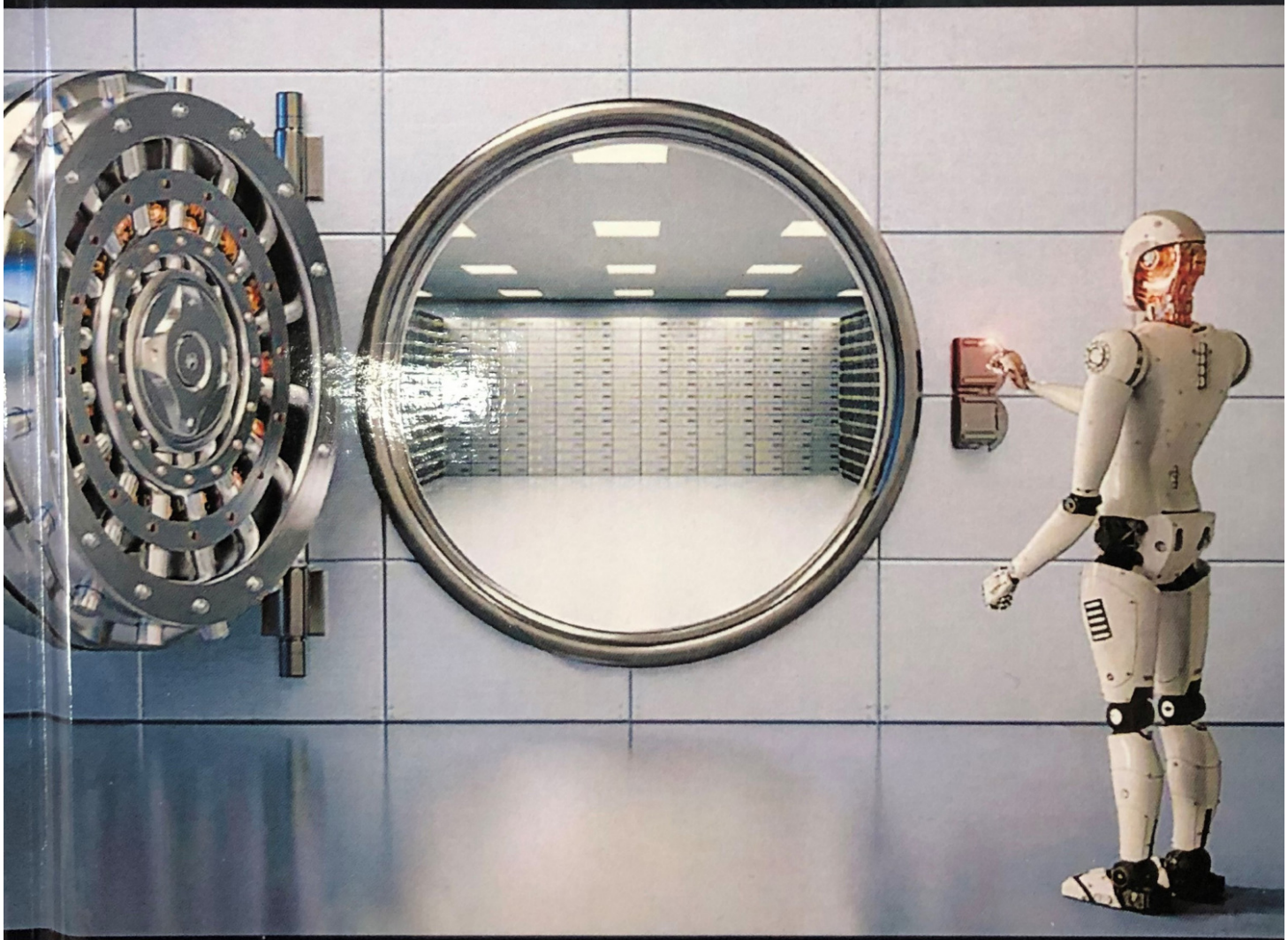
VRB

АССОЦИАЦИЯ «ФИНАНСОВЫЕ ИННОВАЦИИ»

Центр исследований платежных систем и расчетов

100 ЛЕТ
ФИНАНСОВЫЙ УНИВЕРСИТЕТ ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

КИБЕРБЕЗОПАСНОСТЬ в условиях электронного банкинга



Практическое пособие под редакцией П.В. Ревенкова

Коллектив авторов

Кибербезопасность в условиях электронного банкинга. Практическое пособие

«Центр Исследований Платежных Систем и Расчетов»

2020

УДК 0.87.2
ББК Бя73

Коллектив авторов

Кибербезопасность в условиях электронного банкинга. Практическое пособие / Коллектив авторов — «Центр Исследований Платежных Систем и Расчетов», 2020

ISBN 978-5-907244-61-0

В книге рассматриваются вопросы, связанные как с обеспечением кибербезопасности в условиях применения систем электронного банкинга, так и с анализом источников рисков, возникающих при использовании технологии дистанционного банковского обслуживания. Описаны основные принципы управления рисками электронного банкинга. Рассмотрены риски, возникающие в кредитных организациях при внедрении систем интернет-банкинга, и риски легализации преступных доходов при использовании электронных денег (включая описание вариантов использования интернет-трейдинга как инструмента отмывания денежных средств на фондовых биржах). Даны рекомендации по организации внутреннего контроля в банках и обеспечению кибербезопасности в условиях применения систем электронного банкинга. Представлены практические рекомендации по обеспечению защиты информации при использовании систем электронного банкинга, проанализировано влияние «теневого интернета» на безопасность электронного банкинга и дана характеристика хищений денежных средств с использованием вредоносных компьютерных программ неправомерного доступа к информации. Издание предназначено для банковских специалистов, практикующих консультантов и аудиторов, преподавателей, аспирантов и студентов, обучающихся финансовым и техническим специальностям, а также может быть полезно всем, кто интересуется тематикой обеспечения кибербезопасности в условиях применения систем электронного банкинга. В формате PDF A4 сохранен издательский макет.

УДК 0.87.2

ББК Бя73

ISBN 978-5-907244-61-0

© Коллектив авторов, 2020
© Центр Исследований Платежных Систем и Расчетов, 2020

Содержание

Кибербезопасность в условиях электронного банкинга Практическое пособие под редакцией П.В. Ревенкова

© Коллектив авторов, 2020

Авторы и рецензенты

Авторы

Бердюгин Александр Александрович – аспирант кафедры «Информационная безопасность» Финансового университета при Правительстве РФ, автор более 20 научных работ, включая 1 учебное пособие и 1 коллективную монографию (глава 2)

Дудка Александр Борисович – кандидат экономических наук, доцент кафедры экономики и финансовой политики Омского государственного университета им. Ф.М. Достоевского, автор более 30 научных работ, включая 3 коллективных монографии (глава 7)

Конявская Светлана Валерьевна – кандидат филологических наук, автор более 150 публикаций, включая 8 книг (4 монографии, 1 учебное пособие, 2 методических пособия, 1 коллективная монография) и 2 патента. Заместитель генерального директора ОКБ САПР (глава 10)

Конявский Валерий Аркадьевич – доктор технических наук, автор более 300 работ, включая 12 книг (в т. ч. 3 учебных пособия), 33 патента. Имеет государственные, ведомственные и общественные награды. Лауреат премии и «золотой медали» имени В.М. Глушкова, академик РАЕН, академик АЭН РФ. Научный консультант ОКБ САПР (глава 10)

Назаров Игорь Григорьевич – кандидат технических наук, старший научный сотрудник, автор более 30 публикаций, включая 9 книг (2 монографии, 7 пособий). Действительный государственный советник 3-го класса, ветеран Вооруженных сил Российской Федерации, почетный сотрудник ФСТЭК России, награжден ведомственными наградами Минобороны России, ФСБ России и ФСТЭК России. Генеральный директор ОКБ САПР (глава 10)

Неваленный Александр Владимирович – независимый эксперт в области информационной безопасности, автор 10 научных работ, включая 2 коллективных монографии (глава 3)

Ожеред Игорь Вячеславович – преподаватель кафедры «Информационная безопасность» Финансового университета при Правительстве РФ, автор 10 научных работ, включая 2 учебных пособия (глава 2)

Ошманкевич Ксения Романовна – аспирант кафедры государственного аудита Высшей школы государственного аудита (факультет) МГУ им. М.В. Ломоносова (глава 2)

Персанов Денис Юрьевич – директор по безопасности AD Group, автор 10 научных работ, включая 3 коллективных монографии (глава 3)

Пименов Петр Александрович – полковник полиции в отставке, сотрудничает с Московским университетом МВД России имени В.Я. Кикотя, автор более 20 научных работ, включая 2 учебных пособия и 1 коллективную монографию (глава 4)

Ревенков Павел Владимирович – доктор экономических наук, профессор кафедры «Информационная безопасность» Финансового университета при Правительстве РФ, автор более 200 научных работ, включая 3 монографии, 2 учебных пособия и 4 коллективных монографии (главы 1, 2, 5–8)

Русин Лев Игоревич – эксперт в сфере проведения финансовых расследований, направленных на выявление и пресечение противоправной деятельности, связанной с неправомерным использованием инсайдерской информации и манипулированием рынком ценных бумаг, а также с легализацией (отмыванием) преступных доходов. Занимал различные должности в Следственном Комитете, Росфинмониторинге и Банке России (глава 9)

Силин Николай Николаевич – заместитель генерального директора FinTech Lab, приглашенный преподаватель программы «MBA – управление инвестициями» Банковского инсти-

тута НОУ «Высшая школа экономики», член Совета по финансово-промышленной и инвестиционной политике ТПП РФ, эксперт «Клуба «Валдай». Один из ключевых разработчиков концепции Форума инновационных финансовых технологий Finopolis, автор более 20 публикаций по тематике информационных, образовательных и бизнес-технологий (глава 11)

Фролов Дмитрий Борисович – доктор политических наук, кандидат юридических наук, советник генерального директора ФГУП «Российская телевизионная и радиовещательная сеть», член экспертного совета Комитета Государственной Думы по безопасности и противодействию коррупции, заведующий кафедрой «Организация технической эксплуатации сетей телевизионного и радиовещания» МТУСИ, автор более 120 научных работ, включая 4 коллективные монографии (глава 2)

Рецензенты

Дворянкин Сергей Владимирович – доктор технических наук, профессор кафедры «Информационная безопасность» Финансового университета при Правительстве РФ, профессор кафедры «Комплексная безопасность критически важных объектов» РГУ НГ им. И.М. Губкина, профессор кафедры защиты информации (ИУ-10) МГТУ им. Н.Э. Баумана, академик, действительный член РАЕН. Автор более 200 научных работ и 5 изобретений, в том числе монографий, учебников и учебных пособий. Член Евразийской ассоциации экспертов в области кибербезопасности

Крылов Григорий Олегович – доктор физико-математических наук, кандидат юридических наук, профессор, заслуженный работник высшей школы, профессор кафедры «Информационная безопасность» Финансового университета при Правительстве РФ, профессор кафедры «Финансовый мониторинг» Национального исследовательского ядерного университета «МИФИ», действительный член (академик) Российской академии транспорта и Академии военных наук. Автор более 300 научных работ, в том числе монографий, учебников и учебных пособий. Полковник в отставке, ветеран военной разведки, ветеран Вооруженных сил, ветеран труда

Принятые сокращения

АПМДЗ – аппаратно-программный модуль доверенной загрузки
АПО – аппаратно-программное обеспечение
АРМ КБР – автоматизированное рабочее место клиента Банка России
АС – автоматизированная система
БАС – банковская автоматизированная система
БКБН – Базельский комитет по банковскому надзору
БКИ – бюро кредитных историй
ВРБ – высшее руководство банка
ВрПО – вредоносное программное обеспечение
ГосСОПКА – Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак
ДБО – дистанционное банковское обслуживание
ДВС – доверенная вычислительная среда
ДСС – доверенный сеанс связи
ЕБС – Единая биометрическая система
ИБ – информационная безопасность
ИКТ – информационно-коммуникационные технологии
ИОК – инфраструктура открытых ключей
ИПС – изолированная программная среда
ИТ – информационные технологии
КА – код аутентификации
КИИ – критическая информационная инфраструктура
КП – ключ подписи
НКЦКИ – Национальный координационный центр по компьютерным инцидентам
НОИ – Национальный оператор идентификации
НСД – несанкционированный доступ
ОКФС – организация кредитно-финансовой сферы
ОС – орган сертификации
ПАК – программно-аппаратный комплекс
ПИБ – политика информационной безопасности
ПИН – персональный идентификационный номер
ПКО – подконтрольный объект
ПОД/ФТ – противодействие легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма
РКБ – резидентный компонент безопасности
РПВ – разрушающие программные воздействия
СБР – системный банковский риск
СВА – служба внутреннего аудита
СВК – служба внутреннего контроля
СВТ – средство вычислительной техники
СД – совет директоров
СДЗ – средство доверенной загрузки
СИБ – служба информационной безопасности
СКЗИ – средство криптографической защиты информации
СН – служебный носитель
СОДС – средство обеспечения доверенного сеанса связи

СУИБ – система управления информационной безопасностью
СФК – среда функционирования криптографии
СЭБ – система электронного банкинга
СЭДО – система электронного документооборота
СЭП – средство электронной подписи
ТБР – типичный банковский риск
УКЭП – усиленная квалифицированная электронная подпись
ЦОД – центр обработки данных
ЭБ – электронный банкинг
ЭБР – элементарный банковский риск
ЭлД – электронный документ
ЭП – электронная подпись
ЭСП – электронное средство платежа
ЭЦП – электронная цифровая подпись
AI – Artificial Intelligence
API – Application Programming Interface
CPS – Cyber-Physical Systems
DDoS – Distributed Denial of Service
DoS – Denial of Service
EBG – Electronic Banking Group
GAN – Generative Adversarial Network
GDPR – General Data Protection Regulation
IoE – Internet of Everything
IoT – Internet of Things
ISP – Internet Service Provider
ML – Machine Learning
OCC – Office of the Comptroller of the Currency
OCF – Open Connectivity Foundation
OFC – OpenFog Consortium
PaaS – Platform as a Service
PFM – Personal Financial Management
RPA – Robotic Process Automation
SCS – Social Credit Score
SWIFT – Society for Worldwide Interbank Financial Telecommunications
VPN – Virtual Private Network
XBRL – eXtensible Business Reporting Language

Вступительное слово

Банковский бизнес одним из первых начал использовать преимущества работы в киберпространстве, что обусловлено значительным сокращением затрат на осуществление операционной деятельности: нет необходимости содержать банковские офисы, а функции операциониста выполняет сам клиент с использованием компьютера, планшета или смартфона.

Однако наряду с очевидной привлекательностью такого способа проведения банковских операций появляется и немало дополнительных рисков (как у банка, так и у его клиентов), источниками которых являются виртуальный характер дистанционных банковских операций и постоянно возрастающая активность киберпреступников, ставящих основной своей целью незаконное завладение денежными средствами банков и (или) их клиентов, а также их персональными данными.

Киберпреступность, обладая высокой степенью латентности, остается одним из главных сдерживающих факторов распространения систем электронного банкинга в кредитно-финансовой сфере. В связи с этим развитие научных подходов к решению данных проблем, несомненно, будет способствовать своевременному принятию эффективных защитных мер, обеспечивающих безопасность работы в киберпространстве. Появление таких работ – это очередной шаг к детальному изучению всех особенностей предоставления как банковских, так и в целом финансовых услуг в киберпространстве.

Предлагаемая вашему вниманию книга написана профессионалами своего дела, имеющими большой практический опыт работы по обеспечению кибербезопасности как в регулирующих органах, так и в бизнес-структурах. Она может представлять интерес для студентов, аспирантов, обучающихся по специальностям «Информационная безопасность» и «Банковское дело», а также для преподавателей, работающих по данным специальностям, и всех читателей, желающих получить новые знания в области обеспечения кибербезопасности при использовании систем электронного банкинга.

Р.А. Прохоров,
Председатель Правления Ассоциации
«Финансовые инновации» (АФИ)

Предисловие

Технологии дистанционного банковского обслуживания (включая системы электронного банкинга) стали активно применяться (как в России, так и за рубежом) с начала третьего тысячелетия.

За 20 с небольшим лет системы электронного банкинга для многих людей стали привычным инструментом. Современный смартфон выступает не только как средство связи, органайзер, хранилище аудио- и видеофайлов, игровой компьютер, но и как удобное устройство, с помощью которого можно выбирать товары и услуги, заказывать билеты, а также моментально производить оплату своего выбора.

Для того чтобы любая технология получила широкое распространение, а самое главное – доверие со стороны клиентов, должны выполняться по крайней мере три условия:

– она должна быть легальной (т. е. иметь правовые основания для использования[1]);

– она должна быть безопасной (иначе сложно рассчитывать на доверие к ней со стороны клиентов);

– она должна «хорошо продаваться» (т. е. быть привлекательной для бизнеса – приносить прибыль).

Применяя такой подход к технологиям дистанционного банковского обслуживания, можно сказать, что с правовой точки зрения препятствий для внедрения и использования таких технологий почти нет. Однако есть некоторое отставание нормативной базы, регламентирующей банковскую деятельность, что в ряде случаев может привести к ослаблению контроля над кредитными организациями со стороны регулирующих органов.

В рамках обеспечения безопасности многие кредитные организации стараются использовать комплексный подход, применяя различные меры на всех этапах жизненного цикла систем электронного банкинга. Однако возрастающая активность киберпреступников, которые используют различные способы получения конфиденциальной информации (в т. ч. применяя методы социальной инженерии), и недостаточный уровень финансовой грамотности и киберграмотности граждан не позволяют считать технологии дистанционного банковского обслуживания в полной мере безопасными. Минимизировать сопутствующие риски можно только за счет успешного решения всех задач, связанных с должным уровнем кибербезопасности, как на стороне банков, так и на стороне их клиентов (при непосредственном участии всех регулирующих органов).

Добавим, что сегодня для развития технологий дистанционного банковского обслуживания (включая системы электронного банкинга) складываются достаточно хорошие условия. Повсеместно растет число клиентов, которые ежедневно пользуются одним из видов электронного банкинга, заметно улучшаются качество работы и безопасность самих банковских вебприложений.

Возвращаясь к проблеме обеспечения кибербезопасности, можно сказать, что она является основной для успешного внедрения и распространения технологий дистанционного банковского обслуживания. Именно от уровня обеспечения кибербезопасности зависит доверие клиентов как к отдельным элементам систем электронного банкинга, так и ко всей банковской системе Российской Федерации.

Обеспечение кибербезопасности (или, другими словами, безопасности в киберпространстве) включает в себя целый комплекс организационных и технических мероприятий. Но помимо этого надо минимизировать сопутствующие риски, которые возникают при использовании технологий дистанционного обслуживания.

---

[1] В ряде случаев вводят так называемый «режим регуляторной песочницы».

Данная коллективная монография – это попытка рассмотреть наиболее характерные источники рисков, возникающие в условиях применения систем электронного банкинга, и предложить меры по снижению возможных негативных последствий их проявления. Также мы попытались оценить возможные сценарии развития технологий и социального поведения, существенно влияющие на природу и масштабы таких рисков. Книга не претендует на полное рассмотрение всех возможных угроз и сопутствующих рисков, связанных с внедрением в кредитных организациях систем электронного банкинга, однако может оказать помощь менеджерам банков, специалистам риск-подразделений и служб внутреннего контроля в разработке внутренних методических документов, направленных на минимизацию возможных последствий проявления источников рисков, связанных с использованием систем электронного банкинга.

П.В. Ревенков,
доктор экономических наук,
профессор кафедры «Информационная безопасность» Финансового университета при Правительстве Российской Федерации

1. Электронный банкинг и риски недостаточного обеспечения информационной безопасности

В природе ничего не возникает мгновенно и ничто не появляется в свет в совершенно готовом виде.
Александр Иванович Герцен, русский прозаик, публицист, критик и философ

Введение

Настанет время, когда наши потомки будут удивляться, что мы не знали таких очевидных вещей.
Луций Анней Сенека, древнеримский философ

Электронный банкинг (ЭБ) – один из самых динамично развивающихся видов дистанционного банковского обслуживания (ДБО)[2]. Получив широкое распространение в Америке и Европе, ЭБ завоевывает и российский рынок.

Вот только самые известные преимущества, которые получает клиент кредитной организации, использующий для совершения своих банковских операций системы ЭБ (СЭБ):

– нет необходимости посещать банк лично и можно контролировать свои счета или управлять ими в режиме «24/7» (т. е. круглосуточно 7 дней в неделю);

– ряд кредитных организаций устанавливают продленный режим операционного дня и все платежи (зачисления и списания), поступившие в банк до 18:00 по московскому времени, исполняются банком в этот же операционный день;

– вся информация по счетам и операциям хранится на сервере кредитной организации и всегда доступна для пользователей СЭБ;

– для защиты информации используются современные средства криптографической защиты;

– разработчики большинства программных продуктов СЭБ производят обновление своих программ автоматически (не требуется обращения в кредитную организацию) [103, с. 172].

Внедрение данной услуги обходится кредитной организации относительно недорого и в дальнейшем быстро окупается только за счет абонентской платы.

Однако, несмотря на очевидную привлекательность такого способа совершения банковских операций, как у кредитной организации, так и у ее клиентов возникает немало дополнительных источников банковских рисков. Основными причинами этого являются:

– виртуальный характер дистанционных банковских операций;

– общедоступность открытых телекоммуникационных систем;

– предельно высокая скорость выполнения транзакций;

– глобальные масштабы межсетевого операционного взаимодействия;

– активное участие фирм – провайдеров услуг в проведении операций.

Таким образом, организации кредитно-финансовой сферы должны постоянно совершенствовать свои системы информационной безопасности, а специалистам риск-подразделений необходимо учитывать возможные последствия проявления рисков, связанных с работой в

[2] Как правило, под ДБО понимают совокупность методов предоставления банковских услуг с помощью средств телекоммуникации, при использовании которых присутствие самого клиента в банке не требуется.

киберпространстве, и своевременно принимать меры по минимизации негативных последствий.

1.1. Интернет и банковский бизнес

Если новое поколение будет повторять устаревшие понятия, то как мы обеспечим быстрое движение вперед?
Иван Ефремов. Туманность Андромеды

Современный банковский бизнес невозможно представить без использования новейших достижений в области информационных и телекоммуникационных технологий. Технологии ДБО стали не только способом снижения себестоимости самих процессов выполнения банковских операций, но и основным конкурентным преимуществом любой кредитной организации на рынке банковских услуг.

Одним из условий повышения доверия к технологиям ДБО является обеспечение должного уровня информационной безопасности.

Перед тем как начать разговор о проблемах, связанных с безопасным применением различных систем ДБО (включая СЭБ), необходимо разобраться, что такое безопасность.

Безопасность (как самостоятельный объект исследования) имеет некоторые фундаментальные свойства:

1) безопасность никогда не бывает абсолютной – всегда есть некий риск ее нарушения. Таким образом, усилия по обеспечению безопасности реально сводятся к задаче понижения уровня риска до приемлемого;

2) измерить уровень безопасности невозможно, можно лишь косвенно его оценить, измерив соответствующие показатели, характеризующие состояние безопасности банка[3];

3) наступление всех рисковых событий предотвратить невозможно, можно лишь понизить вероятность наступления отдельных событий, то есть рисковые события будут наступать реже;

4) можно также понизить степень ущерба от наступления такого события, но при этом чем реже наступает рисковое событие, тем сильнее ущерб от него;

5) при любом несанкционированном вмешательстве в процесс принятия управленческих решений и обработки информации в первую очередь страдает ее безопасность.

Современный банк представляет собой комплекс, включающий в себя не только квалифицированный персонал, но и сложные автоматизированные системы, и одним из наиболее уязвимых элементов этого комплекса является банковская автоматизированная система (БАС).

Современные достижения в развитии информационных и коммуникационных технологий, в основе которых лежат возможности интернета, значительно повлияли на эволюционные процессы, связанные с формами проявления функции денег как средства платежа, и привели к формированию глобальной электронной среды для экономической деятельности за счет существенного снижения себестоимости банковских операций. Технологии ДБО можно рассматривать и как качественный аспект поступательного развития кредита[4].

Еще в конце прошлого века эксперты в области экономики стали говорить о новой среде – сетевой экономике (networked economy)[5]. Так, например, в докладе, подготовленном Европейской комиссией[6], глобальная сетевая экономика определяется как «среда, в которой любая компания или индивид, находящиеся в любой точке экономической системы, могут контак-

---

[3] В связи с этим можно говорить только о вероятности наступления того или иного события и масштабе его последствий, то есть использовать для оценки уровня безопасности рисковый подход.

[4] См.: Валенцева Н.И. Законы и закономерности развития кредита // Банковские услуги. 2010. № 12. С. 2–9.

[5] Данное понятие часто упоминается в сочетании со словом «глобальная».

[6] Status Report on European Telework // Telework 1997, European Commission Report, 1997. URL: http://www.eto.org.uk/twork/tw97eto.

тировать легко и с минимальными затратами с любой другой компанией или индивидом по поводу совместной работы, для торговли, для обмена идеями и ноу-хау или просто для удовольствия». Возникновение сетевой экономики приводит к эволюции современных экономических систем, развитию нерыночных механизмов регулирования и сетевых организационных структур [102, с. 539].

Новые возможности глобальной коммуникации между людьми дают им и новые инструменты для реорганизации форм их совместной деятельности.

Одним из самых эффективных способов модернизации инфраструктуры в экономике и создания сетевых институциональных структур является использование возможностей интернет-технологий.

Интернет-технологии не только быстро внедряются в политику, бизнес, государственное управление, но и трансформируют характер межличностных отношений в обществе (формируются виртуальные онлайновые сообщества, устанавливаются отношения информационного партнерства, осуществляется группировка пользователей по определенным информационным интересам). Все это приводит к тому, что общество привыкает к активному использованию современных информационных и коммуникационных технологий. Тенденция распространяется и на банковские услуги. Это свидетельствует о том, что мы имеем дело с самым быстрорастущим в истории человечества рыночным сообществом. Буквально за несколько лет все основные экономические виды деятельности были освоены интернетом: появились интернет-коммерция, интернет-реклама, интернет-банкинг и т. д.

Анализ трудов отечественных и зарубежных ученых позволил выявить ряд отличительных признаков всемирной паутины, способных существенным образом влиять на экономику:

– интернет втягивает в глобальную конкуренцию все компании и организации (в т. ч. коммерческие банки) независимо от места их расположения. Большинство кредитных организаций предоставляют одинаковый набор банковских услуг, поэтому выбор клиентов, как правило, связан с качеством их оказания и уровнем доверия к данному коммерческому банку;

– глобальная сеть значительно обострила конкурентную борьбу и потребовала от всех участников банковского рынка соответствовать международным стандартам (оформление вебсайтов, поддержка нескольких языков, доступность и функциональность представительств в интернете и т. д.);

– целый ряд процессов, в том числе обслуживание и эксплуатацию аппаратно-программного обеспечения систем ДБО (включая СЭБ), можно передать на аутсорсинг. Веб-сайты многих кредитных организаций разрабатывали профессиональные компании, хорошо владеющие вопросами продвижения брендов и привлечения максимального числа клиентов;

– клиенты, использующие системы интернет-банкинга, более требовательны к качеству выполнения банковских операций, так как легко могут сравнить услуги банка с аналогичными услугами кредитных организаций – конкурентов (банки, значительно отдаленные друг от друга географически, в глобальной сети находятся «на расстоянии одного клика»);

– интернет позволяет выбирать коммерческие банки практически в любой стране и строить с ними взаимовыгодное сотрудничество для повышения эффективности и снижения издержек;

– стремительное развитие интернет-технологий не позволяет однозначно спрогнозировать все стратегические риски, связанные с ДБО;

– интернет ускоряет распространение новых технологий и идей. Коммерческие банки в любой стране, в том числе в развивающейся, могут с помощью глобальной сети отслеживать технологические инновации, получать информацию о новых банковских продуктах, используемых в Европе, Японии, Северной Америке, а также о новых проектах и действиях лидеров в каждом секторе банковского бизнеса – с точки зрения бизнеса национальные границы утратили былое значение;

– электронные банковские технологии требуют от коммерческих банков действовать «в режиме интернета» или «со скоростью интернета» – скорость становится одним из основных достоинств успешного бизнеса;

– технологии ДБО (включая СЭБ) позволяют оформлять первичные бухгалтерские документы намного быстрее;

– интернет является самым дешевым на сегодняшний день каналом обслуживания клиентов. Предоставление банковских услуг через интернет позволяет сократить служащих, которые ведут телефонные переговоры, оформляют банковские документы, консультируют клиентов по вопросам выполнения отдельных банковских операций, принимают различные претензии, предложения и др.[7];

– под интернет-проекты относительно легко получить инвестиции. Во многих странах инвестиции в интернет-проекты поддерживаются государством, так как, развивая интернет-технологии во всех отраслях экономики (включая банковский бизнес), страна выходит на новый качественный уровень;

– интернет-технологиям постоянно требуется ценный ресурс – человеческий талант: как в форме технических знаний и опыта, так и в форме управленческих ноу-хау. Самые ценные в конкурентном отношении активы организации – это лидерство в разработке ключевых технологий и кадры с уникальными опытом и знаниями.

Благодаря возможностям интернета сообщество людей стало преобразовываться в новую социально-экономическую формацию – глобальное информационное общество.

На данном этапе развития общества можно говорить об информационной революции, которая постепенно охватывает все страны, невзирая на их экономическое развитие и уровень финансовой грамотности населения.

Интернет изменил мир, и эти изменения возрастают в геометрической прогрессии. Трансформировались отношения людей, их общение, мировоззрение, поиск данных, а вместе с тем методы работы институтов и организаций. Каких-то 15 лет назад еще не было таких профессий, как разработчик архитектуры социальных сетей и руководитель цифровой рекламы. В последние годы в нашу жизнь ворвались, заняв в ней доминирующие позиции, Facebook, LiveJournal, YouTube, Twitter, Skype и многие другие интернет-продукты и социальные сети. Темпы развития этих технологий стабильно растут.

Многие банки сегодня рассматривают Facebook как важный источник информации, поскольку данная социальная сеть содержит огромное количество сведений о пользователях. Эти данные могут быть применены для оценки кредитных рисков и кредитоспособности клиентов.

Отметим одну особенность в поведении людей, которая связана с появлением интернета. Все больше людей предпочитают потреблять значительное количество маленьких фрагментов информации, а не целостный блок текста[8].

Зная об этом, западные информационные агентства на своих интернет-страницах иногда публикуют абзацы, состоящие из одного предложения. В маленьком фрагменте сложно (а чаще невозможно) передать много информации, но для совершения транзакции с помощью систем ДБО клиент и не должен читать длинные инструкции (они могут быть оформлены в виде аудио- или видеоролика).

---

[7] Еще в середине 1999 г. на веб-сайте Международного валютного фонда были приведены расчеты затрат на выполнение банковских операций: стоимость ручной обработки транзакции в филиале коммерческого банка составляла в среднем более 1 доллара, телефонное обслуживание оценивалось в 60 центов за услугу, транзакции через банкоматы и клиринговые центры стоили около 25 центов, а транзакция через интернет обходилась всего в 1 цент. Учитывая постоянное снижение тарифов на предоставление доступа в интернет, можно предположить, что сейчас банковские операции, выполняемые в рамках интернет-банкинга, обходятся еще дешевле.

[8] По этой же причине у многих возникает желание пропустить большой абзац.

Заметим, что информационные процессы в сознании человека, такие как обнаружение и интерпретация сенсорных сигналов, память, образы, мышление, и их изменения во времени представляют объект исследования когнитивной психологии. Поэтому серьезные компании, занимающиеся созданием программ для систем ДБО и пользовательских интерфейсов, основывают свои разработки на моделях, являющихся плодами когнитивной психологии.

По мере проникновения интернета в нашу жизнь растет популярность всевозможных мобильных устройств. Классические ноутбуки слишком громоздки, а планшеты еще не всегда обладают нужной функциональностью, поэтому и появляются все новые и новые миниатюрные лэптопы с сенсорными экранами.

Подобные устройства теперь не роскошь, а неотъемлемые компаньоны современного человека (в этом убеждаешься, когда забываешь дома мобильный телефон или планшетный компьютер).

Согласно докладу Антимонопольного центра БРИКС, количество интернет-пользователей в крупнейших странах по состоянию на март 2019 г. составило:

– 829 млн в Китае (первое место);

– 560 млн в Индии (второе место);

– 293 млн в Соединенных Штатах Америки (третье место);

– 109,5 млн в России (восьмое место)[9].

В декабре 2018 г. Международный союз электросвязи (ITU) представил отчет, в котором сообщил, что в интернет выходят 3,9 млрд человек, или 51,2 % населения планеты[10]. При этом в России 81 % граждан пользуются интернетом с той или иной периодичностью. То есть:

– 65 % выходят в сеть ежедневно;

– 14 % – несколько раз в неделю или месяц;

– 2 % пользуются интернетом крайне редко;

– 19 % не обращаются ни к каким интернет-ресурсам.

В первую очередь россияне заходят в интернет, потому что им это требуется для работы и учебы (44 %). Опрошенные стали реже искать через интернет новых знакомых, людей с близкими интересами (снижение с 16 % в 2014 г. до 4 % в 2018 г.).

Покупки через интернет ежедневно оформляют 2 % опрошенных (против 7 % в 2014 г.)[11].

Еще одно изобретение человечества в сфере высоких технологий – это «облака». Облачные платформы все чаще и успешнее используются для решения корпоративных и операторских задач. В целом применение облачных технологий позволяет:

– создать простую абстрактную среду, в которой пользователь может получить ресурсы по требованию, а компания – легче и быстрее внедрить новые приложения и услуги;

– отвлечь организацию от рутинных задач и сконцентрировать внимание на главных направлениях, выделяющих ее из конкурентной среды и значительно повышающих эффективность работы.

Нигерийская кредитная организация Renaissance Credit, образованная в октябре 2012 г., за первые полгода расширила клиентскую базу до 3 тыс. человек. Все информационные процессы компании (составление документов, работа с электронными таблицами и почтой, а также все банковские операции) происходят в «облаке», что позволило сократить штат НТ-специалистов до одного человека[12].

По мнению экспертов компании Microsoft, в богатых странах банки с помощью облачных технологий уже начали обрабатывать данные, не содержащие значимой информации о клиен-

[9] Интернет-доступ (мировой рынок). URL: http://www.tadviser.ru/a/53635.

[10] Там же.

[11] Просторы интернета: для работы или развлечений? ВЦИОМ. URL: https:// wciom.ru/index.php?id=236&uid=9322.

[12] Подробнее см.: The IT cloud // The Economist. 2013. No. 8845. P. 61.

тах, но требующие больших вычислительных мощностей. Испанский банк Bankinter использует облачную платформу Amazon для моделирования кредитных рисков: вычисления, выполнявшиеся на оборудовании самого банка за 20 часов, теперь занимают 20 минут. Также крупные банки задействуют «облака» для тестирования своих компьютерных систем, не подвергая себя опасности сбоев. Многие банки переконфигурируют свои системы в частные облачные платформы, что позволяет подключаться к облачным технологиям, находящимся в общественном доступе.

Разумеется, у широкого применения «облаков» есть свои недостатки, связанные прежде всего с безопасностью и защитой данных. Небольшим банкам крупные информационные центры, созданные такими компаниями, как Amazon и Microsoft, обеспечивают более высокий уровень безопасности, чем они сами могут себе позволить. Крупные банки, имеющие собственные вычислительные центры, опасаются передавать клиентскую информацию в посторонние руки. Кроме того, кража информации или сбой в работе банка, пользующегося «облаком», вызовет жесткую реакцию регулирующих органов. Некоторые страны настаивают на том, чтобы данные клиентов хранились в пределах национальных границ. Компании, предоставляющие облачные услуги, будут вынуждены строить небольшие информационные центры, снижая тем самым издержки. При этом такие компании из соображений безопасности стремятся не раскрывать местонахождение своих «облаков».

Впрочем, возможность повышения рентабельности делает переход банков на облачные технологии неизбежным, а указанные выше проблемы могут повлиять лишь на скорость данного процесса.

1.2. Основные виды мошенничества в интернете

Во всех странах железные дороги для передвижения служат, а у нас сверх того и для воровства.
Михаил Евграфович Салтыков-Щедрин, русский писатель

Благодаря развитию интернета появилась возможность совершения покупок, банковских переводов и платежей в режиме реального времени (онлайн). Несомненно, это позволило улучшить жизнь граждан, предоставив им новые, более современные сервисы. Однако вместе с ними возникли и новые способы мошенничества.

Наиболее активно мошенничество в интернете осуществляется в кредитно-финансовой сфере и сфере ритейла. Это обусловлено прежде всего тем, что в указанных сферах злоумышленники могут получить наибольшую материальную выгоду.

Самым распространенным способом совершения мошенничества в интернете является фишинг (phishing). Понимание данного явления постоянно изменяется, что усложняет процесс выявления и раскрытия правонарушений.

Так, можно привести несколько распространенных и широко используемых понятий:

1. Фишинг – способ мошеннических действий, при котором злоумышленник рассылает множество сообщений по электронной почте с целью получения личной и финансовой информации о потенциальных жертвах (для дальнейшего доступа к их банковским счетам и другим важным ресурсам).

2. Фишинг – информационная система, применяемая для получения от третьих лиц (пользователей системы) конфиденциальных сведений за счет введения этих лиц в заблуждение относительно ее принадлежности (подлинности) вследствие сходства доменных имен, оформления или содержания информации[13].

3. Фишинг – разновидность попыток несанкционированного доступа, когда жертву провоцируют на разглашение информации, посылая ей фальсифицированное электронное письмо с приглашением посетить веб-сайт, который на первый взгляд связан с законным источником[14].

4. Фишинг – мошеннические веб-сайты, веб-сайты, навязывающие платные услуги на базе SMS-платежей, веб-сайты, обманным путем собирающие личную информацию[15].

При анализе данного понятия можно заметить изменения в самом понимании процедуры фишинга.

Так, при применении первого понятия следует исходить из того, что фишинг осуществляется в виде сообщений, которые приходят якобы от банков, платежных систем, онлайн-аукционов, крупных и широко известных интернет-магазинов. Письмо создается, форматируется и оформляется таким образом, чтобы выглядеть как отправленное из легального источника. Причем подделываются заголовки письма, его внешний вид (включая графические и текстовые элементы), а также ссылки на реальный веб-сайт. В случае с интернет-банкингом письмо, как правило, содержит информацию о внезапно возникших технических проблемах на веб-сайте банка, в связи с чем необходима проверка учетных записей и регистрационных данных пользователей. Далее жертве предлагается открыть «регистрационную форму» и ввести инте-

[13] Правила регистрации доменных имен в доменных зонах. RU и. РФ. URL: https: / / cctld.ru/ru/docs/project/algoritm/rules_draft.pdf.

[14] ГОСТ Р 56205-2014/IEC/TS 62443-1-1:2009. Национальный стандарт Российской Федерации. Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 1–1. Терминология, концептуальные положения и модели (утв. и введен в действие Приказом Росстандарта от 10.11.2014 № 1493-ст).

[15] Письмо Минобрнауки России от 28.04.2014 № ДЛ-115/03 «О направлении методических материалов для обеспечения информационной безопасности детей при использовании ресурсов сети Интернет».

ресующие мошенника данные. Так как эта регистрационная форма загружается не с веб-сайта банка, вся личная информация жертвы отправляется мошеннику (рис. 1).

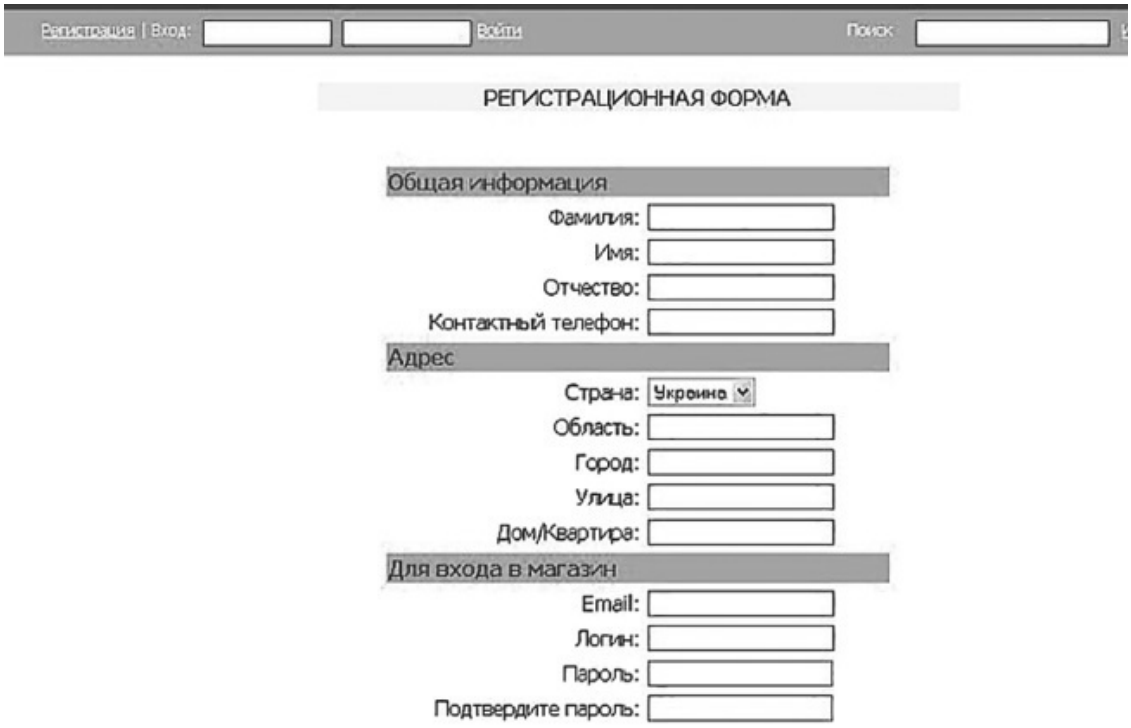


Рис. 1. Регистрационная форма на веб-сайте лжебанка

Получив эти данные, мошенник распоряжается банковским счетом жертвы и кредитной картой, привязанной к этому счету, по своему усмотрению (рис. 2).

Приведем основные рекомендации для клиентов систем интернет-банкинга, помогающие определить действия интернет-мошенников[16]:

[16] Эти же рекомендации должны знать и специалисты кредитной организации, отвечающие за бесперебойное и безопасное функционирование веб-сайта, чтобы без промедления пресекать подобные мошеннические действия.

Рис. 2. Использование фальшивого веб-сайта для выманивания данных по кредитным картам

Данные по кредитным картам

– никогда не отвечать на запросы по электронной почте, касающиеся личной информации, данных банковских счетов, кредитных карт и паролей доступа;

– не переходить по ссылкам на интернет-ресурсы, присланным в сообщениях по электронной почте, а вводить ссылки в адресную строку веб-браузера самостоятельно;

– убеждаться, что при работе с веб-сайтом кредитной организации информация передается в кодированном (шифрованном) виде[17];

– регулярно проверять состояние баланса банковского счета (кредитной карты);

– немедленно сообщать уполномоченным сотрудникам кредитной организации о всех подозрениях на несанкционированный доступ к личной информации и злоупотребление ею.

Далее представлены несколько признаков, по которым можно определить, что произошло соединение с фальшивым веб-сайтом:

– невозможно просмотреть исходный текст веб-сайта[18];

– при использовании другого веб-браузера место адресной строки заметно отличается от привычного;

– при сворачивании окна веб-браузера на панель задач окно с адресом не сворачивается, а «зависает» в нижней части экрана;

---

[17] Речь идет об адресной строке. Для проверки наличия кодированного (шифрованного) вида пользователю необходимо обращать внимание на конфигурацию ссылки веб-сайта банковского учреждения. Кодированным (шифрованным) и безопасным соединением считается ссылка, в начале которой указывается аббревиатура https.

[18] Самостоятельно получить сведения о веб-сайте можно на следующих сетевых ресурсах: www.dnsdtuff.com,www.geobytes.com,www.nextwebsecuritj.com, www.do-maintools.com и др.

– окно с адресной строкой ведет себя как самостоятельное окно Windows-задачи с возможностью перемещения по экрану монитора, но с тенденцией занять определенное место;

– адресную строку невозможно редактировать.

Второе же понимание термина «фишинг» значительно отличается от ранее рассмотренного.

При применении второго определения следует исходить из того, что данное противоправное деяние совершается с использованием домена (веб-сайта). Злоумышленник создает в интернете ресурс, который ввиду сходства информации или интерфейса должен создать у потребителя ложное представление о нахождении на легальном ресурсе. Противоправные деяния с использованием указанной схемы можно формально разделить на несколько категорий. Рассмотрим самые распространенные из них.

1.2.1. Лжебанки

Это одна из самых распространенных категорий фишинговых ресурсов. Недобросовестное лицо создает ресурс фиктивного банка и начинает привлекать денежные средства граждан и юридических лиц во вклады. Пользователь не задумывается о правомерности деятельности данного лица, поскольку интерфейс иногда схож с интерфейсом ресурса, принадлежащего реально существующему банку. Представленные фиктивные документы на ресурсы, такие как сканы лицензий и доверенностей, создают у потребителя впечатление, что банк является легальным (рис. 3).

На рис. 3–7 приведены примеры фиктивных банков[19].

В рамках проекта «Лжебанк» злоумышленники готовы предоставлять «лжекредиты». Потребитель обращается в фиктивный банк с просьбой предоставить ему кредит, псевдобанк якобы одобряет заявку и просит потребителя оплатить курьерскую доставку договора и перечислить страховую сумму. После внесения потребителем оплаты лжебанк, как правило, прекращает контакты с ним.

[19] Автор сознательно приводит не один, а несколько однотипных примеров вебсайтов, чтобы показать разнообразие уловок кибермошенников.

Рис. 3. Веб-сайт фиктивного банка (1)

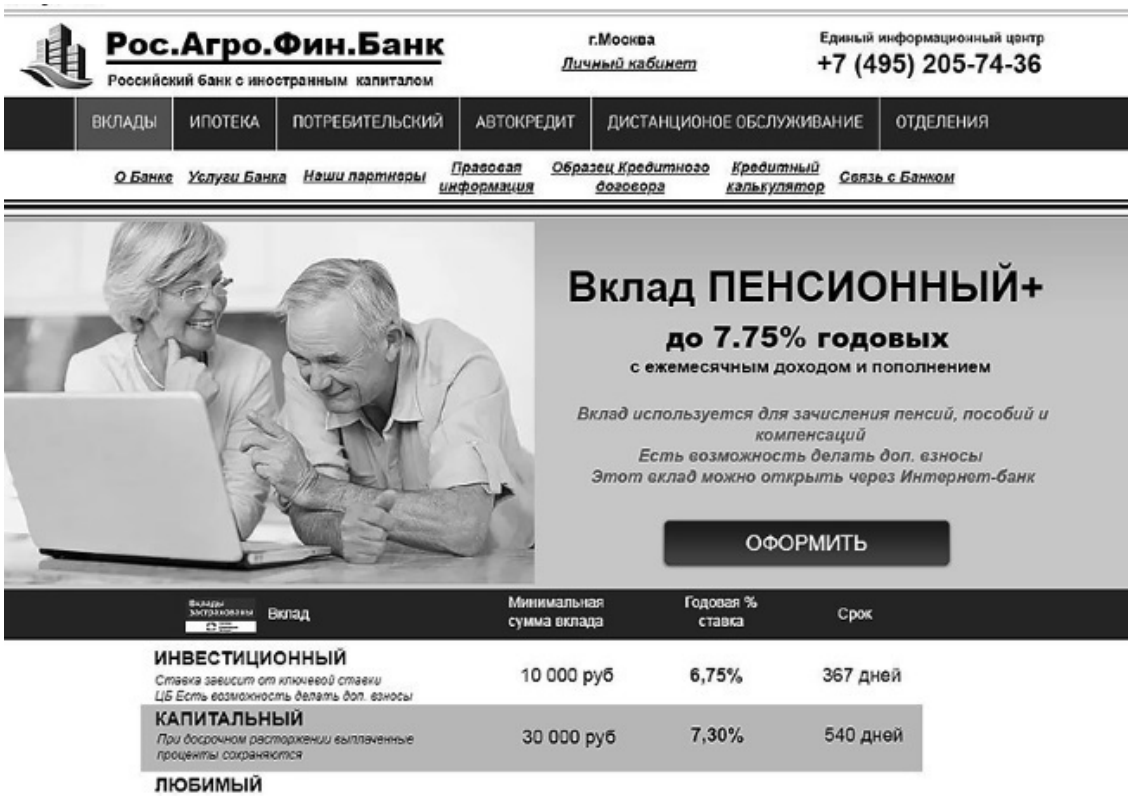


Рис. 4. Веб-сайт фиктивного банка (2)

Рис. 5. Веб-сайт фиктивного банка (3)

Рис. 6. Веб-сайт фиктивного банка (4)

Рис. 7. Веб-сайт фиктивного банка (5)

Согласно статистике ФинЦЕРТ Банка России[20], за 2017–2018 гг. сняты с делегирования 489 веб-сайтов, которые выдавали себя за банки[21]. Количество ресурсов в данной категории позволяет сделать вывод, что злоумышленники активно используют наименования реальных банков и создают интерфейсы веб-сайтов, сходные с интерфейсами вебсайтов данных финансовых институтов. Необходимо отметить, что злоумышленники также активно создают сайты-клоны или сайты-двойники, что позволяет ввести пользователя в заблуждение.

Приведем перечень признаков фишинговых ресурсов данной категории:

1. Информация об организации отсутствует в справочниках/реестрах Банка России, размещенных на официальном веб-сайте Банка России.

На официальном веб-сайте Банка России (www.cbr.ru) размещены следующие информационные ресурсы, позволяющие уточнить наличие или отсутствие лицензии у банка:

– Книга государственной регистрации кредитных организаций;

– Справочник по кредитным организациям (http://www.cbr.ru/credit/main.asp).

2. Информация об организации отсутствует в соответствующих реестрах ФНС России и Роскомнадзора России.

Информацию об организации, представленной на веб-сайте, также возможно проверить в следующих реестрах:

– Едином государственном реестре юридических лиц, размещенном на официальном веб-сайте ФНС России;

– Реестре операторов, осуществляющих обработку персональных данных, размещенном на официальном веб-сайте Роскомнадзора России.

3. Веб-сайт не является официальным и не имеет никакого отношения к организации.

---

[20] ФинЦЕРТ, или Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере, входит в состав Департамента информационной безопасности Банка России.

[21] Подробнее см.: Отчет центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Департамента информационной безопасности Банка России. URL: www.cbr.ru/fincert.

Третий признак – один из сложнейших. Вместе с тем данную информацию можно проверить на официальном веб-сайте Банка России с использованием Сведений об адресах вебсайтов кредитных организаций Российской Федерации. Также отметим, что на сегодняшний день благодаря взаимодействию Банка России и «Яндекса» появилась маркировка банков и кредитных организаций, имеющих лицензию Банка России[22].

Создание веб-сайтов лжебанков стало одним из самых распространенных способов мошенничества на территории России, поскольку злоумышленникам не приходится точно копировать ресурсы реально действующих кредитных организаций: достаточно оформить на вебсайте вкладки с названиями «Кредит», «Вклады» и т. д. Данные наименования позволяют ввести пользователя в заблуждение и создать у него иллюзию, что он находится на веб-сайте действующего банка.

Потребителям необходимо обращать внимание на оформление ресурса: лжебанки, как правило, не утруждают себя размещением на официальном веб-сайте соответствующей документации, в некоторых случаях даже не указывают номер лицензии на осуществление операций. Указанные обстоятельства должны насторожить потребителя и заставить его проверить данную организацию. Фиктивные банки также активно привлекают людей с помощью почтовых рассылок или звонков на номера мобильных телефонов. В данном случае потребители должны быть бдительными и не разглашать свои конфиденциальные данные, которые могут быть использованы для хищения денежных средств.

1.2.2. Лжестраховщики

Появление возможности оформлять электронные полисы ОСАГО с использованием интернета не только облегчило жизнь автолюбителям, но и спровоцировало рост мошенничества в данной сфере.

Злоумышленник в рамках рассматриваемой категории действует различными способами:

– создает копию ресурса реально действующей страховой компании с предложением оформления электронных полисов ОСАГО;

– предлагает фальшивые или необеспеченные бланки страховых организаций.

Потребитель либо оплачивает лжеполис ОСАГО, либо оплачивает доставку и покупает фальшивые бланки.

Согласно статистике ФинЦЕРТ Банка России[23], за 2017–2018 гг. сняты с делегирования 164 веб-сайта, которые выдавали себя за субъекты страхового рынка.

Веб-сайт фиктивной страховой организации позволяет создать у потребителя иллюзию, что покупка бланка не влечет за собой негативных последствий. Вместе с тем, приобретая заведомо фальшивые, пустые и недействительные бланки, потребитель теряет возможность претендовать на страховое возмещение при наступлении страхового случая.

Фиктивная страховая компания привлекает потребителей стоимостью бланков: как правило, она на 60–70 % меньше, нежели стоимость действующего полиса реально зарегистрированной страховой компании.

Вместе с тем в данной категории мошенничества активно используется метод социальной инженерии, помогающий получить доверие потребителя.

На веб-сайты лжестраховщиков потребителей завлекают различными способами, такими как:

---

[22] Маркировка осуществляется в виде зеленой галочки, которая устанавливается рядом с адресной строкой и наименованием веб-сайта при поиске ресурса в поисковой системе «Яндекс».

[23] Подробнее см.: Отчет центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Департамента информационной безопасности Банка России. URL: www.cbr.ru/fincert.

– всплывающая реклама в поисковых системах;

– SMS-рассылки и звонки на абонентские номера клиентов различных страховых компаний;

– запросы в поисковых системах.

Псевдостраховые компании становятся достаточно распространенными в России, поскольку потребитель старается сэкономить время и денежные средства при оформлении страхового полиса в надежде на то, что страховой случай не наступит.

Также на практике встречаются случаи, когда потребитель заказывает ту или иную страховую услугу, оплачивая ее переводом на карту лжестраховщика или на его счет. Лжестраховщик обязуется передать страховой полис или предоставить иную услугу в определенное время, но потребитель так и не получает полис или услугу.

В связи с этим потребитель должен не только обращать внимание на оформление и содержание ресурса страховой компании, но и проверять данную организацию в соответствующих справочниках и реестрах (Справочнике участников финансового рынка Банка России, перечне Российского союза автостраховщиков).

Отметим, что в соответствии с перечнем Российского союза автостраховщиков и информацией, размещенной на его официальном вебсайте, не все страховые организации уполномочены на оформление электронных полисов ОСАГО. Потребитель при переходе на веб-сайт страховой компании должен проверить следующее:

– наличие организации в Справочнике участников финансового рынка Банка России (http://www.cbr.ru/finmarket/nfo/cat_ufr/);

– присутствие веб-адреса в перечне Российского союза автостраховщиков (https://www.autoins.ru/e-osago/chleny-rsa-osushchestvlyayushchie-oformlenie-elektronnykh-polisov/).

На рис. 8-10 приведены примеры веб-сайтов фиктивных страховых компаний.

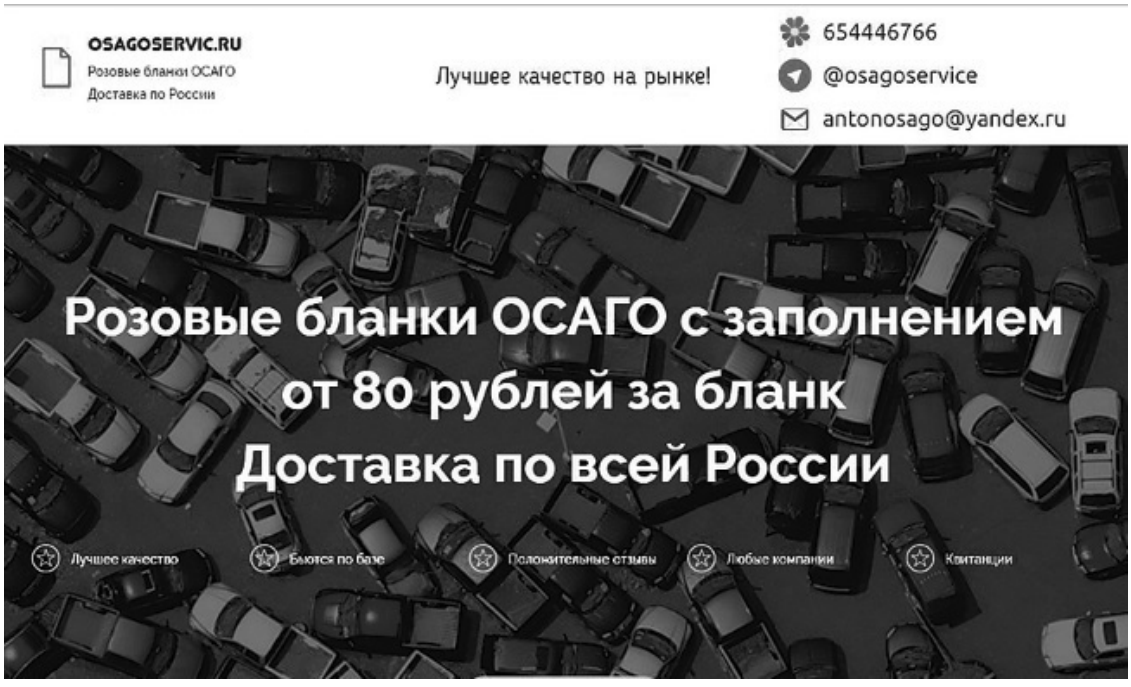


Рис. 8. Веб-сайт фиктивной страховой организации (1)

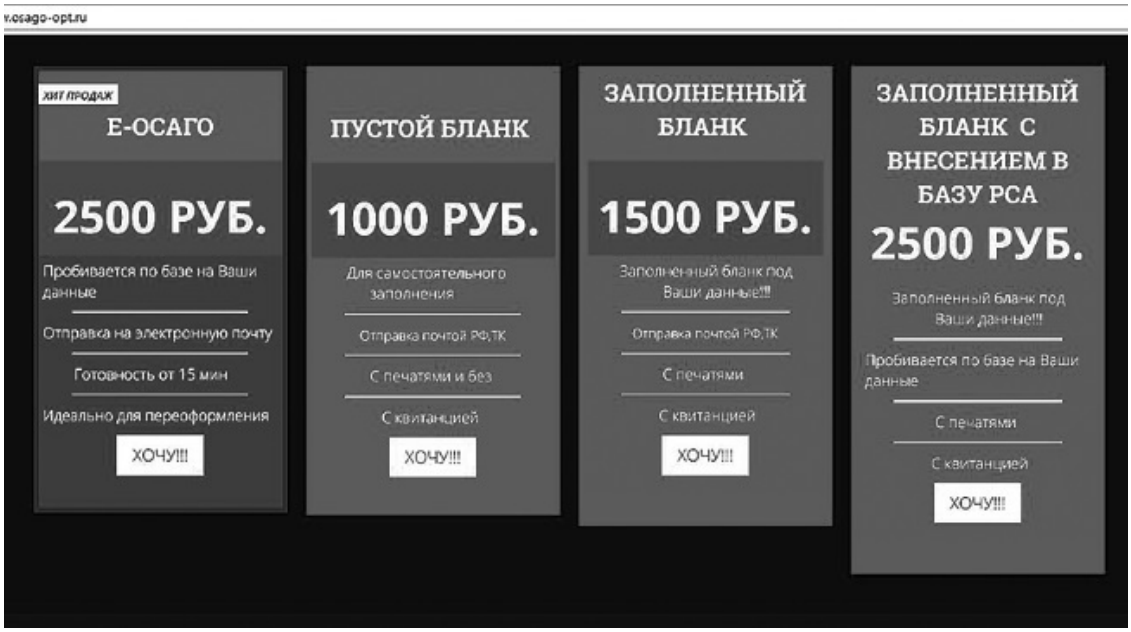


Рис. 9. Веб-сайт фиктивной страховой организации (2)

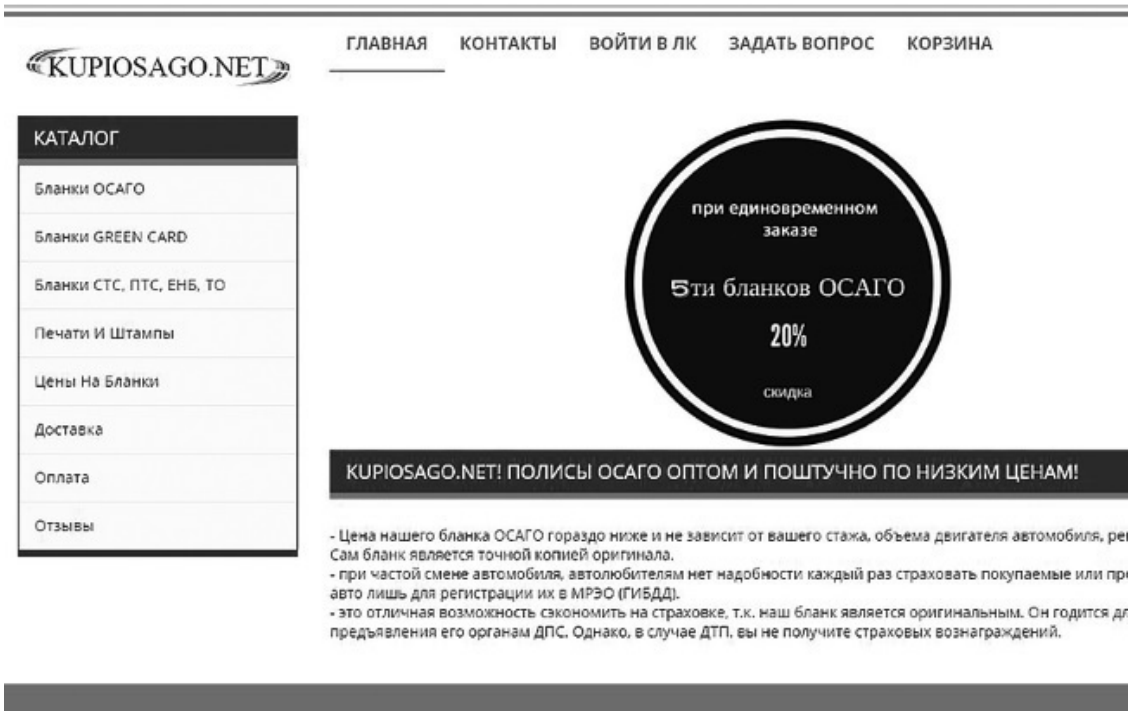


Рис. 10. Веб-сайт фиктивной страховой организации (3)

1.2.3. ПсевдоP2P-переводы

Данная категория является одной из самых привлекательных для злоумышленников. Согласно статистике ФинЦЕРТ Банка России, за 20172018 гг. сняты с делегирования 209 веб-сайтов, которые выдавали себя за ресурсы, предоставляющие услуги по переводу денежных средств с карты на карту[24].

[24] Подробнее см.: Отчет центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Департамента информационной безопасности Банка России. URL: www.cbr.ru/fincert.

Привлекательность этой категории обусловлена простотой оформления информационного ресурса для хищения денежных средств. Злоумышленники получают конфиденциальные данные как платежной карточки, так и самого потребителя.

Простота оформления информационных ресурсов, предоставляющих услуги P2P-переводов, позволяет мошенникам достаточно легко их подделывать: оформляется изображение пластиковых карт, указываются эмблемы и наименования платежных систем или кредитной организации. Данные атрибуты позволяют сформировать у потребителя ложное представление, что он находится на веб-сайте реально действующей организации.

Интересным представляется тот факт, что пользователь передает злоумышленникам не только свои персональные данные, но и данные платежной карты третьего лица, которому он осуществляет перевод.

Данные ресурсы очень заманчивы для потребителей, поскольку предлагают услуги беспроцентного перевода или перевода с низким процентом между платежными картами разных банков или платежных систем.

Чтобы не допустить использование недобросовестных ресурсов, пользователь должен проанализировать следующие критерии применительно к веб-сайту:

– наличие на веб-сайте информации об операторе платежной системы;

– наличие организации в Реестре операторов платежных систем Банка России;

– использование защищенного соединения при осуществлении перевода[25].

При этом если на ресурсе указано, что услуги предоставляются какой-либо кредитной организацией, то необходимо проверить ее наличие в соответствующем перечне Банка России.

Также можно убедиться в достоверности партнерских (договорных) отношений данного ресурса и кредитных организаций или платежных систем, позвонив на официальный контактный номер платежной системы или кредитной организации с просьбой подтвердить сотрудничество с ресурсом.

Проверка ресурсов потребителем позволит обеспечить безопасность его персональных и платежных данных.

На рис. 11 и 12 приведены примеры веб-сайтов мошеннических организаций, которые предоставляют услуги по осуществлению псевдоP2P-переводов.

[25] Более подробно процедуру выявления фиктивных кредитных организаций мы рассматривали в разделе 1.2.1 «Лжебанки». Потребителю необходимо быть бдительным и проверять не только сам веб-сайт, но и информацию об организации, предоставляющей на нем платежные услуги.

Рис. 11. Веб-сайт мошеннической организации, осуществляющей фиктивные P2P-переводы (1)

Рис. 12. Веб-сайт мошеннической организации, осуществляющей фиктивные P2P-переводы (2)

1.2.4. Схемы с использованием страхового (закрепительного) платежа

В рамках этой категории мошенничества можно выделить два подвида:

– организация проводит псевдоопросы, за которые якобы полагается выплата денежных средств;

– организация предлагает выплату несуществующей компенсации.

В первом случае пользователь проходит опрос на веб-сайте. Как правило, опрос состоит из семи-десяти простых вопросов. После прохождения опроса ресурс якобы генерирует выигрыш и предлагает пользователю перевести денежные средства на его платежную карту. Вместе с тем с целью сохранения денежных средств и оформления их вывода ресурс предлагает пользователю заплатить закрепительный платеж. Сумма платежа обычно незначительна и составляет от 250 до 1000 руб. Пользователь, воодушевленный возможностью получить крупный выигрыш, соглашается на оплату небольшой, по его мнению, суммы и переходит на страницу оплаты.

Пользователь предоставляет злоумышленникам данные карт и персональные данные, что позволяет списать денежные средства с его платежной карты.

Вместе с тем мошенники развиваются и совершенствуются. Более изощренным является второй способ мошенничества: предоставление возможности получить якобы от государства неиспользованные страховые платежи за медицинские услуги. Как правило, на ресурсе размещается фальшивая документация Правительства Российской Федерации, якобы позволяющая осуществить возврат и выплатить компенсацию населению.

На данную категорию ресурсов пользователей активно завлекают за счет звонков и SMS-рассылок, в которых граждан убеждают в том, что компенсация предоставляется в рамках одной из федеральных программ и что она не подлежит огласке общественности, поскольку существует лимит по выплатам. Злоумышленникам необходимо привлечь потребителя и убедить его зайти на ресурс. На ресурсе предлагается заполнить специальную форму якобы для определения количества денежных средств и срока уплаты в соответствующий государственный фонд. В рамках данной формы пользователь передает мошенникам свои персональные данные, в том числе иногда скан паспорта. Веб-сайт якобы генерирует компенсацию, положенную пользователю, и так же, как в ситуации с опросами, предлагает оплатить страховой (закрепительный) платеж.

На рис. 13 и 14 приведены примеры веб-сайтов организаций, которые осуществляют описанную мошенническую деятельность.

Рис. 13. Веб-сайт организации, осуществляющей псевдоопросы, за которые якобы полагается выплата денежных средств

Рис. 14. Веб-сайт организации, предлагающей выплату несуществующей компенсации

Вместе с тем необходимо обратить внимание, что опросы могут проводиться и компенсации могут выплачиваться реально действующими организациями и государственными службами. Чтобы не стать жертвой мошенников, пользователь должен обратить внимание на следующие признаки, которые чаще всего указывают на мошеннический характер ресурса данной категории:

– перечисление денежных средств третьим лицам в счет оплаты;

– отсутствие организации в Едином государственном реестре юридических лиц;

– осуществление деятельности, не предусмотренной лицензией, разрешением.

Поиск данных признаков при обращении к различным ресурсам позволит снизить риски мошеннических действий в отношении потребителей. Пользователи того или иного ресурса должны быть осмотрительными и проверять размещенную на нем информацию.

1.2.5. Схемы быстрого обогащения: «Золотой поток» (Golden Stream), «Алмазный дождь» (Diamond Rain) и др

Речь идет о всевозможных пирамидах. Как правило, все начинается с того, что на электронный адрес потенциальной жертвы приходит письмо с предложением заработать большие деньги, участвуя в игре. Например, перечислив 100 руб. (такое предложение было в игре «Золотой поток»), можно заработать 1 млн руб. всего за 90 дней[26]. В ответ на пересылку 100 руб. жертва получает какую-нибудь дополнительную информацию или программу. Далее, как обе-

[26] Все эти махинации носят название MLM-схем (Multi-Level Marketing – многоуровневый маркетинг).

щают организаторы, все зависит только от активности игрока: чтобы заработать свой миллион, он должен искать новых «участников», и чем быстрее, тем лучше.

Вариантов писем, которые начинаются с просьбы обязательно дочитать до конца и не сравнивать эту игру с другими, много. Однако принцип во всех этих схемах один: в начале игры жертва теряет некоторую сумму денег и все дальнейшие усилия тратит на компенсацию своих потерь, подыскивая новых «участников».

1.2.6. «Нигерийские письма»

Афера с «нигерийскими письмами»[27] – это современный вариант известного сотни лет назад мошенничества «Испанский узник», когда самозваные графы Монте-Кристо XVIII в., используя обычную почту, выманивали деньги у доверчивых людей, обещая им несметные сокровища, зарытые где-то в дальних странах.

Мошенники рассылают письма (в нашем случае по электронной почте, хотя может использоваться и обычная почта или факс), в которых содержится очень выгодное деловое предложение по переводу значительной суммы денег с африканского континента за рубеж под солидные комиссионные (до 40 %)[28]. От жертвы требуется совсем немного – предоставить свои личные данные в качестве гарантии сохранности денег и расчетный счет в банке для размещения средств [65].

Сценарии дальнейшего развития сюжета похожи на описанные выше. Под каким-либо предлогом мошенники просят перечислить незначительную сумму за оказание услуг. Это могут быть просьбы внести деньги на оплату услуг юриста, компенсировать стоимость пересылки каких-либо документов и т. д. Дальше злоумышленники, если у них есть необходимая информация для снятия денег со счета жертвы, опустошают ее счет, а могут и пригласить в какую-нибудь страну, где также, но уже с применением силы, отнимают все деньги.

Существует много разновидностей «нигерийской» аферы, но идея везде одна: требуется оказать помощь по переводу значительной суммы денег под очень высокий процент[29] (рис. 15).

[27] Другое распространенное название – «Афера 419» (по номеру соответствующей статьи в Уголовном кодексе Нигерии).

[28] Надо отметить, что география подобных преступлений постоянно растет. Были даже примеры, когда делили сбережения российских олигархов.

[29] Сразу хочется задать вопрос, почему обладатель такого состояния решает обратиться через интернет к незнакомцу, а не иметь дело со знакомым и проверенным человеком.

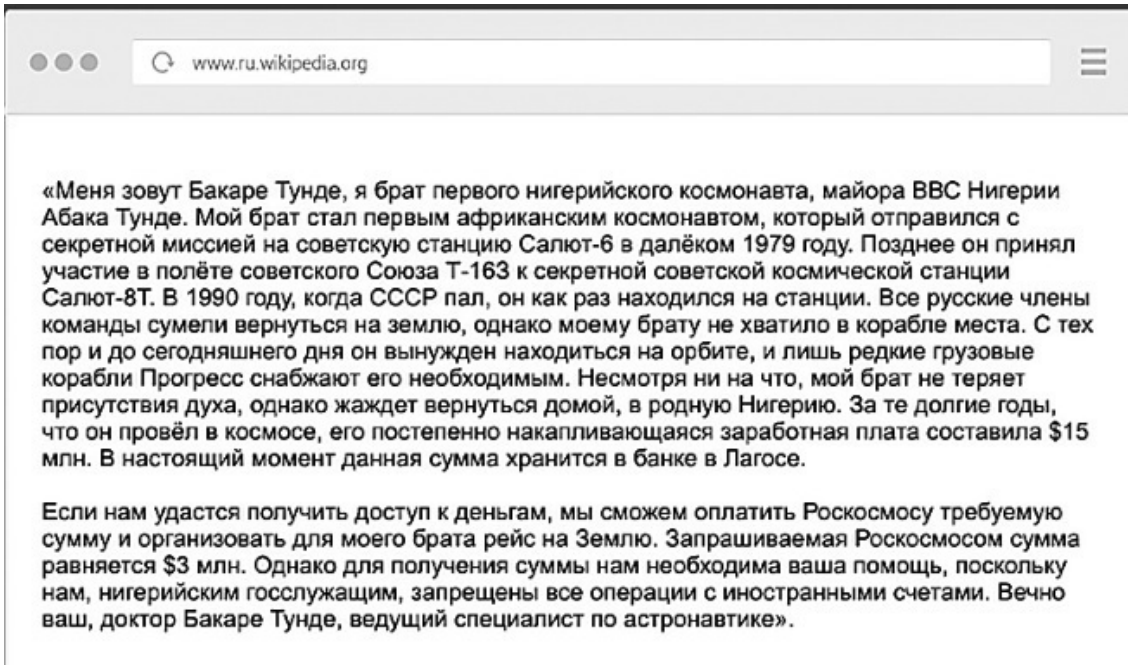


Рис. 15. Пример «нигерийского письма»

1.2.7. Опасные инвестиции

Сущность данных афер заключается в предложениях инвестировать денежные средства в какое-нибудь дело (выпуск дорогостоящего продукта, ценные бумаги и т. д.). Проценты (очень высокие), как правило, начисляются каждый день (об этом инвестор может узнать на веб-сайте инвестиционного фонда). Но как только инвестор захочет взять свои деньги, у него, как и во всех перечисленных выше случаях, возникают проблемы: веб-сайт инвестиционного фонда исчезает или становится недоступен, а адрес электронной почты (зарегистрированный на одном из бесплатных почтовых серверов) оказывается безответным (рис. 16).

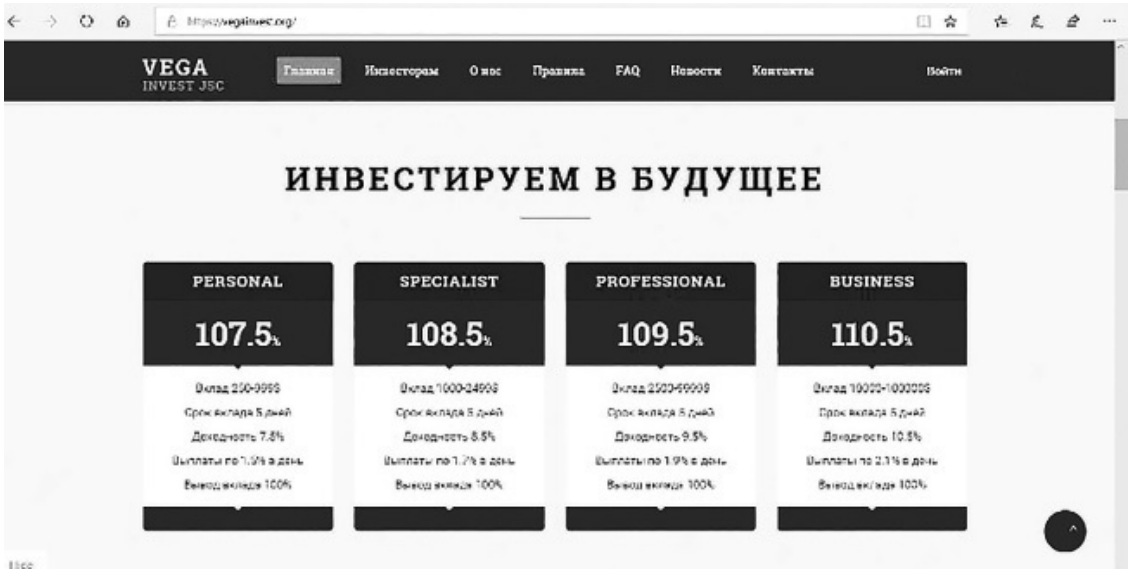


Рис. 16. Пример лжеинвестиционной компании

1.2.8. Виртуальная медицина

«Хватит переплачивать за лекарства – посетите наш магазин», – примерно такие сообщения с указанием веб-сайта приходят на многие адреса электронной почты. Практически все лекарственные препараты (более 97 %), которые реализуются через интернет-сайты, рекламируемые в спаме, являются контрафактными. Фальсифицированные таблетки производятся без надлежащего контроля качества и с нарушениями технологического процесса (при этом внешний вид и упаковка практически неотличимы от настоящих). Очевидно, что ничего кроме вреда такие препараты принести не могут.

Другой исход при обращении в подобные виртуальные аптеки – потеря денежных средств, отправленных в виде предоплаты за лекарства и доставку.

По статистике, на подобные веб-сайты заходят от 500 тыс. до 2 млн посетителей в месяц. Помимо опасности отдать преступникам свои деньги и приобрести контрафактные и некачественные лекарственные препараты здесь существует еще одна опасность. Открывая такие спам-письма, можно загрузить на компьютер вредоносную программу (червя[30], трояна[31] и др.), и в дальнейшем придется заниматься не только своим лечением, но и лечением компьютера.

1.2.9. Виртуальное трудоустройство

Организации, осуществляющие фиктивное устройство на работу, привлекают пользователей возможностью получить «легкие деньги». Пользователи, рассчитывая на быстрый заработок, передают злоумышленникам персональные данные, в том числе карточные, якобы для перечисления заработной платы. Нередки случаи, когда для «устройства на работу» предлагается оплатить страховой взнос для предоставления заказов или фиксирования выплат либо оплатить доставку трудового договора.

Интерфейс ресурсов данной категории, как правило, идентичен интерфейсу реальных ресурсов, что позволяет ввести пользователя в заблуждение относительно получения дохода (рис. 17).

[30] Червь (worm) – разновидность самовоспроизводящихся компьютерных программ, распространяющихся в локальных и глобальных компьютерных сетях. В отличие от компьютерных вирусов, червь является самостоятельной программой.

[31] Троянская программа, или троян (trojan), – разновидность компьютерных программ, которые «претендуют» на то, что выполняют определенную функцию, в действительности же работают совершенно иначе (свое название получила в честь «троянского коня»).

Рис. 17. Веб-сайт организации, осуществляющей фиктивное устройство на работу

Один из вариантов схемы – предложения работы в интернете (на дому), например «виртуальным бухгалтером». Будущему работнику предлагают заниматься определенными посредническими услугами не больше 2–3 часов в день и получать заработную плату около 400 долларов. Чаще всего работать предлагают с системой WebMoney Работодатель открывает для работника счет (кошелек) и получает для него аттестат. Владельцем счета является работодатель. Работа заключается в том, чтобы осуществлять денежные переводы (WMZ[32]). Все переводы (их бывает от 30 до 50 в день) нужно совершить в течение суток. В среднем на один перевод затрачивается 2–3 минуты. Предложение достаточно заманчивое (как, впрочем, и все те, которые были описаны выше), только работодатель просит перевести 7 долларов (7 WMZ) на получение аттестата (своего рода компенсация затрат работодателя на случай отказа работника продолжать сотрудничество).

Конечно, 7 долларов – не такая уж большая сумма, но на это и рассчитана данная афера. После того как жертва перечислит деньги на получение аттестата, связь с ней прекратится.

Кстати, если потенциальный работник представится опытным пользователем интернета, знакомым со всеми платежными системами, и сообщит, что имеет счет в платежной системе, в которой предстоит работать, а также персональный аттестат и хорошо знает, как работать с денежными переводами, то, скорее всего, мошенники сразу оставят жертву в покое. Такие «кадры» им не нужны.

Ниже приведены несколько признаков, по которым можно определить, что работу, скорее всего, предлагают мошенники:

– расплывчатые описания вакансий;
– неясные требования к работникам;
– бесплатное обучение;
– слишком высокая заработная плата;
– обширный социальный пакет;
– анонимный абонентский ящик или адрес электронной почты в качестве реквизитов;
– гарантия трудоустройства.

[32] В системе WebMoney используются различные валюты. WMZ – средства, эквивалентные долларам США.

1.2.10. Горячие торговые точки

Интернет-магазины сегодня привлекают покупателей своими ценами (за счет экономии на аренде помещений), а также возможностью удобной доставки. Но и среди них бывают магазины с такими низкими ценами, что это выделяет их из общего ряда. Причем продавец обосновывает эти цены, иногда совсем не скрывая таких фактов, как «товар краденый», «товар конфискованный» и т. п.

Поэтому если жертва и решит купить такой товар, то вряд ли потом пойдет жаловаться, так как по сути является соучастником преступления (скупка краденого).

Схема мошенничества в данном случае прежняя: как только покупатель переводит деньги на счет продавца, связь с ним прекращается (веб-сайт магазина перестает работать, электронная почта не отвечает).

В общем случае все мошеннические интернет-магазины можно разделить на два вида:

– магазины, которые продают несуществующий товар;

– магазины, которые доставляют не тот товар, который представлен на веб-сайте.

Оформление и содержание ресурса заставляют пользователя думать, что данный веб-сайт принадлежит действующей организации (рис. 18).

Рис. 18. Веб-сайт фиктивного интернет-магазина

Для того чтобы обезопасить себя, потребителю необходимо проверить информацию об организации, указанной на веб-сайте, которая предоставляет товары или услуги. Данную информацию можно проверить на официальном веб-сайте ФНС России в разделе «Единый государственный реестр юридических лиц».

1.2.11. Сетевое попрошайничество

Если раньше большинство попрошаек можно было встретить на городских площадях и вокзалах, то теперь появился целый класс сетевых попрошаек, которые обращаются за помощью посредством интернета, выпрашивая деньги под разными предлогами: на срочную и дорогую операцию, чтобы избавиться от угроз вымогателей, погасить кредит и т. п.

Можно встретить сообщения о внезапно возникших проблемах в платежной системе WebMoney[33], для решения которых администратор просит перечислить какую-то сумму на свой кошелек. Причем если клиент, к которому обращается администратор, не перечислит деньги, в дальнейшем он не сможет воспользоваться своим кошельком (т. е. своими деньгами).

К сожалению, есть случаи, когда люди, особо не вдумываясь в суть происходящего, перечисляют свои деньги и потом узнают, что обращение поступило от мошенника, а не от администратора системы WebMoney.

Пользователям можно порекомендовать ни в коем случае не перечислять свои деньги до тех пор, пока не пришло подтверждение достоверности полученного сообщения.

Пример мошеннического сообщения приведен на рис. 19.

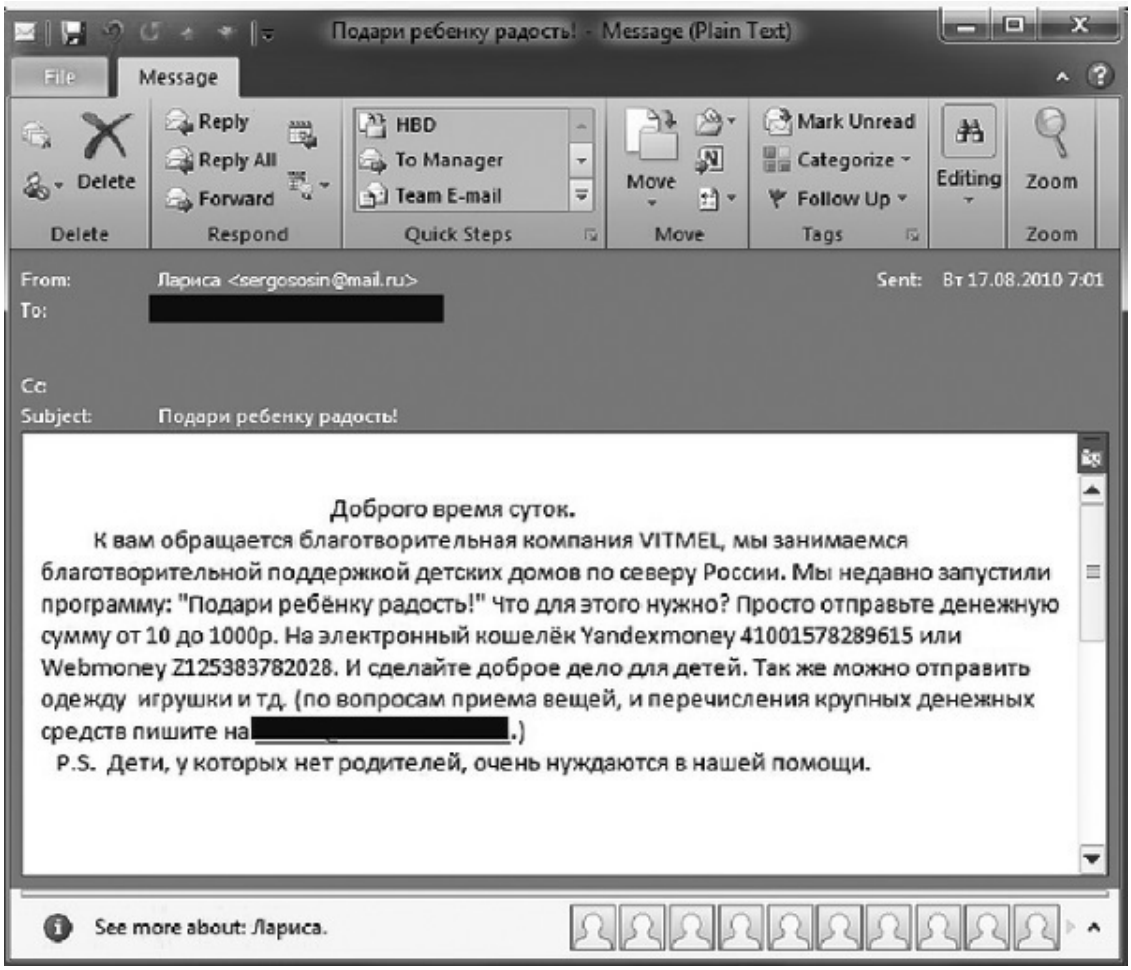


Рис. 19. Пример мошеннического сообщения

Одним из способов попрошайничества является отправка SMS якобы от родственников с просьбой перечислить денежные средства (рис. 20). В данном случае мошенники играют на чувствах потерпевших, вводят их в заблуждение. Часто в таких SMS сообщается о сложной жизненной ситуации, аварии или смерти кого-либо. Потерпевший должен быть бдительным, не поддаваться эмоциям и все проверить. При наличии возможности необходимо самостоятельно связаться с родственником, от которого якобы пришло сообщение. Следует также известить оператора связи о получении такого SMS.

[33] В последнее время в качестве причин проблем все чаще называют финансовый кризис.

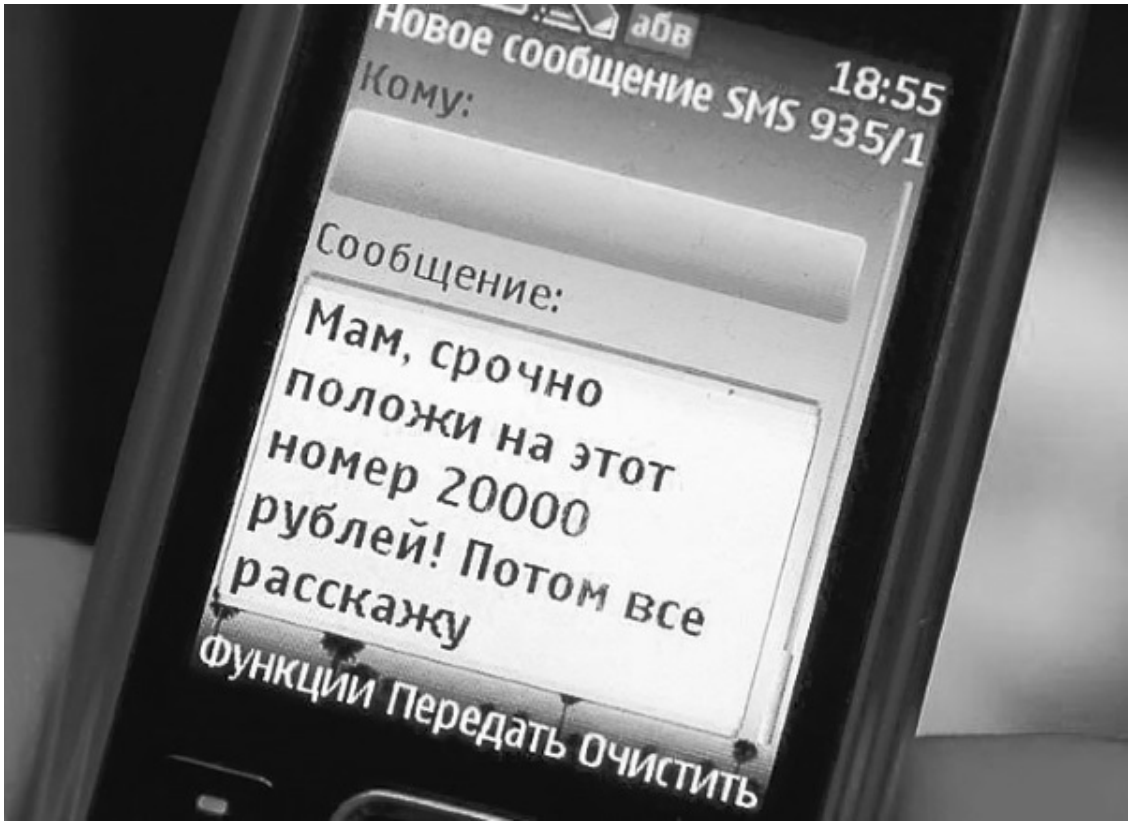


Рис. 20. Пример мошеннического сообщения, поступившего якобы от родственника

Другим распространенным видом SMS-мошенничества является направление сообщения о том, что якобы на счет мобильного телефона жертвы ошибочно перечислена некая сумма, которую необходимо вернуть (рис. 21). Потенциальный потерпевший должен проверить баланс телефона, позвонить оператору связи и уточнить данные.

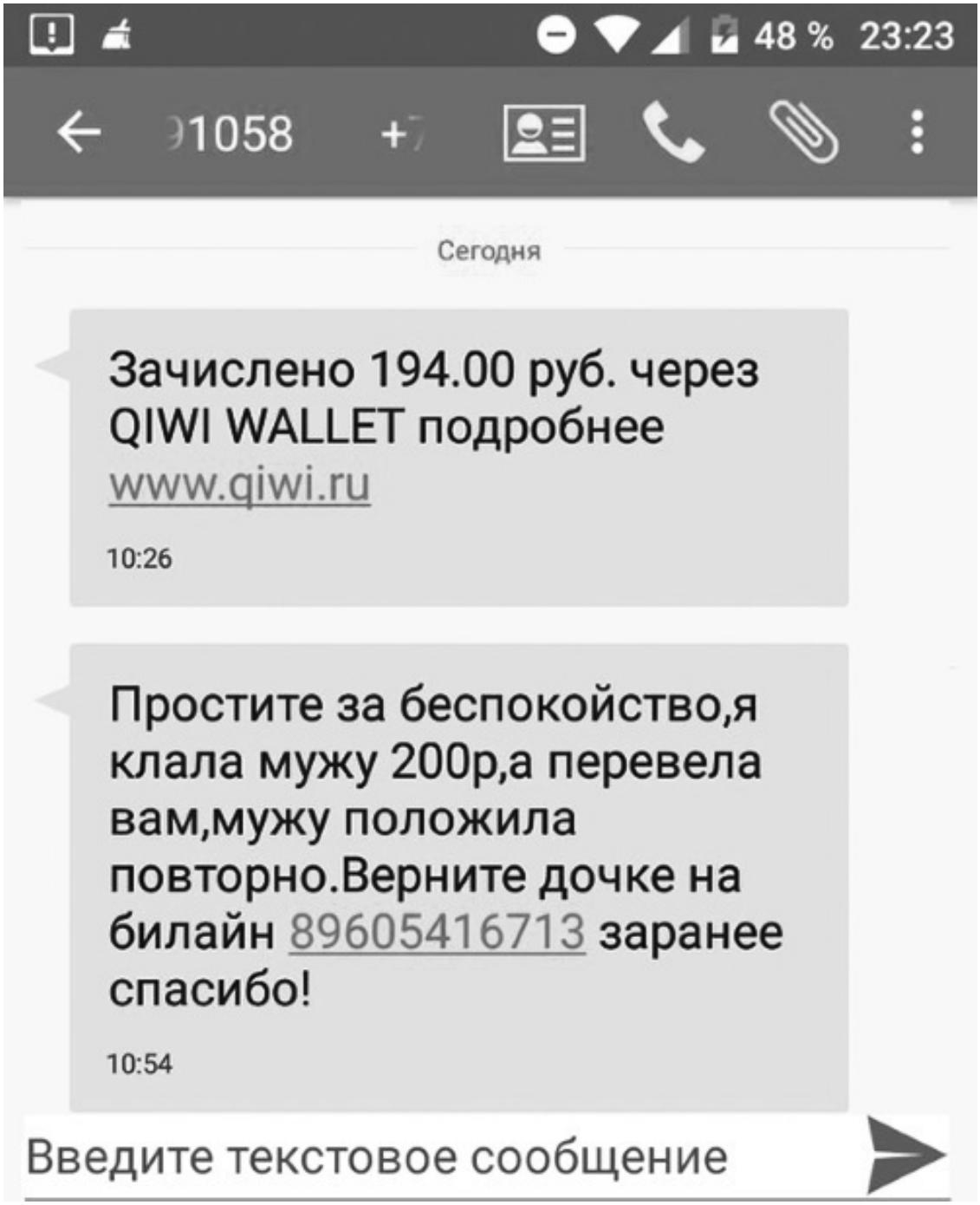


Рис. 21. Пример мошеннического сообщения о якобы ошибочном пополнении баланса телефона

1.2.12. Ботнеты[34]

Термин «бот» появился намного раньше, чем его стали использовать для обозначения компьютерного вируса и инструмента для атаки на компьютеры и сети. В IRC-сетях он до сих пор обозначает специальную программу, которая замещает собой живого человека и может поддерживать активность на IRC-канале даже в то время, когда к нему не подключен ни один из пользователей. Бот может контролировать и модерировать содержание бесед на канале, удалять

[34] Ботнет (botnet) – компьютерная сеть, состоящая из некоторого количества зараженных компьютеров (ботов).

посетителей, которые нарушают принятые правила поведения, и т. д. Это своего рода вариант искусственного разума.

Однако бот в арсенале хакера способен доставить серьезные проблемы. Хакеры могут находить через интернет незащищенные компьютеры и загружать на них специальные программы, которые будут по их команде выполнять различные действия (такие как рассылка спама или участие в DDoS-атаке[35]).

В качестве защиты от подобного заражения можно порекомендовать хороший мощный анализатор сетевого трафика, который позволит выполнять диагностику, идентификацию и перенаправление всего подозрительного интернет-трафика. Можно также использовать программное обеспечение для фильтрации пакетов, комбинируя его со специальными техническими и аппаратными средствами, которые устанавливаются между маршрутизаторами и межсетевыми экранами.

Достаточно эффективный способ решения этих проблем разработало правительство Австралии. Во взаимодействии с пятью крупнейшими интернет-провайдерами страны оно создало технологию и программу для своевременного обнаружения компьютеров-зомби и принятия оперативных мер по их блокировке. В большинстве случаев владельцы своих компьютеров даже не представляли, что участвовали в DDoS-атаке или что с их IP-адреса рассылался спам.

1.2.13. Сетевые банды

Одной из тенденций сегодняшнего дня является заметный рост числа новых компьютерных вирусов, червей и троянских программ. Троянские программы не могут рассылать себя по интернету самостоятельно, подобно компьютерным вирусам, так что масштабы их распространения должны быть меньше, чем у вирусов. Но на самом деле троянских программ и пораженных ими компьютеров с каждым годом становится все больше. Специалисты компании Sophos[36] сделали вывод, что такая ситуация стала следствием активности профессиональных преступников.

Криминальные группы, которые ранее занимались исключительно мошенничеством с банковскими картами, начали объединяться и все более тесно сотрудничать с создателями компьютерных вирусов, спамерами и группами безжалостных хакеров.

Приведенные примеры мошенничества в интернете ни в коем случае нельзя считать исчерпывающим перечнем ухищрений компьютерных злоумышленников.

К сожалению, во всемирной паутине, которая по своей сути является неуправляемой средой, постоянно возникают все новые и новые угрозы со стороны хакеров.

И от того, насколько своевременно будет построена защита от этих угроз, зависит доверие клиентов кредитных организаций к технологиям ДБО (включая СЭБ).

В условиях ДБО кредитные организации вынуждены существенно повышать уровень обеспечения информационной безопасности, так как основные атаки киберпреступников направлены именно на тех клиентов банков, которые осуществляют свои операции удаленно (т. е. вне офиса).

Очевидно, что абсолютной защиты от угроз для ДБО не существует. Компьютерные злоумышленники в состоянии взломать практически любую систему[37].

---

[35] DoS-атака (от англ. *Denial of Service* — отказ в обслуживании) и DDoS-атака (от англ. *Distributed Denial of Service* — распределенный отказ в обслуживании) – разновидности атак на вычислительную систему. Цель этих атак – довести систему до отказа, то есть создать такие условия, при которых легитимные (правомерные) пользователи системы не могут получить доступ к предоставляемым системой ресурсам либо этот доступ затруднен.

[36] Компания Sophos является одним из мировых лидеров в области решений для информационной безопасности.

[37] Кроме того, сами банки иногда используют недостаточно надежные системы ДБО.

Однако непрерывная работа по поддержанию достаточного уровня информационной безопасности может сильно осложнить и (или) свести к минимуму возможности кибермошенников.

Масштабы кибермошенничества заставляют серьезно относиться к данному виду преступлений. Так, например, в июне 2012 г. новостные агентства распространили информацию о задержании преступной группы, включая ее организатора[38], который вместе со своими сообщниками похитил из систем ДБО более 150 млн руб.

По словам генерального директора компании Group-IB[39] Ильи Сачкова, принимавшего участие в расследовании деятельности данной преступной группы, это самая большая по численности участников киберпреступная группировка в России из тех, о которых известно специалистам по информационной безопасности[40]. В течение 2011 г. работала целая группа технических специалистов: заливщиков (распространителей вредоносного программного обеспечения), специалистов по шифрованию, администраторов, обслуживавших ботсети, и других.

На протяжении последних нескольких лет, по данным Group-IB, мошенники использовали зарекомендовавшую себя в хакерских кругах троянскую программу Carberp[41].

Обобщая наиболее распространенные схемы совершения киберпреступлений в системах ДБО, можно выделить два способа.

Если сумма украденного составляет не более 1–1,5 млн руб., то деньги выводят сразу на пластиковые карты так называемых дропов (специально нанятых владельцев банковских карт, которые занимаются обналичиванием похищенных денег). Обычно в течение 15 минут после того, как деньги поступили на карточные счета, дропы обналичивают их через банкоматы и затем отдают своим нанимателям (рис. 22).

---

[38] Более известен во всемирной сети под псевдонимами Гермес и Араши.

[39] Group-IB – международная компания, лидер российского рынка по оказанию полного комплекса услуг в области расследований инцидентов информационной безопасности и компьютерных преступлений: начиная от оперативного реагирования на инцидент и заканчивая постинцидентным консалтингом (официальный веб-сайт компании: http://www.group-ib.ru).

[40] Подробнее см. интервью Ильи Сачкова для РИА Новости: Хакер, укравший 150 млн рублей, работал с 25 сообщниками // Прайм. Бизнес-лента 22 июня 2012 г.; Гендиректор Group-IB: у хакеров есть несколько собственных платежных систем // ПЛАС-daily 19 июля 2012 г.

[41] Carberp – распространенная среди киберпреступников вредоносная программа. Она собирает информацию о пользователе и системе и отправляет ее на сервер злоумышленников. Также бот может делать снимки экрана, перехватывать нажатия клавиш, содержимое буфера обмена с отправкой на сервер. Троян имеет возможность самоудаления, установки дополнительных вредоносных модулей, кражи цифровых сертификатов для популярных систем ДБО.

Рис. 22. «Простая» схема – примерно до 1,5 млн руб.

Если суммы крупнее, используются более сложные схемы обналичивания. Они применяются обычно при хищении средств в объеме от 1 до 5 млн руб.

В этом случае деньги предварительно переводят на счет юридического лица. Дальше сумму могут раздробить и распределить по другим счетам, чтобы сильнее запутать следы (рис. 23).

Группы мошенников, специализирующиеся на обналичивании, оставляют себе минимум 50 %.

Такой большой процент объясняется тем, что хищению предшествует длительный период подготовки. «Обнальщики» и похитители договариваются заранее.

К моменту хищения у «обнальщиков» уже все готово: создано подставное юридическое лицо, открыт счет в банке и выпущены карты, которые раздали дропам.

Современные условия позволяют любому юридическому лицу удаленно создать «зарплатный проект». Условно говоря, представитель компании сообщает в банк: у нас работает 15 человек, нам нужны зарплатные карты.

Рис. 23. «Сложная» схема – примерно до 5 млн руб.

Далее банку предоставляются паспортные данные «сотрудников», и тот выпускает карты. Паспортные данные берутся у тех же дропов или покупаются на хакерских форумах.

Кибермошенники чаще прибегают к помощи «обнальщиков», чем самостоятельно разворачивают дроп-проекты[42].

В последнее время участились кражи из электронных платежных систем. Схемы примерно те же, только деньги выводятся либо на другие кошельки, либо опять же на банковские карты.

Исходя из проведенного нами исследования, можно сформулировать следующие общие рекомендации для граждан:

– быть бдительными и проверять не только веб-сайты организаций, предоставляющих финансовые услуги, но и информацию, получаемую в SMS;

– не сообщать свои персональные данные, в том числе карточные данные, неизвестным третьим лицам;

– не переводить денежные средства в пользу третьих лиц без соответствующей проверки информации;

– если денежные средства все-таки похищены, незамедлительно сообщить в уполномоченные организации (в полицию, банк, оператору связи и т. д.).

Только бдительность и применение мер безопасности могут уберечь от хищений денежных средств.

[42] Главари организованных преступных группировок с большим интересом участвуют в таких махинациях, поскольку хакеры готовы отдавать до 50 % украденных денег.

1.3. Актуальные направления регулирования в условиях электронного банкинга

Никакой транспорт не будет попутным, если не знаешь, куда идти.
Эдгар Аллан По, американский писатель, поэт, эссеист, литературный критик и редактор

Распределение ответственности в сфере применения технологий ДБО в связи с вступлением в действие ст. 9[43] Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе» [51] – наиболее острый вопрос, требующий доработки и четкого понимания обеими сторонами (банками и их клиентами). В действующей редакции большая часть ответственности переходит на кредитные организации, поэтому становятся понятны их многочисленные обращения к регулятору с просьбой выстроить сбалансированную справедливую систему, в которой все участники защищены и имеют возможность получить необходимую информацию.

Суть обращений сводится к тому, что каждая из сторон должна нести ответственность за свои действия (или бездействие) в пределах, не превышающих ее физические возможности, а также не должна допускать неотвратимого и безнаказанного причинения ущерба другой стороне.

Напомним, что коммерческие банки, работая в условиях жесткой конкуренции, не заинтересованы расходовать на обеспечение информационной безопасности больше средств, чем конкуренты. Информационная безопасность всегда связана с затратами для кредитных организаций, неудобствами для банковского персонала и клиентов. Что касается клиентов, то они обращают больше внимания на удобство банковских услуг, чем на их безопасность.

Поэтому кредитным организациям нужен разумный компромисс, который строится на нескольких базовых принципах организации информационной безопасности:

– стоимость защиты не должна превышать стоимости защищаемых информационных ресурсов;

– банк и клиент должны выйти на такой уровень защиты транзакций, когда для клиента защита еще удобна и приемлема по стоимости, а злоумышленнику уже невыгодно совершать преступление из-за высоких расходов на преодоление защиты.

Наряду с очевидными преимуществами СЭБ принесли в банковский бизнес дополнительные риски (рис. 24). А если говорить точнее, то количество типичных банковских рисков[44] осталось прежним, а вот их техническая составляющая значительно возросла.

[43] Вступила в действие с 1 января 2014 г.

[44] Перечень типичных банковских рисков приведен в Письме Банка России от 23.06.2004 № 70-Т «О типичных банковских рисках».

Рис. 24. Дополнительные источники банковских рисков в условиях применения СЭБ

Непрерывность выполнения банковских операций стала во многом зависеть:

– от различных сбоев в аппаратно-программном обеспечении (АПО) СЭБ;

– качества и надежности каналов связи;

– наличия резервных источников электропитания;

– качества архивации данных об операциях с использованием СЭБ;

– недостатков в обеспечении информационной безопасности конфиденциальных сведений.

Однако необходимо хорошо понимать, что, применяя современные технологии и средства, мы можем осуществить те или иные процедуры удобнее, быстрее и в гораздо больших объемах, но при этом не надо рассчитывать на чудеса – за все надо платить. И если регулирование в области ДБО (включая услуги ЭБ) будет отставать от появления и распространения новых источников типичных банковских рисков, то «удобнее, быстрее и в больших объемах» в целом будет дороже. В первую очередь возрастают затраты на обеспечение безопасности данного способа оказания банковских услуг, так как кредитные организации будут вынуждены учитывать не только внутрибанковские риски, но и риски, возникающие на стороне клиента и различных провайдеров (например, интернет-провайдеров в случае интернет-банкинга, сотовых операторов в случае мобильного банкинга)[45].

По мнению авторов, на сегодняшний день есть четыре причины, по которым применение СЭБ нуждается в дополнительном регулировании:

1) расширение профиля операционного риска в условиях ЭБ;

2) значительный рост числа киберпреступлений в финансовой сфере (включая хищения денежных средств в СЭБ);

[45] Следует отметить, что риски, возникающие на стороне различных провайдеров услуг и сотовых операторов, сотрудникам кредитных организаций весьма затруднительно (а в ряде случаев невозможно) контролировать.

3) использование СЭБ в схемах, направленных на легализацию преступных доходов (или, другими словами, отмывание денег);

4) недостаточная подготовка сотрудников коммерческих банков по вопросам обеспечения информационной безопасности и управления сопутствующими рисками в условиях ЭБ.

Рассмотрим каждую из выделенных проблем более подробно.

1.3.1. Управление операционным риском

Причиной повышенного внимания к операционному риску стал выход соглашения Базельского комитета по банковскому надзору (БКБН) «Международная конвергенция измерения капитала и стандартов капитала: новые подходы» – Basel II. Соглашение Basel II является одним из наиболее актуальных нормативных актов, регулирующих банковский сектор. Оно предъявляет требования к минимальному размеру банковского капитала, на основании которых кредитные организации обязаны оценивать операционные, рыночные и кредитные риски, а также резервировать капитал на их покрытие.

Basel II трактует операционный риск как риск убытков, возникающий в результате неадекватных или ошибочных внутренних процессов, действий сотрудников и систем или в результате внешних событий.

В качестве возможных проявлений операционного риска можно выделить следующие типы событий:

– внешние воздействия (наводнения, пожары, аварии и т. п.);
– внутренние и внешние мошенничества;
– ошибки персонала;
– сбои в реализации бизнес-процессов и обслуживании клиентов;
– физический ущерб активам;
– сбои информационных систем;
– нарушение процессов обработки и хранения данных.

Требования, предъявляемые документами Basel II, были дополнены в документах Basel III, в том числе и в отношении операционного риска.

Отметим, что БКБН рекомендует привлекать к процессу управления рисками, возникающими при внедрении СЭБ в кредитных организациях, не только риск-подразделения, но и совет директоров, высшее руководство банка, а также топ-менеджеров банка.

Операционный риск является одним из основных типичных банковских рисков, на который в большей степени оказывают влияние СЭБ.

Он определяется как вероятность образования убытков и (или) неполучения прибыли вследствие сбоев в выполнении каждодневных, рутинных банковских операций. Применительно к ЭБ выделяются три главные зоны операционного риска:

1) функционирование системы безопасности;

2) привлечение сторонних организаций к предоставлению некоторых видов электронных банковских услуг (аутсорсинг);

3) освоение новых технологий сотрудниками банка [78, с. 499].

В первом случае речь идет о том, что возможны нарушения в процессах электронного хранения, передачи и обработки информации (искажение, уничтожение, перехват данных или злоупотребление ими в результате технических неполадок, действий хакеров, ошибок или мошенничества персонала и клиентов) и отказы в функционировании банковских информационных систем (возникновение перегрузок из-за недостаточной мощности аппаратно-программного обеспечения и целенаправленных DoS-атак на веб-серверы банка).

Вторая потенциально подверженная операционному риску сфера становится в последнее время весьма значимой. Предоставление банковских услуг в области информационных техно-

логий посредством специализированных фирм (в первую очередь банки сотрудничают с компаниями по разработке прикладных программ) позволяет сократить инвестиционный бюджет и избежать найма дорогостоящих специалистов, что особенно важно для небольших финансовых учреждений. В то же время банки оказываются в определенной степени зависимыми от подобных партнеров, а общий уровень банковского обслуживания начинает определяться результатами работы нескольких, нередко никак не связанных между собой, компаний, сотрудники которых могут и не обладать достаточными знаниями о специфике банковского дела.

Наконец, ускорение процесса модернизации информационных систем повышает требования к адаптационным способностям персонала банков и увеличивает опасность возникновения трудностей при переходе ко все более сложным интегрированным электронным решениям. Довольно часто внедрение более «умной» и производительной технологии оборачивается для работников и клиентов банков значительными проблемами[46].

Смысл управления операционным риском заключается в прогнозе периодичности различных сбоев и нарушений непрерывности функционирования аппаратно-программного обеспечения СЭБ и оценке величины вероятных убытков. Отметим, что у потерь есть и положительная сторона – они вскрывают слабые места и открывают новые возможности. Поэтому самая большая ошибка – сокрытие нежелательного инцидента. Даже после того, как устранены рисковая ситуация или последствия неблагоприятного события, нельзя оставлять произошедшее в тайне: гораздо лучше использовать инцидент в качестве наглядного урока для других сотрудников.

Формы проявления операционного риска в условиях ЭБ могут быть самыми разнообразными. Однако все они вызваны, как правило, несоответствием определенных процедур требованиям законодательства, несоразмерностью технических возможностей СЭБ и объема бизнеса, техническими сбоями и отказами оборудования, непреднамеренными или умышленными действиями персонала и внешних субъектов, что отвечает классическому определению операционного риска.

Минимизировать операционный риск в условиях ЭБ можно с помощью общепринятых стратегий:

– принятие риска (отказ от превентивных мероприятий, воздействие на источники риска, самострахование (в т. ч. через кэптивные страховые компании), диверсификация активов и т. д.);

– полная или частичная передача риска (страхование, хеджирование, синдицирование и т. п.);

– избежание риска (отказ от применения конкретной системы, профилактика как устранение источников риска и пр.).

1.3.2. Противодействие киберпреступлениям в финансовой сфере

Следующая проблема связана с возрастанием активности киберпреступников, чьи усилия направлены на хищение денежных средств клиентов банков, использующих для выполнения своих операций СЭБ.

На конец 2019 г. было известно об активности 38 групп, кампании которых затрагивают все регионы мира. Аналитики Group-IB изучают в основном группы из России, Северной Кореи, Пакистана, Китая, Вьетнама, Ирана, США, ОАЭ, Индии, Турции, региона Южной

[46] В основном это связано с обучением персонала и совершенствованием методик проведения проверок специалистами риск-подразделений и служб внутреннего контроля.

Америки. К 2022 г., по прогнозу Всемирного экономического форума, сумма планетарного ущерба от кибератак вырастет до $8 трлн[47].

По статистике компании Group-IB, объем российского рынка киберпреступности во второй половине 2018 г. – первой половине 2019 г. составил почти 510 млн руб. (примерно $8 млн; снижение на 85 % к прошлому периоду)[48]. Из отчета МВД России «Состояние преступности в России»[49] следует, что за январь-октябрь 2019 г. в стране было зарегистрировано 2376 преступлений в сфере компьютерной безопасности.

Компьютерные злоумышленники сегодня совсем не похожи на тинейджеров, получивших первоначальные знания с хакерских веб-сайтов, а представляют собой специалистов с достаточно высокой подготовкой в области информационных технологий и в финансовых вопросах. Причем большинство из них действуют в составе организованных преступных групп. Сегодня доходы от компьютерных преступлений значительно превышают доходы, получаемые от продажи оружия и наркотиков.

Очевидно, что в будущем угрозы не станут проще. Уже сегодня многие атаки – это комбинации различных методик. Использование только традиционных систем, таких как сигнатурные антивирусы, не дает возможности адекватно защищаться от современных типов атак. Кредитные организации, которые защищаются только от известных угроз, всегда рискуют, поскольку атакующие продолжают создавать новые техники атак.

1.3.3. Противодействие использованию систем электронного банкинга в схемах, направленных на легализацию преступных доходов

Следующая проблема, связанная с применением СЭБ, заключается в активном привлечении данных систем к процессу легализации преступных доходов. В последнее время отмывание денег стало одной из основных международных проблем, к решению которой привлечены ведущие страны мира. Процедура отмывания денег имеет решающее значение для функционирования практически всех форм транснациональной и организованной преступности. Различные меры экономического характера, призванные исключить или ограничить возможность использования преступниками полученных незаконными путями доходов, представляют собой важнейший и действенный компонент программ по борьбе с преступностью. Приведем лишь некоторые факторы, способствующие отмыванию денег:

– высокая доля неофициальных доходов населения и бизнеса (существование параллельной экономики и (или) «черного рынка»);

– несовершенство механизмов контроля и мониторинга деятельности кредитных организаций;

– несоблюдение международных стандартов регулирования финансовой деятельности, разработанных специализированными международными организациями;

– распространение коррупции в различных органах власти;

– законодательное закрепление тайны финансовых операций;

– широкое использование предприятиями и банками операций с вовлечением офшорных компаний и др.

---

[47] Потери компаний от кибератак в мире в 2019 г. могут достигнуть $2,5 трлн. URL: https://www.kommersant.ru/doc/3957187.

[48] Hi Tech Crime Trends 2019/2020. URL: https://www.group-ib.ru/resources/threat-research/2019-report.html.

[49] Краткая характеристика состояния преступности в Российской Федерации за январь-октябрь 2019 г. URL: https://мвд.рф/reports/item/19007735/.

Как правило, в процесс отмывания денег включается целый ряд операций, направленных на сокрытие источника финансовых активов, но все они входят в одну из трех составляющих (стадий) обобщенной модели отмывания денег: размещение (placement), расслоение (layering) или интеграцию (integration). Указанные стадии могут быть пройдены одновременно или частично накладываться друг на друга в зависимости от выбранного механизма легализации и от требований, предъявляемых преступной организацией.

На стадии размещения необходимо изменить форму денежных средств с целью сокрытия их нелегального происхождения. Например, поступления от незаконной торговли наркотиками чаще всего представляют собой мелкие купюры. Конвертирование их в более крупные купюры, чеки или иные финансовые документы часто производится с помощью предприятий, имеющих дело с большими суммами наличных денег (рестораны, гостиницы, казино, автомойки) и используемых в качестве прикрытия.

На стадии расслоения лица, отмывающие деньги, стараются еще больше скрыть следы, по которым их могут обнаружить. Для этого одни сложные финансовые сделки наслаиваются на другие. Например, для отмывания больших денежных сумм создаются фиктивные компании в странах, отличающихся строгими законами о банковской тайне или слабыми механизмами обеспечения соблюдения законодательных положений, касающихся отмывания денег. Затем «грязные» деньги переводятся из одной фиктивной компании в другую до тех пор, пока не приобретут видимость законно полученных средств [100, с. 106].

На этой стадии активно используются СЭБ (рис. 25).

На стадии интеграции преступник пытается трансформировать доходы, полученные от противозаконной деятельности, в средства, внешне имеющие легальное происхождение (деньги обычно вкладываются в бизнес, недвижимость, драгоценности и др.).

Рис. 25. Обобщенная схема отмывания денег с использованием СЭБ

Поскольку процесс отмывания денег в определенной степени базируется на используемых преступником финансовых системах и операциях, выбор конкретных механизмов ограничивается лишь его изобретательностью. Деньги отмываются через валютные и фондовые биржи, торговцев золотом, казино, компании по продаже автомобилей, страховые и торговые компании. Частные и офшорные банки, подставные корпорации, зоны свободной торговли, электронные системы и торгово-финансовые учреждения – все эти структуры могут скрывать незаконную деятельность. Далее приведем наиболее распространенные негативные последствия отмывания денег:

1. Удар по репутации банков. Бесконтрольное отмывание денег способно негативно влиять на курсы валют и процентные ставки вследствие высокой интеграции фондовых рынков. Эти деньги могут поступать в глобальные финансовые системы и подрывать экономику и валюту отдельных стран. Нужно учитывать, что проведение банковских операций через интернет позволило значительно сократить время на осуществление различных платежей.

2. Подрыв целостности финансовых рынков. Кредитные организации, полагающиеся на доходы от преступных деяний, сталкиваются с дополнительными трудностями. Например, крупные суммы отмытых денег могут поступить в банк и затем внезапно бесследно исчезнуть через электронные переводы в ответ на такие нерыночные факторы, как операции правоохранительных органов.

3. Утрата контроля над экономической политикой. В некоторых странах с формирующейся рыночной экономикой незаконные доходы могут намного превосходить государственные бюджеты, что приводит к утрате правительственного контроля над экономической политикой. В ряде случаев огромная база активов, накопленная за счет отмытых денег, может использоваться для спекулятивной скупки рынков или даже целой экономики небольшой страны.

4. Экономические деформации и нестабильность. Лица, отмывающие деньги, заинтересованы не столько в извлечении прибыли, сколько в защите доходов, поэтому направляют свои средства в области, не обязательно приносящие экономическую выгоду той стране, в которой они размещены.

5. Потеря доходов. Отмывание денег снижает налоговые доходы правительства и тем самым наносит косвенный ущерб честным налогоплательщикам (затрудняется государственный сбор налогов). Такая потеря доходов означает более высокие ставки налогообложения по сравнению с нормальной ситуацией, при которой доходы были бы законными и облагались налогами.

6. Риск для программ приватизации. Отмывание денег угрожает стремлению многих стран реформировать свою экономику путем приватизации. Преступные организации располагают финансовыми средствами, позволяющими приобретать по более высоким ценам предприятия, прежде находившиеся в государственной собственности.

7. Социальные издержки. Отмывание денег ведет к росту государственных расходов на правоохранительные органы (создание специализированных подразделений) и здравоохранение (например, лечение наркотической зависимости).

В целом отмывание денег ставит перед мировым сообществом сложную задачу, постоянно приобретающую новые формы. Характер процессов требует разработки глобальных стандартов и международного сотрудничества для уменьшения возможности преступников осуществлять свою деятельность.

Регулирующие органы рекомендуют банкам эффективнее использовать все ресурсы для выявления сомнительных операций, направленных на отмывание денег. Меры по предотвращению отмывания денег предпринимаются банками не только в соответствии с требованиями законодательства, но и в собственных интересах [97, с. 32].

В рамках проведения **процедур идентификации клиентов** кредитным организациям следует:

– разработать и внедрить комплексные процедуры, связанные с открытием счетов, установлением кредитных и других деловых взаимоотношений, а также совершением операций с лицами, не имеющими счетов;

– иметь данные о действительной личности клиента, пользующегося услугами банка, в том числе о подлинном владельце счета, открытого на другое имя;

– подвергать проверке данные, удостоверяющие личность, во избежание открытия счетов фиктивным пользователям;

– располагать данными о роде занятий или профессиональной деятельности клиента, об источниках его доходов, состояния или активов, а также о конкретном источнике денежных средств, вовлеченных в совершаемые через банк операции;

– знать цель, с которой открывается счет, и иметь представление о типах операций, в которые обычно вовлечен данный клиент. При открытии счета сотрудники банка должны понимать, нужно ли отнести клиента к категории высокого риска, требующей повышенного внимания.

В рамках выполнения **процедуры мониторинга** кредитным организациям следует:

– иметь внутренние системы для идентификации и мониторинга операций, вызывающих подозрения;

– оценивать риск, исходя из конкретных видов счетов, регионов и операций;

– обращать внимание на случаи превышения установленного денежного порога депозитов при открытии счета, а также на ежемесячные телеграфные переводы, операции с наличностью, дорожными чеками, получение кредитов и заключение сделок (включая покупку и продажу валют, опционов и драгоценных металлов) и т. п.;

– обращать внимание на усиление активности по банковским счетам, особенно тем, которые могут стать объектами сомнительных операций (офшорные и корреспондентские счета, счета небанковских финансовых институтов, политических деятелей и др.);

– установить пороговые размеры сделок и время от времени проверять их адекватность.

Отдельно следует отметить роль топ-менеджеров кредитных организаций. Они должны стремиться к постановке и практической реализации задач в области предотвращения незаконных операций и демонстрировать, что банк как субъект корпоративной культуры заботится о своей репутации не меньше, чем о прибылях, маркетинге и качестве обслуживания клиентов.

Топ-менеджерам кредитных организаций необходимо хорошо представлять, что клиенты коммерческих банков, использующие для выполнения своих операций СЭБ и занимающиеся противоправной деятельностью, могут не только нанести удар по репутации банка, но и создать для него серьезные осложнения во взаимоотношениях с регулирующими органами, вплоть до отзыва лицензии на осуществление банковских операций.

1.3.4. Подготовка сотрудников коммерческих банков по вопросам обеспечения информационной безопасности

Четвертая область связана с совершенствованием профессиональной подготовки персонала банка (включая сотрудников служб внутреннего контроля) по вопросам обеспечения информационной безопасности. Учитывая заметное увеличение источников банковских рисков, основу которых составляют особенности функционирования СЭБ, специалистам коммерческих банков, в чьи функции входит управление рисками, необходимо иметь не только экономическое или юридическое, но и техническое образование, позволяющее достаточно уверенно ориентироваться в особенностях функционирования различных технологий ДБО.

Ненадлежащее обеспечение информационной безопасности СЭБ (в частности, продажа населению слабо защищенных финансовых услуг) ведет к созданию предпосылок для хищения денежных средств и финансирования криминала. Существующая динамика развития современных процессов, связанная с ростом технических возможностей, способна многократно увеличить объемы финансирования криминала. Если допустить рост хищений в больших объемах (что приведет к соизмеримости объема хищений с объемами денежных средств в госсекторе), это может быть серьезной угрозой экономической безопасности страны.

2. Кибербезопасность в условиях применения систем электронного банкинга

Кольчуга не слишком защищает от стрелы, особенно если та нацелена вам между глаз.
Терри Пратчетт, английский писатель

2.1. Парадигмы построения системы кибербезопасности

Добрые нравы имеют большую силу, чем хорошие законы.
Публий Корнелий Тацит, древнеримский историк

В современном обществе интернет и сотовая связь стали привычными каналами предоставления информационных услуг. В банковской сфере эти два способа связи легли в основу ЭБ, который является лидером среди технологий ДБО. СЭБ фактически переместили весь процесс взаимодействия кредитных организаций с клиентами в виртуальное пространство, или, другими словами, киберпространство.

Внедрение СЭБ не только значительно сокращает операционные издержки, но и является одним из основных конкурентных преимуществ кредитных организаций. В то же время, перенося бизнес в киберпространство, кредитные организации не освобождаются от ответственности за качество предоставления финансовых услуг и должны в полной мере осознавать, что сегодня компьютерные атаки кибермошенников направлены в первую очередь на СЭБ с целью кражи денег со счетов как банков, так и их клиентов.

Если рассматривать информационный контур банковской деятельности, формируемый в условиях применения СЭБ, то наиболее слабым звеном является клиент. АПО СЭБ достаточно хорошо защищено на стороне банка, но не на стороне клиента. Поэтому взломать современные системы защиты, используемые кредитными организациями, намного сложнее, чем получить доступ в личный кабинет клиента.

К основным факторам, сдерживающим развитие ДБО, можно отнести отсутствие доверия клиентов к технологиям ДБО из-за роста компьютерных атак на СЭБ (в т. ч. с использованием социальной инженерии) и низкий уровень финансовой грамотности клиентов (включая недостаточную информированность о возможностях современных технологий ДБО и способах обеспечения кибербезопасности).

Повышение уровня финансовой грамотности населения – это задача, которая должна решаться комплексно. Во многих странах с основами кибербезопасности начинают знакомить еще в начальной школе, а в университетах этот предмет является обязательным – в информационный век не может быть другого подхода.

Следует принимать во внимание, что уровень финансовой грамотности населения всегда будет уступать уровню и скорости развития мошеннических технологий. Поэтому разработчики АПО СЭБ изначально должны ориентироваться на «среднего» пользователя и обеспечивать максимальную защиту от внешних воздействий.

Минимизировать риски «успешного» воздействия компьютерных атак можно с помощью построения комплексной системы кибербезопасности в кредитно-финансовой сфере.

В основе такой системы безопасности может лежать одна из двух парадигм: парадигма защищенности или парадигма развития.

Парадигма защищенности предполагает, что основу обеспечения безопасности составляет борьба с опасностями (угрозами). Менталитет защищенности приводит к отождествле-

нию безопасности с жизнедеятельностью, вследствие чего идея безопасности ставится во главу угла всей деятельности.

Необходимой предпосылкой обеспечения безопасности в рамках данной парадигмы является определение угроз безопасности, на устранение которых и направляется соответствующая деятельность, прежде всего специальных служб[50].

Парадигма развития базируется не столько на борьбе с опасностями, сколько на развитии собственных внутренних сил. И потому опасность представляет собой не только то, что отрицает существование объекта, но и прежде всего то, что угрожает его самоутверждению [69, с. 154].

В настоящее время наблюдается устойчивая тенденция смещения акцентов в деятельности по обеспечению безопасности с парадигмы защищенности на парадигму развития. Появилось понятие «безопасность через развитие». Его суть заключается в том, что обеспечение безопасности все в большей степени осуществляется через развитие и все в меньшей – через защиту[51].

Система не может быть жизнеспособной, только сохраняя достигнутое, без изменений и развития, поэтому следование исключительно парадигме защищенности в действительности не укрепляет безопасность, а постепенно разрушает объект, так как он не развивает свои внутренние силы, а лишь противостоит опасностям. И наоборот – только самоутверждение, постоянное изменение без сохранения основы системы ставят под удар существование последней. Таким образом, парадигмы защищенности и развития должны не исключать, а дополнять друг друга. Именно такого подхода необходимо придерживаться при построении комплексной системы кибербезопасности в кредитно-финансовой сфере.

Очевидно, что большая работа должна быть проведена регулятором. Как минимум он должен обеспечить определение необходимых условий ведения банковского бизнеса в киберпространстве и разработать рекомендации по снижению рисков для кредитных организаций.

В условиях применения СЭБ в ряде случаев в пользу киберпреступников работают:

– стремительная скорость устаревания техники. Именно поэтому многие успешные компьютерные атаки реализовываются при запуске новых банковских сервисов (речь идет об атаках «нулевого дня» – когда атака уже реализуется, а противоядие еще не найдено; такие атаки наносят самый большой вред);

– безграничность интернета и неадекватность нормативно-правовой базы, регулирующей информационные потоки. В связи с этим чрезвычайно сложно идентифицировать киберпреступников (особенно если они находятся на территории офшорных государств, где действует запрет на выдачу определенной информации).

Очевидно, что в будущем угрозы не станут проще. Уже сегодня многие атаки – это комбинации различных методик. Использование только традиционных систем обеспечения информационной безопасности (ИБ), таких как сигнатурные антивирусы, не дает надежной защиты от современных типов атак. Кредитные организации, которые защищаются только от известных угроз, всегда рискуют, поскольку атакующие выдумывают и создают все новые технологии и схемы.

---

[50] Эта парадигма уходит корнями в историю России. Так, система государственной безопасности СССР и деятельность КГБ были построены на этой модели. Четко просматривается эта парадигма и в начале 1990-х гг. XX в. Например, в Законе РФ от 05.03.1992 № 2446-I «О безопасности» безопасность определяется как состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз.

[51] Подтверждением этому может служить принятие ряда важнейших концептуальных документов, направленных на обеспечение разных видов безопасности Российской Федерации (в которых акценты сделаны именно на проблемах развития): Стратегии национальной безопасности Российской Федерации (2009 г.), Доктрины информационной безопасности Российской Федерации (2000 г.), Стратегии развития информационного общества в Российской Федерации (2008 г.) и др.

2.2. Методология анализа рисков недостаточного обеспечения кибербезопасности

– Есть новости. Хорошая и плохая, – сказал Сэм. – С какой начать?

– С хорошей.

– Девяносто процентов, что торпед внизу нет…

– А плохая?

– Всего девяносто процентов, что торпед внизу нет.

Клайв Касслер, Грант Блэквуд.
Золото Спарты

Основными причинами повышенного внимания регулирующих органов к технологиям ДБО (включая СЭБ) являются «виртуальная» форма совершения банковских операций (когда каждая проводка выражается в мгновенном изменении содержания центральной базы банковских данных), снижение надежности и устойчивости кредитных организаций, а также банковской системы в целом, так как любые высокотехнологичные нововведения повышают и усложняют банковские риски.

В условиях применения СЭБ возникают ранее не учитываемые источники угроз, которые способны создать дополнительные проблемы, связанные со снижением уровня надежности банковских автоматизированных систем и угрозами безопасности информационных ресурсов (в т. ч. АПО, находящегося на стороне провайдеров). Для перехода на новый качественный уровень управления рисками, возникающими в условиях применения СЭБ, не следует ограничиваться только выявлением причин и определением размеров возможных финансовых потерь. Необходимо шире рассматривать проблемы, связанные с использованием СЭБ, выходить за рамки привычных методов учета рисков. В качестве итоговых оценок следует рассматривать риски, связанные с системными характеристиками и показателями (риски системного уровня): возможность продолжения функционирования банка и выполнения им функций финансового посредника в неизменном или измененном масштабе, временный запрет на выполнение определенного вида банковских операций, введение временной администрации, отзыв лицензии на банковскую деятельность.

Иерархию рисков можно представить в виде трех уровней: системный банковский риск (СБР), типичный банковский риск (ТБР) и элементарный банковский риск (ЭБР). Они имеют разную природу. Каждый ЭБР отражает некий выявляемый факт, каждый ТБР – какое-либо событие в банке, образуемое совокупностью фактов и связанное с финансовыми потерями, а СБР описывает некоторую итоговую рисковую ситуацию (рис. 26). Количество источников ЭБР для каждого ТБР различно.

Поиск источников ЭБР и дальнейшее выстраивание причинно-следственных связей представляют собой наиболее сложную задачу для адекватной оценки. Поэтому специалисты, входящие в риск-подразделения и службы внутреннего контроля, должны хорошо представлять особенности функционирования СЭБ и возможные последствия проявления сопутствующих рисков (включая воздействие компьютерных атак на информационные ресурсы банка). Очевидно, что реализованные компьютерные атаки значительно расширяют профили типичных банковских рисков.

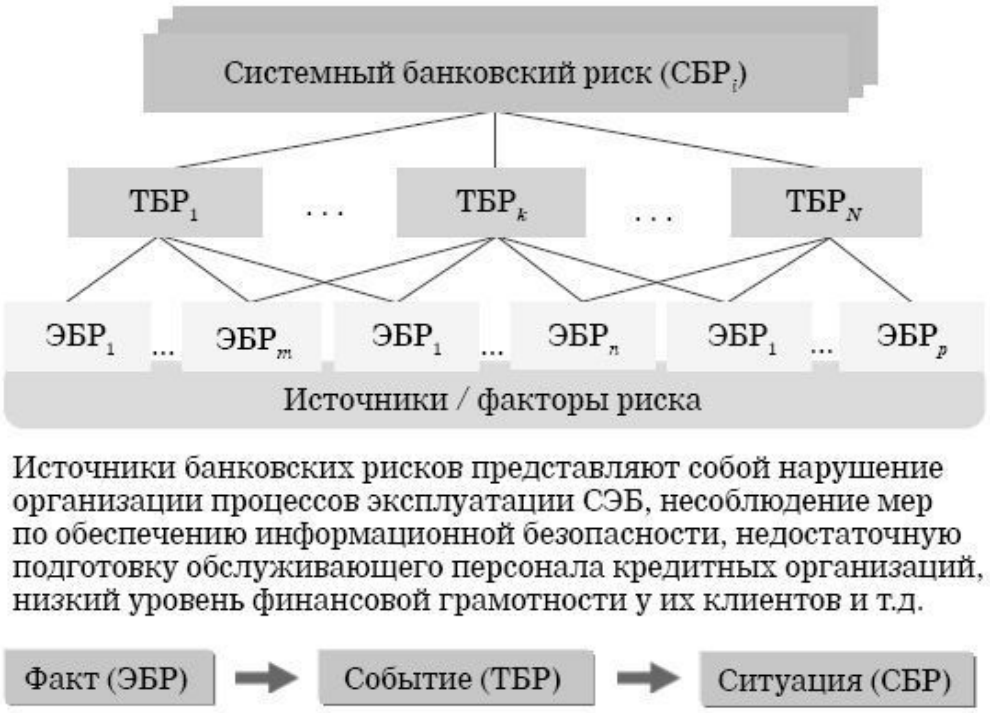


Рис. 26. Иерархическая схема для выявления, анализа и мониторинга банковских рисков

Примерная схема анализа возможного влияния нарушения кибербезопасности в условиях ДБО на деятельность кредитных организаций представлена на рис. 27, влияние компьютерных атак на устойчивость и стабильность банковской системы показано на рис. 28. Например, в случае реализованной компьютерной атаки на системы ДБО банка вполне вероятно, что многие клиенты откажутся от услуг данной кредитной организации. Следовательно, сумма остатков на их счетах и будет возможной суммой единовременного снятия средств клиентами (риск ликвидности). Далее такие клиенты могут быстро распространить отрицательные отзывы о банке, и вполне вероятно, что их знакомые, которые также являются клиентами банка, могут последовать их примеру и закрыть свои счета (репутационный риск и возрастание риска ликвидности).

Рис. 27. Взаимосвязь кибератак на АПО БАС и возможных последствий для банка[52]

[52] АРМ КБР – автоматизированное рабочее место клиента Банка России.SWIFT – Society for Worldwide Interbank Financial Telecommunications.

Рис. 28. Влияние компьютерных атак на устойчивость и стабильность банковской системы

Добавим, что некоторые клиенты могут обратиться в суды за возмещением не только похищенной суммы, но и суммы упущенной выгоды (например, в случае временной неплатежеспособности при взаимодействии с выгодным клиентом, деловым партнером и т. п.). Судебные издержки, негативная информация об этих судебных решениях в СМИ могут серьезно повлиять на репутацию организации (правовой и репутационный риски).

Для многих кредитных организаций существует управленческая задача, обусловленная несоразмерностью мер по информационной безопасности (включая обеспечение кибербезопасности) основным целям и общему уровню принимаемых рисков. Это говорит о нехватке качественного управления рисками и о том, что кибербезопасность обеспечивается постфактум, по итогам уже совершившегося события, а должна носить превентивный характер и работать на опережение.

К основным причинам появления рисков недостаточного обеспечения кибербезопасности в условиях применения СЭБ можно отнести:

– наличие множественных уязвимостей АПО СЭБ, отсутствие должной реализации процедур контроля за соответствием СЭБ требованиям информационной безопасности;

– низкую эффективность проводимых кредитными организациями мероприятий по внедрению и использованию документов Банка России в области стандартизации обеспечения информационной безопасности;

– отсутствие правовой основы для распространения нормативных требований к обеспечению защиты информации, устанавливаемых Банком России, на все процессы в деятельности кредитных организаций;

– отсутствие должной достоверности контроля выполнения технических требований, реализуемого, как правило, в форме самооценки [107, с. 118].

Банк России выделяет следующие ключевые направления деятельности для минимизации последствий проявления рисков недостаточного обеспечения кибербезопасности:

– проработка вопроса о законодательном закреплении права Банка России совместно с ФСТЭК России и ФСБ России осуществлять нормативное регулирование и контроль всех вопросов, связанных с обеспечением информационной безопасности в кредитных организациях, в том числе вопросов защиты информации, отнесенной к категории банковской тайны;

– законодательное закрепление основ деятельности по реализации системы противодействия хищениям денежных средств (системы антифрода) и создание такой системы на базе ФинЦЕРТ Банка России;

– обеспечение скорейшей разработки и ввода в действие национальных стандартов, регулирующих технические вопросы обеспечения информационной безопасности в организациях кредитно-финансовой сферы;

– создание совместно с ФСБ России и ФСТЭК России системы для подтверждения соответствия обеспечения информационной безопасности кредитно-финансовых организаций требованиям национальных стандартов;

– пересмотр технологических требований, связанных с осуществлением переводов денежных средств, внедрение безопасных технологий, в том числе для участников платежной системы Банка России;

– пересмотр технологии контроля со стороны Банка России за соблюдением участниками платежной системы Банка России требований к обеспечению информационной безопасности;

– реализация системы надзорных мер, учитывающей результаты контроля информационной безопасности в рамках системы подтверждения соответствия национальным стандартам.

В ближайшей перспективе из-за развития технологий ДБО количество «физических» банковских офисов в России будет постепенно уменьшаться. Наличие собственного кабинета в киберпространстве станет таким же распространенным явлением, как сегодня наличие мобильного телефона.

Активное использование СЭБ в банковском бизнесе создает не только новые общие возможности, но и общие уязвимости, формируя при этом общую ответственность. Создание системы кибербезопасности и соблюдение культуры кибербезопасности всеми участниками информационного обмена в условиях применения СЭБ являются залогом доверия клиентов не только к конкретной кредитной организации, но и ко всей банковской системе в целом.

Конец ознакомительного фрагмента.

Текст предоставлен ООО «ЛитРес».

Прочитайте эту книгу целиком, купив полную легальную версию на ЛитРес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.