Тип работы: ВКР (Выпускная квалификационная работа)

Предмет: Криптография

Введение

В современном обществе при внедрении компьютерных технологий во многих сферах деятельности необходимым условием работы системы является использование коммуникационных технологий. Связь между компьютерами обеспечивают сети. Использование глобальных сетей дает возможность повсеместного использования систем электронных платежей, позволяющих совершать покупки в Интернет-магазинах, проводить платежи за услуги коммунальных предприятий, уплачивать пошлины и штрафы. Использованием электронных денег снижает нагрузку на инфраструктуру банков, магазинов, транспортные сети, позволяя удаленно использовать платежные сервисы.
Актуальность исследования обусловлена тем, что одной из главный проблем при использовании электронных денег является необходимость обеспечения защищенности электронных кошельков и проведения электронных платежей. Гарантия безопасности платежных сервисов позволит значительно увеличить клиентскую базу платежных систем, увеличить перечень предоставляемых сервисов.
Целью данной работы является анализ защищённости использования электронных платежей с использованием криптографических алгоритмов.
Задачи работы:
- анализ технологий использования электронных денег в условиях Российской Федерации;
- анализ рынка электронных платежей, оценка их доли в общем объеме денежного оборота и тенденций роста;
- оценка защищенности платежных систем;
- определение технологий по обеспечению безопасности при проведении электронных платежей с использованием систем VPN;
- программная реализация криптографического алгоритма;
Объект исследования – технологии электронных платежей.
Предмет исследования – безопасность использования электронных денег.
Метод исследования – изучение научной и технической литературы по исследуемой тематике, математические методы, анализ, синтез.
Работа включает: введение, три главы, заключение и список использованных источников. Глава 1 содержит общую характеристику технологий проведения электронных платежей, оценка перспектив их развития, объемов занимаемых рынков денежного обращения. В главе 2 проведен анализ защищенности наиболее распространённых платежных систем, определены основные угрозы, а также методы защиты от них,

определены перспективы развития систем безопасности при проведении электронных платежей. В главе 3 рассмотрены вопросы методологии разработки криптографических алгоритмов.

1.Теоретическая часть

1.1. Правовые основы функционирования электронных платежных систем

Понятие "электронные деньги" является относительно новым и зачастую используется применительно к широкому кругу платежного инструментария, использование которого базируется на современных технических решениях. Вследствие этого, отсутствует единый, признанный подход к определению электронных денег, однозначно определяющий их экономический и правовой статус.
В РФ одними из наиболее популярных электронных кошельков являются: Яндекс.Деньги и Киви.
Яндекс-деньги являются одной из самых универсальных ПС (платёжных систем) в России. Её выбирают пользователи, чей заработок связан с работой в сети Интернет.
К основным возможностям системы относят:
- оплату различных услуг, в т.ч. мобильных телефонов, налоговых и коммунальных платежей;
- проведение переводов, в т.ч. на пластиковые карты и банковские счета;
- возможность работы с картой Яндекс.Деньги.
Кроме того, с помощью данной системы оплачиваются различные электронные сервисы (покупки на сайтах, оплата программного обеспечения и электронных игр).
Датой запуска системы считается 24 июля 2002 года, когда данный проект был запущен как партнерская прогармма с системой PayCash, с 14.11.2002 система получила аккредитацию для проведения Интернет-платежей.
Изначально команда PayCash осуществляла техническую поддержку платежной системы, а Яндекс — за инструменты работы с массовой аудиторией. При этом платить Яндекс.Деньгами можно было только через клиентскую программу. Простой и удобный пользовательский веб-интерфейс появился в 2005 году. Тогда пользователи получили возможность управлять счетом с любого компьютера. Это привлекло внимание крупных игроков на рынке электронной торговли: Яндекс.Деньги стали первым сервисом электронных денег, подключившим возможность оплаты сервисов Skype для России.
На рисунке 1 показана диаграмма основных направлений использования электронных кошельков на примере системы «Яндекс.Деньги».

Рисунок 1 – Диаграмма основных направлений использования электронных кошельков на примере системы «Яндекс.Деньги»

Федеральный закон № 161-ФЗ определяет организационные, формально-юридические и целевые критерии (совокупность компаний, осуществляющих взаимодействие по правилам работы с платежными системами в целях проведения переводов денежных средств).
Организационная основа работы платежных систем включает [4]:
— регламентацию работы операторов платежных систем;
— работу операторов платежной инфраструктуры (операционные, платежные клиринговые и расчетные центры);
— участников платежной системы.
Юридическая основа работы платежных систем включает комплекс правил платежной системы, содержащих условия участия в платежных системах, проведение переводов денежных средств, перечень услуг платежной инфраструктуры и другие условия, которые определяются оператором платежных систем в соответствии с действующим законодательством. Регламенты работы платежных систем, за исключением регламентов Центрального Банка, определяются в нормативных актах Банка России (Положение Банка России от 29 июня 2012 г. № 384-П), представляют собой договор присоединения.
В отношении операторов платежной системы в соответствии со статьей 15 Федерального закона № 161-ФЗ предусматриваются:
• Перечень основных обязанностей операторов платежных систем (в которых определяются правила платежной системы, порядок организации и контроля за их соблюдением, привлечения операторов услуг платежных систем, организации технологии управления рисками в платежных системах, досудебное и (или) третейское рассмотрение споров при работе платежной системы);

• Функции регистрации оператора платежных систем в реестре операторов, которые ведётся Банком России;
• Регламенты платежной системы;
• Документация, подтверждающая соответствия требованиям, в сответствии с 161-ФЗ.
Безопасность проведения платежей в электронной форме определяется безопасностью использования криптографических и сетевых технологий.
Одним из главных рисков, связанных с работой электронных платежных систем, является риск потери денежных средств, хранящихся в платежных системах.
Риски могут быть обусловлены влиянием следующих факторов:
- вероятностью взлома учетных записей в платежных системах;
- хакерские атаки и активность вредоносного ПО;
- несовершенством системы аутентификации;
- непродуманностью политики защиты учетных записей, что допускает вероятность их взлома.
Источники рисков в работах с платежными системами включают:
- ошибки в действиях пользователей;
- активность злоумышленников;
- ошибки в работе платежных систем, приводящие к ошибкам при проведении платежей и нарушениям безопасности учетных записей.
В силу значительного количества прецедентов, связанных с потерей денежных средств в электронных кошельках, подобного рода механизмы не используются как инструмент накопления денег. Как правило, пользователи хранят деньги в электронных кошельках в суммах, не превышающих стоимость 1-2 покупок.
Стандартными способами защиты при использовании электронных денег является принятия комплекса мер по информационной безопасности домашних пользователей:
- использование актуальных версий антивирусного ПО и антивирусных баз;
- соблюдение требований к сложности паролей для входа в системы управления электронными кошельками и частоте их смены;
- своевременное обновление браузеров, а также операционных систем;
- при работе с браузерами необходимо использование оптимальных настроек безопасности;
- в случае, если электронный кошелек интегрирован с почтовой системой, то следует применять максимальные настройки защиты почтового ящика: использовать систему СМС – подтверждения при манипуляциях с паролями, использовать СПАМ-фильтры, не открывать вложения, полученные в письмах от неизвестных отправителей.
Также к уязвимостям платежных систем следует отнести возможности авторизации с использованием аккаунтов в социальных сетях. В силу того, что аккаунт в соцсетях менее защищены, чем учетные записи в платежных системах, возможен несанкционированный вход в интерфейс платежной системы в случае взлома учетной записи в соцсети.
Основным недостатком использования электронных денег является то, что электронные счета гарантированы эмитентом, государственные гарантии таких счетов отсутствуют. Таким образом, электронные деньги не рискованно использовать при осуществлении крупных платежей, а также использовать как средство накопления значительных сумм в течение длительных периодов времени. Таким образом, электронные деньги являются в первую очередь платежным, а не накопительным средством.
Несмотря на отличную портативность, платежные системы нуждаются в применении специальных инструментов хранения и обращения, а в случаях физического уничтожения носителей электронных денег, восстановление информации и счета является может быть невозможным. Средства криптографической защиты, использующиеся для защиты систем электронных денег, ещё не набрали длительного опыта спешного использования, соответственно обеспечение безопасности с их использованием (защищенности от хищений, подделок, изменений номинала и т.п.) не подтверждается опытом широкого обращения и беспроблемной истории. Теоретически возможно проведение хищений электронных денег, через использование уязвимостей операционных систем или нарушения безопасности в самих платежных системах. Одним из основных требований при использовании платежных систем является обеспечение сохранности средств на электронных кошельках, обеспечение безопасности при проведении платежных операций, обеспечение идентификации платежа на стороне получателя.
Основные способы защиты при работе с платежными системами включают [14]:
- установку сложного пароля;
- многофакторную аутентификацию в системе;

- установку лимитов на проведение платежей в течение суток, либо проведение усиленной аутентификации при проведении платежей большими суммами;
- введение системы идентификации пользователя.

Проведем анализ защищенности платежных систем согласно вышеуказанным критериям (таблица 1).

Таблица 1 - Анализ защищенности платежных систем

Уровень защищенности	Яндекс. Деньги	Киви	Сбербанк. Онлайн	ePayments
Контроль сложности платежных паролей	Присутствует	Нет	Нет	Присутствует
Дополнительная аутентификация при входе в систему	Нет	Нет	Присутствует	Присутствует
Подтверждение транзакции через СМС	Присутствует	Присутствует	Присутствует	Присутствует
Установка суточных лимитов	При отсутствии идентификации пользователя	При отсутствии идентификации пользователя	Присутствует	При отсутствии идентификации пользователя
Дополнительная идентификация	Нет	Нет	Нет	Присутствует
Обращение к платежной системе из сторонних приложений	Присутствует	Нет	Нет	Нет
Возможность перехода к платежам из системы сайтов-партнеров	Присутствует	Через выставление счета	Нет	Нет
Аппаратная аутентификация	Нет	Нет	Присутствует	Нет
Привязка банковских карт	Присутствует	Присутствует	Присутствует	Нет

Потери данных также относятся к категории угроз конфиденциальности, так как в данном случае вероятно неконтролируемое распространение защищаемой информации при её разглашении, получении к ней несанкционированного доступа или получении доступа со стороны заинтересованных субъектов, в качестве которых могут выступать физические лица, конкурирующие коммерческие структуры, спецслужбы государств, криминальные структуры [3].

Существует следующая классификация угроз по видам полученного сетевого доступа.

1. Угрозы разглашения информации
1.1. Преднамеренное разглашение с прямым умыслом.
1.2. Угрозы разглашения разглашение по неосторожности.
2. Угрозы получения несанкционированного доступа к информации
2.1. Угрозы получения физического доступа к сетевым ресурсам (например, через включения в свободные порты ЛВС)
2.2. Угрозы программно-аппаратного доступа.
2.3. Угрозы получения доступа к системе с использованием специализированного ПО
3. Угрозы перехвата информации (предполагают утечку информации с использованием технических каналов)
3.1. Перехват данных, обрабатываемых техническими средствами.
3.2. Перехват аудиосигналов.
3.3. Перехват сетевого трафика.
4. Хищение носителей информации.

Угрозы доступности связаны с получением доступа к хранимым и обрабатываемым данным в любой момент. Наиболее частые и опасные по размеру причиняемого ущерба ошибка связаны с работой штатных пользователей информационной системы.

Ошибки подобного рода могут генерировать угрозы (например, некорректно введенные данные или ошибки в программе, становящиеся причиной уязвимостей для сетевых атак). Ошибки в действиях администраторов, могут открывать возможности для внешних вторжений в сеть.

Сетевые атаки на информационно-программные ресурсы можно условно разделить на локальные, удаленные и атаки на потоки данных [11].

При проведении локальных атак злоумышленники получают физический доступ к сетевым информационным ресурсам. Источники атак подобного класса, как правило, внутренние. Технологически атаки подобного класса проводятся на область загрузки операционной системы, на средства аутентификации и т.п.

Удаленные атаки осуществляются теми, кто не имеет прямой доступ к интересующим объектам. Внешние атаки могут осуществляться на маршрутизаторы, на сбор сведений о системе, на запуск вредоносных кодов и т.д.

Атаки на поток данных производятся, когда между двумя компьютерами проводится обмен данными по сети, и злоумышленник при этом проводит атаку на сегмент сети или сетевой узел, расположенный между

двумя взаимодействующими сетевыми узлами. Такой тип атак позволяет реализовывать и внутренние преднамеренные угрозы, и внешние. Существуют атаки на потоки данных пассивного типа (когда атакующий, никак не выдавая свое присутствие, проводит перехват всех электронных документов для дальнейшего анализа, но не имеет возможности модификации передаваемых сообщений) и активного типа (когда злоумышленник проводит перехват передаваемых данных с целью модификации сообщений, либо передачи собственных данных).

1.2. Анализ угроз безопасности при работе с электронными платежными системами

Также несанкционированный доступ к платежным системам может быть получен легальными средствами, включающими:
- подбор пароля;
- подбор данных, позволяющих восстановить доступ к платежной системе.
В данном случае идентификация нарушителя может проводиться на стороне банка путем анализа инцидента, связанного со сменой аутентификационных данных.
На компьютере злоумышленника возможно наличие следующих следов от совершенных несанкционированных операций по доступу к платежным системам:
- наличие установленного программного обеспечения, позволяющего обходить защиту платежных систем;
- наличие программного обеспечения, скрывающего IP-адрес атакующего компьютера;
- кэш браузера;
- системные журналы;
- сетевые протоколы роутера;
- временные файлы.
Таким образом, при проведении экспертизы на предмет обнаружения попыток несанкционированного взлома платежных систем

Список использованных источников

1. Электронные платежные системы в России. [Электронный ресурс]. Режим доступа: http://www.tadviser.ru/index.php/
2. Количество банковских карт в России. [Электронный ресурс]. Режим доступа: http://www.cbr.ru/statistics/print.aspx?file=p_sys/sheet013.htm
3. Количество пользователей Сбербанк-Онлайн. [Электронный ресурс]. Режим доступа: http://www.my-sberbank.ru/chislo-polzovatelej-servisa-sberbank-onlajn-prevysilo-6-millionov-chelovek.html
4. Особенности работы банков с пластиковыми картами. [Электронный ресурс]. Режим доступа: http://bankir.ru/publikacii/20121112/osobennosti-analiza-raboty-banka-s-plastikovymi-kartami-10002526/
5. Популярные платежные системы России и Китая. [Электронный ресурс]. Режим доступа: http://web-klik.ru/elektronnye-platyozhnye-sistemy/#i-2
1. Бабаш, А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, 2013. - 136 с.
2. Баймакова, И.А.. Обеспечение защиты персональных данных– М.: Изд-во 1С-Паблишинг, 2010. – 216 с.
3. Гафнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. - Рн/Д: Феникс, 2010. - 324 с.
4. Гашков С.Б., Применко Э.А., Черепнев М.А. Криптографические методы защиты информации. – М.: Академия, 2010. – 304 с.
5. Герасименко В.А., Малюк А.А. Основы защиты информации. - М.: МИФИ, 1997.
6. Грибунин В.Г., Чудовский В.В. Комплексная система защиты информации на предприятии. – М.: Академия, 2009. – 416 с.
7. Гришина Н.В. Комплексная система защиты информации на предприятии. – М.: Форум, 2010. – 240 с.
8. Громов, Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. - Ст. Оскол: ТНТ, 2010. - 384 с.
9. Емельянова Н.З., Партыка Т.Л., Попов И.И. Защита информации в персональном компьютере. – М.: Форум, 2009. – 368 с.
10. Ефимова, Л.Л. Безопасность проведения платежей Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга. - М.: ЮНИТИ-ДАНА, 2013. - 239 с.
11. Завгородний В.И. Комплексная защита в компьютерных системах: Учебное пособие. – М.: Логос; ПБОЮЛ

Н.А.Егоров, 2001. - 264 с.
12. Комплексная система защиты информации на предприятии. Часть 1. – М.: Московская Финансово-Юридическая Академия, 2008. – 124 с.
13. Грекул В. И., Денищенко Г. Н., Коровкина Н. Л. Проектирование информационных систем. — М.: Интернет-университет информационных технологий – М.: ИНТУИТ.ру, 2013. с.135
14. Гринберг, А.С. Информационные технологии управления: [Учеб. пособие для вузов по специальностям 351400 "Прикладная информатика (по обл.)", 061100 "Менеджмент орг.", 061000 "Гос. и муницип. упр."] /А.С. Гринберг, Н.Н. Горбачев, А.С. Бондаренко.-М.: ЮНИТИ, 2010.-479 с.
15. Диго, С.М. Базы данных: проектирование и использование: [Учеб. для вузов по специальности "Прикладная информатика (по обл.)"] /С.М. Диго.-М.: Финансы и статистика, 2010.-591 с.
16. ДнепровА.Г. Microsoft SQL Server 2008. Самоучитель. - М.: Финансы и статистика, 20012 – 361с.
17. Емельянова Н.З., Партыка Т.Л., Попов И.И. Защита информации в персональном компьютере. – М.: Форум, 2013. – 368 с.
18. Обзор агрегаторов для приема платежей. [Электронный ресурс]. Режим доступа: https://habrahabr.ru/company/web_payment_ru/blog/265349/
19. Рейтинг платежных систем 2020. [Электронный ресурс]. Режим доступа: http://tagline.ru/payment-systems-rating/
20. Электронные кошельки. [Электронный ресурс]. Режим доступа: http://user-life.ru/internet/elektronnye-koshelki-obzor-populyarnyx-platezhnyx-sistem.html