ОСОБЕННОСТИ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КРЕДИТНЫХ ОРГАНИЗАЦИЙ

PECULIARITIES OF POLICY OF INFORMATION SECURITY OF CREDIT ORGANIZATIONS

A. Marchenko

Summary. The article is devoted to the study of the specifics of the information security policy of credit institutions. Distinctive features of information security of credit institutions are considered in comparison with transport enterprises. The results of the analysis made it possible to identify the objects of information protection, the purpose and objectives of the information security policy, threats and sources of attack. In detail one of the most vulnerable spheres of activity of credit organizations is considered: the system of electronic payments and promising directions for improving the information security policy of credit institutions.

Keywords: information, security, attack, protection, encryption.

Марченко Андрей Юрьевич
Аспирант, Ростовский Государственный Экономический Университет (РИНХ)
Thevanila@mail.ru

Аннотация. Статья посвящена изучению особенностей политики информационной безопасности кредитных организаций. Отличительные черты информационной безопасности кредитных организаций рассмотрены в сравнении с транспортными предприятиями. Результаты анализа позволили обозначить объекты информационной защиты, цель и задачи политики информационной безопас ности, факторы угроз и источники атак. Детально рассмотрена одна из наиболее уязвимых сфер деятельности кредитных организаций — система электронных платежей. Отдельно выделены перспективные направления усовершенствования политики информационной безопасности кредитных организаций.

Ключевые слова: информация, безопасность, атака, защита, шифрование.

Стремительное развитие информационных технологий, расширение глобальной информационной среды, широкое применение средств обмена информацией, комплексная компьютеризация всех сфер жизнедеятельности обусловливают актуальность исследования вопросов безопасности информацион ной инфраструктуры. Обеспечение эффективной защиты информации является чрезвычайно актуальным для кредитных учреждений, в которых ежедневно обрабатывается большой объем информации различного уровня конфиденциаль ности [1]. Эта информация в большинстве случаев и выступает объектом действий конкурентов и злоумышленников, что обусловливает обострение вопросов защиты ее от незаконного использования и несанкционированного доступа.

Итак, сегодня у руководства большинства кредитных организаций нет сомнений в необходимости обеспечения собственной информационной безопасности (сохранение банковской и коммерческой тайн, тайны вкладов, безопасности электронных документов и учетных данных). Применение современных информационных технологий в финансовых системах расширяет возможности для различных злоупотреблений, связанных с использованием вычислительной техники (так называемых компьютерных преступлений). Ежегодные потери от преступлений в этой сфере для кредитных организаций составляют в мире, по разным оценкам, от 170 млн. до 10 млрд. долл. [2].

Указанные обстоятельства обуславливают тот факт, что сегодня кредитные учреждения предпринимают ряд мер, позволяющих им противостоять несанкционированному доступу и разглашению коммерческой информации.

Вместе с тем следует отметить, что стратегия информационной безопасности кредитных учреждений очень сильно отличается от аналогичных стратегий других компаний и организаций. Это обусловлено специфическим характером угроз, а также их публичной деятельностью, обязывающей давать достаточно легкий доступ к счетам с целью удобства клиентов.

Таким образом, с учетом вышеизложенного, исследование особенностей политики информационной безопасности кредитных организаций является актуальной научно-методической задачей, которая и обусловила выбор темы данной статьи.

В экономической литературе много внимания уделяется исследованию проблем информационной безопасности, в том числе важное место занимают труды таких ученых как: С. Расторгуев, А. Белорус, Д. Лукьяненко, Е. Макаренко, А. Гуз и др. Различные аспекты защиты банковской информации рассматривали И. Горячкивская, В. Евдокимов, И. Остряков, М. Слободина и др.

Таблица 1. Цели, объекты и субъекты нападения на информацию в транспортной отрасли

Цели нападения						
Кибершпионаж — несанкционирован ная передача с помощью скрытых (незадекларирован ных) каналов связи данных, программ в автоматизированных системах управления или географических координат (GPS или ГЛОНАСС и др)	Кибераудит — разработка сценариев компьютерных методов нападения, хакерские и «дружественные» кибератаки, поиск уязвимостей информационно-коммуникационной среды транспорта	Кибермошенничество — «продажа» фальшивых электронных билетов, взлом автоматов продажи билетов и квитанций оплаты багажа, взлом счетчиков учета грузов, энергоносителей и автоматических расходомеров и заправщиков и др		Киберсаботаж — снижение пропускной спо собности авто мобильных, железнодорожных, трубопроводных магистралей, в частности, до полной остановки транспортных процессов	Кибердиверсии — создание враждебных (ложных) и опасных маршрутов следования (движения), особенно при перевозке особо опасных и социально значимых грузов, пассажирских и военных перевозках	
Виды транспорта и объекты нападения						
Железнодорожный	Автомобильный	Воздушный	Морской и речной	Трубопроводный	Муниципальный	Системы навигации
Объектами кибератак могут быть системы диспетчерского и автоматизированного управления, ответственные за формирование безопасных маршрутов движения подвижного состава; системы безопасного движения подвижного состава и безопасного проезда переездов; системы защиты и регулирования электроснабжения; автоматические системы пожаротушения и термостабилизации; системы автоматики в морских и речных портах, железнодорожных депо, АТП и др.; системы связи GSM-R, VSAT и др., а также операторы, обслуживающий персонал — диспетчеры, дежурные, и машинисты, водители транспортного средства, экипажи судов и воздушного транспорта						
Атакующая сторона						
Хакеры, конкуренты, инсайдеры, организованные преступные группировки, спецслужбы, вооруженные силы иностранных государств (кибервойска). При этом уровень «вооруженности» (технической оснащенности) и компетентности (информационной осведомленности) «злоумышленника» может быть очень высоким						

Вместе с тем, современный этап развития информационной безопасности требует комплексного подхода к разработке и внедрению методов и средств защиты ресурсов информационно-коммуникационных систем и сетей кредитных организаций.

Итак, цель статьи заключается в изучении особенностей политики информационной безопасности кредитных организаций, выявлении ключевых проблем и перспектив развития.

Так, в целом информационная безопасность — это формирование информационных ресурсов и организация гарантированной их защиты [3]. Достигается она созданием системы сбора и обработки информации, проведением соответствующих мероприятий по ее хранению и распределению, определением категорий и статуса информации, утверждением порядка и правил доступа к ней, соблюдением всеми работниками и клиентами норм и правил работы с коммерческой информацией, своевременным выявлением попыток и возможных каналов утечки информации и их пересечением.

В свою очередь, информация, которая хранится и обрабатывается в кредитных организациях, представляет собой реальные деньги. Вполне понятно, что незаконное манипулирование такой информацией может привести к серьезным убыткам.

Как уже отмечалось ранее, особенности политики информационной безопасности кредитных организаций не являются одинаковыми в сравнении с субъектами хозяйствования из других секторов экономики.

Так, например, сравним объекты информационной безопасности кредитных учреждений и информационно-коммуникационной среды транспорта.

Объектами информационной безопасности кредитных организаций является информация о персонале (руководство, ответственные исполнители, сотрудники); информация о технологиях, используемых кредитной организацией; информационные ресурсы (информация относительно деятельности и финансового состояния клиента, которая стала известна в процессе обслуживания, информация обо всех операциях кредитного учреждения и его финансовая отчетность); конфиденциальные электронные сети [4].

В свою очередь угрозы информационной безопасности в транспортной отрасли заключаются в том, что преступники могут получить возможность перехватывать пароли, отдельные файлы, геолокационную информацию, транслировать аудио- и видеоданные, контролировать Wi-Fi-сети, веб-камеры, информационные табло на автомобильных и железнодорожных путях, вокзалах, аэропортах и др. В табл. 1 приведены более подробные

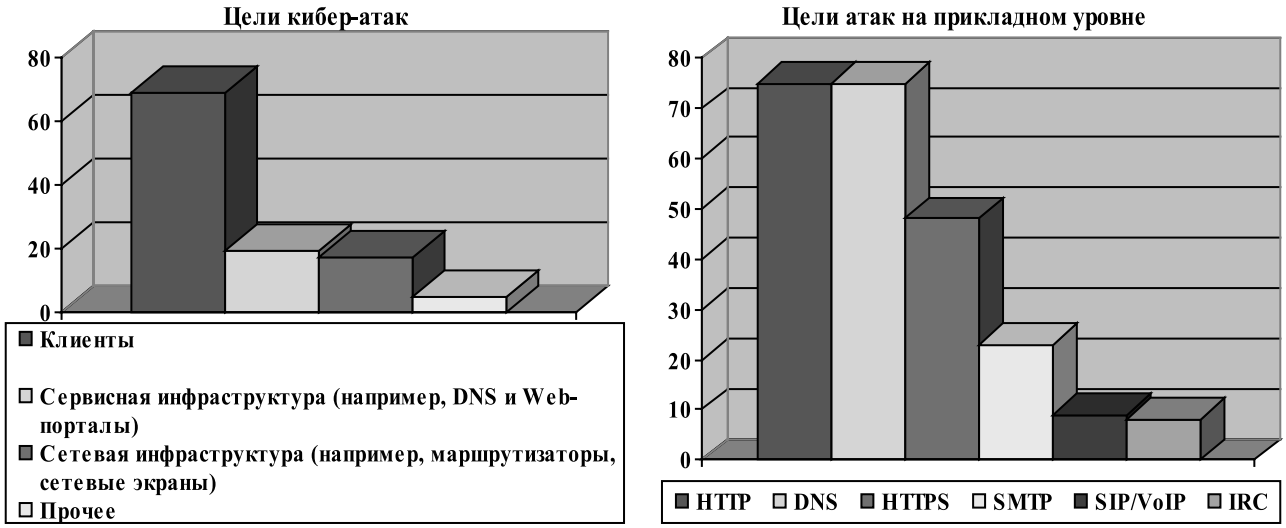

Рис. 1. Типы атак на услуги конфиденциальности и целостности в кредитных организациях (% опрошенных респондентов) [5]

данные в разрезе объектов нападения на информационно-коммуникационную среду транспорта.

Очевидно, учитывая имеющиеся различия, цели, задачи, средства и инструменты политики информационной безопасности кредитных учреждений и других субъектов экономики существенно отличаются.

Так, главной целью системы информационной безопасности кредитной организации является обеспечение ее устойчивого функционирования и предотвращение угроз информационной безопасности; защита от противоправных посягательств, разглашения, потери, утечки, искажения и уничтожения служебной информации, нарушения работы технических средств; поддержка бесперебойной производственной деятельности, включая и работу средств информатизации.

К основным задачам, которые должна решать политика информационной безопасности кредитного учреждения, относятся: обеспечение доступа руководства к конфиденциальной рыночной информации; предотвращение утечки и разрушения конфиденциальной финансовой информации; обеспечение распространения во внешней среде выгодной для организации «конфиденциальной» информации.

Ухудшение состояния информационной безопасности кредитных организаций может быть вызвано действием таких факторов:

1. увеличение объемов информации, накапливаемой, хранимой и обрабатываемой с помощью компьютеров;
2. сосредоточение в базах данных информации различного назначения и различной принадлежности;
3. расширение круга пользователей, имеющих непосредственный доступ к ресурсам вычислительной системы и массивам данных;
4. усложнение режимов работы технических средств вычислительных систем;
5. обмен информацией в локальных и глобальных сетях, в том числе на больших расстояниях.

Особенно уязвимой с точки зрения информационной безопасности кредитного учреждения является система электронных платежей. Одно из наиболее уязвимых мест в системе электронных платежей представляет собой пересылка платежных и иных сообщений между банками, между банком и банкоматом, между банком и клиентом. Результаты исследований атак на современные кредитные организации в России, проведенные компанией «ArborNetworks», отображены на рис. 1.

Для защиты платежных сообщений в системе электронных платежей используется защищенная электронная почта, предназначенная для обмена электронными уведомлениями в формате SMF-70 через сеть передачи данных произвольного типа, которая соответствует определенным критериям.

Общая структура подсистемы защиты информации в системе электронных платежей и возможных угроз на отдельные ее составляющие приведены на рис. 2

Сегодня кредитные организации используют специальные программные комплексы по сканированию

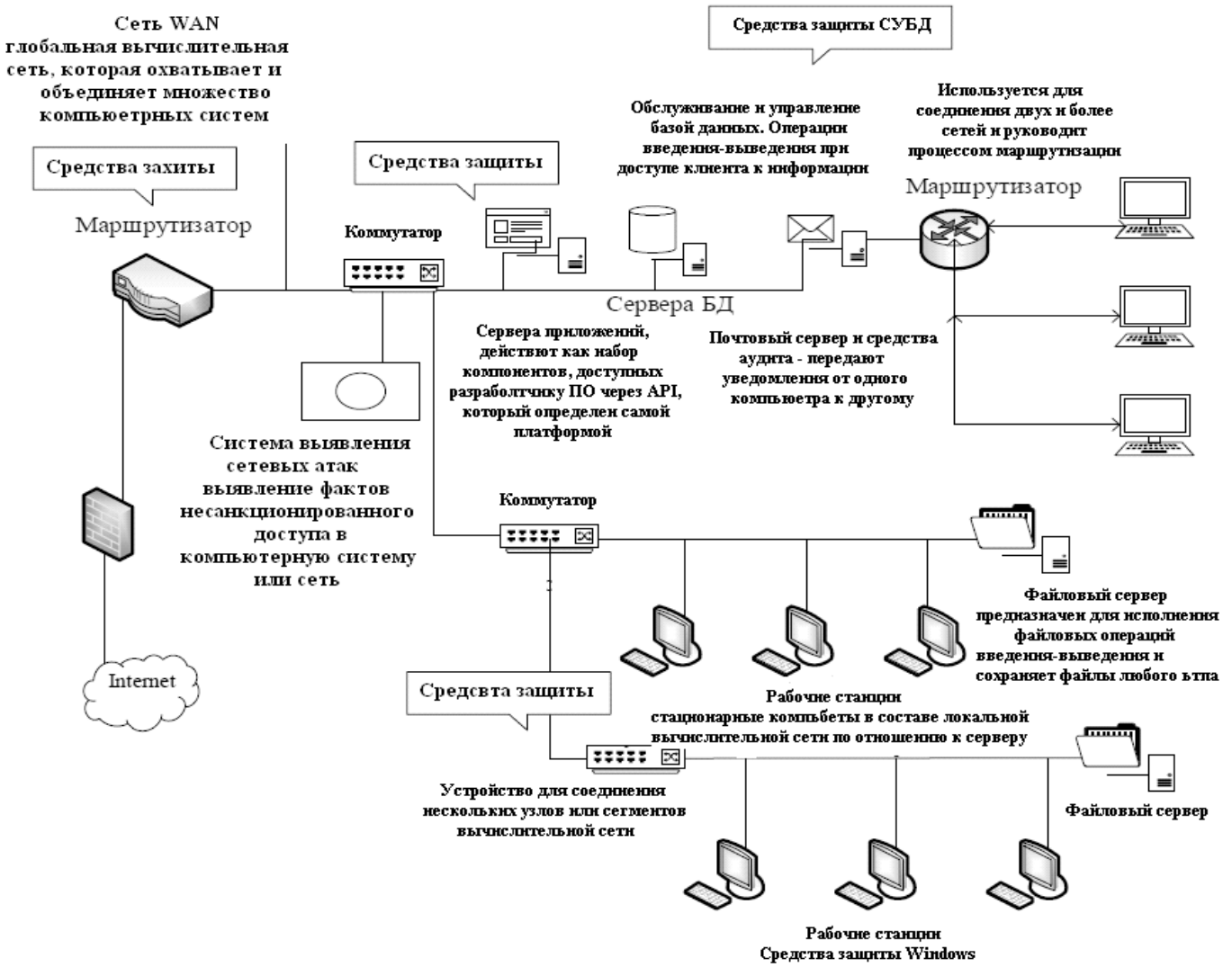

Рис. 2. Структурная схема подсистемы защиты информации в СЭП

уровня информационной защищенности компьютерных сетей. Среди таких комплексов отдельное место занимает специализированные языки, например, Vulnerability Description Language, Internet SafeSuit (Internet Security Systems) и др.

Сейчас на рынке представлено достаточное количество программного обеспечения, относящегося к категории средств поиска «взлома» сетей, например: Internet Security Scanner (фирма Internet Security Systems), NetRecon (фирма Axent), NetProbe (фирма Qualix), Ballista (фирма Secure Networks), NetGuard (фирма Network Guardians), NetSonar (фирма WheelGroup).

Кредитные организации России преимущественно используют специальное банковское программное обеспечение отечественного производства, для защиты своих информационных систем, например:

- комплексную безопасность корпоративных сетей обеспечивают программные продукты VPN ЗАСТАВА 3.3, созданные компанией «ЭЛВИС_ ПЛЮС»;
- криптографическая защита «Крипто Про CSP», разработанная компанией «Крипто Про», помогает эффективно проверять электронную цифровую подпись;
- финансовую безопасность кредиторов обеспечивает система A2 AGRUS APPLICATION, созданная компанией «Агрус MGS»;
- комплекс «Банк_Доступ» обеспечивает централизованное управление, распределяя доступ к информационным ресурсам;
- комплекс «Банк — активный Защита», разработанный фирмой «Андек», используют для ликвидации последствий атак хакеров, если им все же удалось прорвать информационную защиту.

Значительные перспективы для защиты информации в кредитных учреждениях имеют криптографические симметричные и асимметричные алгоритмы шифрования, применение которых предусмотрено международными стандартами ISO 7498, ISO/IEC10181. Эти средства предназначены для криптографической защиты конфиденциальной информации в автоматизированных банковских системах, применяются для обмена информацией внутри корпоративной сети банка с клиентами, которые работают с системой «Клиент-Банк», а также в системах обслуживания пластиковых карт.

Сейчас ведущие компания мира предлагают широкий спектр средств шифрования, так, например, можно отметить предложения от Checkpoint, Cisco и Symantec. Также отдельно следует обозначить современные алгоритмические языки высокого уровня, являющиеся трансплатформенными и поддерживаемыми средами MS CryptoAPI 2.0 и NET Framework.

Таким образом, подводя итоги, можно отметить следующее. На сегодняшний день не подлежит сомнению тот факт, что политика информационной безопасности кредитных организаций должна представлять собой комплекс организационных, технических, программных средств и мероприятий, предназначенных для сбора, классификации, анализа, оценки, защиты и распространения актуальной информации с целью обеспечения защиты ресурсов организации и наиболее оптимальной реализации ее интересов. Совокупность обозначенных аспектов формирования и поддержки информационной безопасности кредитных организаций позволит точно идентифицировать возможные угрозы и оперативно их устранить без негативных последствий для самой организации и ее клиентов.

ЛИТЕРАТУРА

1. Лобов С. А., Чемиренко В. П. Информационная и национальная безопасность: взаимное влияние факторов и подсистем обеспечения безопасности // Электросвязь.— 2017.— № 1.— С. 48–53.
2. Яркова К. В. Обеспечение информационной безопасности в банковских учреждениях // Форум молодых ученых.— 2017.— № 5.— С. 2362–2365.
3. Громова О. О. Информационная безопасность — новые вызовы // Вестник связи.— 2017.— № 3.— С. 28–32.
4. Трифонова А. К., Бескровный Р. Д. Кибератаки на банковский сектор: новые риски и пути преодоления // Экономика. Бизнес. Банки.— 2017.— Т. 2.— С. 83–89.
5. ArborNetworks URL: https://www.arbornetworks.com/

Ростовский Государственный Экономический Университет