многими составляющими, среди которых главное место занимают методы множественных антенн (MIMO). Благодаря эффективным решениям техника MIMO обладает рядом преимуществ перед аналогичными методами повышения спектральной эффективности радиотехнологии и достоверности передачи данных. Ожидается, что в