МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное
учреждение высшего образования
«Санкт-Петербургский политехнический университет Петра
Великого»
Институт промышленного менеджмента, экономики и торговли
Высшая школа технологий управления бизнесом

УДК 336.71

Директор ВШТУБ, д.э.н., профессор
_____И.В.Ильин
«___»_____ 2017 г.

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
БАКАЛАВРА

на тему:

Методы предотвращения рисков при использовании электронных денег

Направление: 38.03.05 – «Бизнес-информатика»

Выполнил студент гр. 437335/0103 _____ Жун И

Руководитель, _____ А.Б.Анисифоров
К.в.н. доцент

Нормоконтроль _____ Г.Ю. Силкина
д.э.н., профессор

Санкт-Петербург
2017

MINISTRY OF EDUCATION AND SCIENCE
OF THE RUSSIAN FEDERATION
Federal State Autonomous Educational Institution of Higher Education
Peter the Great St. Petersburg Polytechnic University
Institute of Industrial Management, Economics and Trade
Department of Information Systems in Economics and Management

UDK 336.71

Director of GS BMT Dr.Econ.Sci.,Prof.
_____ I.V.Ilin
«___»_____ 2017 y.

FINAL QUALIFYING WORK OF BACHELOR

Topic:

The methods of risk prevention in the use of electronic money

Direction: 38.03.05 – «Business Informatics»

Submitted by student of group 437335/0103 _____ Rong Yi

Supervisor _____ A.B.Anisiforov
Cond. of mil. Sci. dot

Norm controller: _____ G.Y.Silcina
Pro.,Dr.Econ.Sci.

Saint-Petersburg
2017

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Санкт-Петербургский политехнический университет Петра Великого»
Институт промышленного менеджмента, экономики и торговли
Высшая школа технологий управления бизнесом

УДК 336.71

УТВЕРЖДАЮ
Директор ВШ ТУБ д.э.н., профессор
_____ И.В. Ильин
«____» _____20____г.

ЗАДАНИЕ
на выполнение выпускной работы бакалавра

студента группы 437335/0103 Жун И
1. Тема выпускной работы :Методы предотвращения рисков при использовании электронных денег
2. Срок сдачи студентом законченной работы: «25» мая 2017 г
3. Исходные данные к выпускной работе: научная и специальная литература по теме работы, учебно-методические материалы ВШТУБ по написанию выпуской квалификационной работы, материалы производственной практики.
4. Содержание расчётно-пояснительной записки (перечень подлежащих разработке вопросов):1) Электронные платежи (сущность, особенности, электронные деньги, виртуальный кошелек, преимущества и недостатки электронных платежей)
2) Технические и инструментальные средства электронных платежей (электронные платежные системы, история развития, виды систем, перспективы развития, электронные платежные системы России, электронные платежные системы КНР, сравнительный анализ, достоинства и недостатки)
3) Риски, возникающие в электронных платежных системах и их предотвращение (идентификация рисков, качественный анализ,

характеристики угроз, способы, используемые злоумышленниками, методы защиты от киберпреступников, законодательные меры)

5. Перечень графического материала (с точным указанием обязательных иллюстраций):Сущность и особенности электронных платежей, электронные деньги, электронные платежные системы России и Китая, анализ рисков в электронных платежных системах и методы их снижения.

6. Консультанты по выпускной квалификационной работе:

_____

7. Дата выдачи задания «22»марта2017 г.

Руководитель,
К.в.н. доцент _____ (Анисифоров А.Б.)
подпись *расшифровка*

Задание принял к исполнению «22»марта 2017 г.

Студент _____ (Жун И)
подпись *расшифровка*

Примечание:

1. *Задание прилагается к законченной выпускной квалификационной работе и вместе с ней представляется в ГАК.*
2. *Кроме задания студент получает от руководителя календарный график процесса проектирования с указанием сроков выполнения и трудоёмкости отдельных этапов.*

РЕФЕРАТ

54с., 8 рис., 3 табл., 23 источников.
ЭЛЕКТРОННЫЕ ДЕНЬГИ, ПЛАТЕЖНЫЕ СИСТЕМЫ, ИНФОРМАЦОННАЯ БЕЗОПАСНОСТЬ, РИСКИ, ПАРОЛИ, ЭЛЕКТРОННЫЕ КЛЮЧИ

Целью данной работы является анализ защищённости использования электронных денег.

Объект исследования – технологии электронных платежей.

Предмет исследования – безопасность использования электронных денег.

В работе рассмотрены теоретические аспекты электронных денег, проанализирована статистика их использования, определены ограничения, проведено сравнение платежных систем России и Китая. В практической части работы рассмотрен перечень рисков при использовании электронных денег, приведен перечень мер предосторожности при использовании электронных кошельков с применением мер информационной безопасности.

.

ESSAY

54 p., 8 pic., 3 tabl., 23 sources.

ELECTRONIC MONEY, PAYMENT SYSTEMS, INFORMATION SECURITY, RISKS, PASSWORDS, ELECTRONIC KEYS

The aim of this work is the analysis of the security of the use of electronic money.

The object of research - the technology of electronic payments.

The object is to study the safety of the use of electronic money.

In the work discussed theoretical aspects of electronic money, analysed the statistics of the defined restrictions, compared the payment systems of russia and china. in the practical part of the work reviewed the list of risks in the use of electronic money, there is a list of precautions in the use of electronic purses using measures of information security.

СОДЕРЖАНИЕ

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 денег.

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.

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 предотвращения рисков при использовании электронных денег, обеспечения информационной безопасности сетевых соединений при проведении электронных платежей.

1.ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННЫХ ПЛАТЕЖНЫХ СИСТЕМ

1.1 Определение электронных денег

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 определении электронных денег различаются следующие подходы [6]:

- Европейский (самый распространенный);
- Американский;
- Азиатский.

Согласно европейскому подходу электронные деньги:

- Представляют собой новый формат денег;
- Предполагают использование особого режима эмиссии и обращения.

Согласно определению ЕЦБ, суть электронных денег в широком смысле можно определить как средство, используемое для электронного хранения эквивалента денежной стоимости с использованием технического устройства, которое может широко применяться при совершении платежей в пользу продавца без необходимости использования при проведении операции банковских счетов и функционирующее в формате предоплаченного финансового продукта на предъявителя.

Согласно определению Европейского парламента и Совета, электронные деньги представляют собой денежную стоимость, представленную требованием на эмитентов, которые:

- Хранятся на электронном устройстве;
- Эмитируются по получении средств эмитентами в размере не менее внесенной в качестве предоплаты денежных сумм;
- Принимаются в качестве средств проведения платежей иными институтами (не самими эмитентами).

Сами эмитенты электронных денег в Европе имеют отдельный статус, регулирование деятельности которых является более либеральным, чем у банков.

Согласно американскому подходу, электронные деньги являются новым видом платежных услуг, предоставляемых именно именно кредитными институтами.

В рамках действия "Акта об унификации денежных услуг", электронные деньги представляют собой денежные средства, преобразованные в информацию, хранящуюся на микрочипах или персональных компьютерах, для того, чтобы обеспечить возможность их передачи с использованием информационных сетей, например, таких как Интернет.

Согласно мнению ФРС, деятельность в области обращения электронных денег, включая проведение эмиссии, обращения и погашения электронных денег должна находиться под действием традиционного банковского законодательства, что связано с имеющейся монополией ФРС в сфере эмиссии любых денежных средств.

Согласно азиатскому подходу (в основном в Японии, Сингапуре, Тайване), электронные деньги являются:

- Новой формой депозитов;
- Электронным заменителем депозитов.

Согласно определению Банка Японии, электронные деньги являются электронным средством платежа, которое сохраняет денежную стоимость, представленную в электронном виде.

В финансовой системе не принято собственного определения электронных денег, при этом существует понятие предоплаченных финансовых продуктов, которые могут представлять собой набор денежных обязательств организаций, заменяющих в процессе их оборота требования физических лиц или организаций по оплате товаров и услуг, в том числе денежных обязательств, составленных в электронной форме.

Таким образом, электронные деньги представляют собой набор денежных обязательств эмитентов в электронной форме, находящиеся на электронных носителях в распоряжении пользователей. Для данных денежных обязательств необходимо обеспечение соответствия следующим требованиям [4]:

- Фиксация и хранение на электронных носителях;
- Выпуск эмитентами при получении от третьих лиц денежных средств в размере не меньшем, чем размер эмитированной денежной стоимости.
- Возможность приёма, как средства совершения платежей иными (помимо эмитента) организациями или лицами.

Для электронных денег характерно наличие внутреннего противоречия - с одной стороны они представляют собой средство платежа, с другой – набор обязательств эмитентов, которые должны выполняться при использовании традиционных неэлектронных денег. Данный парадокс можно объяснить с использованием исторических аналогий: в свое время банкноты также рассматривались, как обязательства, которые подлежат оплате с помощью монетам или драгоценных металлов. Очевидно, что с течением времени, электронные деньги будут являться одного из денежных форматов (наряду с монетами, банкнотами, безналичными деньгами и электронными деньгами). Так же очевидно, что в перспективе центробанками будет производиться эмиссия электронных денег, аналогично печати банкнот и чеканке монет.

Одним из распространённых заблуждений является отождествление электронных и безналичных денег.

Электронные деньги, представляя собой неперсонифицированный платежный продукт, могут находиться в отдельном обращении, отличном от банковского обращения, при этом могут и обращаться также и в государственном или банковском платежном обращении.

Как правило, процесс обращения электронных денег производится с использованием телекоммуникационных технологий, что предполагает работу с платёжными картами, электронными кошельками и устройствами, работающими с платежными картами (банкоматами, POS-терминалами, платежными киосками и т.д.). Также, могут использоваться и другие платежные инструменты в различных формах: браслетов, брелков, блоков мобильных телефонов и т.д., имеющих специальные платежные чипы.

Таким образом, функционирование и безопасность проведения электронных платежей определяется безопасностью и функционированием сетевых технологий, что является одной из уязвимостей использования электронных денег.

Так, очевидно, что при отсутствии возможностей входа в сеть, работа тс электронными кошельками станет невозможной. Также любое нарушение безопасности при работе с компьютерными сетями может привести к сбоям в использовании электронных денег.

В рамках данной работы проведен анализ вопросов обеспечения безопасности при использовании электронных денег.

1.2 Свойства электронных денег

Электронные деньги имеют достаточно более широкие свойства, чем их обычные аналоги, и при этом для них характерна своя специфика [5].

Рассмотрим перечень основных свойств электронных денег.

Свойство анонимности – при отправке и получении денег существует имеют право анонимности отправителя и получателя платежа. В общем случае необходимо обеспечение секретности при проведении операций.

В настоящее время регламентирующими органами данное свойство электронных денег стараются ограничить, так как оно позволяет проводить трансграничные транзакции для финансирования терроризма, сомнительных финансовых операций и преступных схем. Анонимные операции, согласно законодательству РФ в настоящее время не превышают 15000 руб. как на отправку, так и на получение.

Свойство безопасности предполагает возможность использования средств защиты информации (например, криптографических систем). Учитывая то, что процесс перевода электронных денег представляет собой лишь обмен информацией (с пользовательской точки зрения), таким образом, он должен производиться на условиях согласия с переводимыми суммами, которые после согласия не могут быть изменены, скопированы или удалены.

Принцип окончательности расчетов предполагает, что получатели электронных денег не должны иметь непогашенных требований по отношению к третьим лицам.

Принцип универсальности электронных денег предполагает возможность повсеместного их использования. По сути, это дает возможность мобильности пользователей посредством:

- Совместимости платежных систем;
- Использования электронных терминалов;
- Использования площадей обслуживания.

Принцип оффлайновой совместимости необходим для обеспечения пользователей электронных денег при проведении переводов (оплат товарной продукции и услуг) можно было бы не проводить аутентификацию к третьей стороне (например, осуществлять покупки товаров с использованием карте в момент отсутствия связи с аутентификатором).

Принцип двусторонности - это свойство, которое обуславливает возможность отсутствия в расчетах третьей стороны, производящей авторизацию сделки.

Возможность поддержки микроплатежей, что необходимо для проведения платежей в небольших суммах, что зачастую не обеспечивает рентабельность проведения операции. Суть микроплатежей на примере наличных денег предполагает аналогию покупки товара стоимостью в десятки рублей, имея крупную купюру для расчета. Суть микроплатежей с использованием электронных денег предполагает оплату платежей в размерах порядка нескольких рублей, при этом платежная система несет траты на оформление расчета, чем имеет комиссионные с проведенной операции. Некоторые платежные системы выставляют требования к минимальному размеру платежа.

Принцип делимости – возможность размена электронных денег.

Принцип портативности электронных денег, что связано с мобильностью их обладателя. Данное свойство является частным случаем универсальности электронных денег.

Принцип удобства использования - это также является частным случаем универсальности электронных денег, при котором участниками денный вид денег принимается их к оплате, также сторонами имеется определенная степень доверия к электронным деньгам, связанная с простотой и надежностью использования. Электронные деньги, в свою очередь, проистекают из наличия всех вышеперечисленных свойств, частью которых обладают только электронные деньги.

Ряд свойств, такие как свойства ликвидности, деноминируемости, и, следовательно, долговечности наследуются системами электронных денег от обычного наличного оборота.

Таким образом, системы электронных денег на сегодняшний день имеют большее количество свойств, чем обычные деньги, которые не соответствуют требованиям времени, но пока используются ограниченным количеством участников электронного оборота денег.

1.3 Преимущества и недостатки электронных денег

Владельцы электронных кошельков при их использовании получают довольно обширный перечень удобств и преимуществ. Это предполагает, прежде всего, что имеется большой перечень различных товаров и услуг, которые можно оплачивать с

использованием электронных денег, со своего рабочего места или с использованием домашнего компьютера. Данные преимущества предполагают рост числа пользователей электронных платежных систем. Главным преимуществом при проведении удаленных оплат является значительная экономия времени. При этом определенные виды товаров и услуг приобретаются исключительно с использованием электронных денег. Электронные деньги могут быть особенно полезными и удобными при проведении массовых платежей небольшими суммами. Например, при оплате транспортных услуг, кинотеатров, клубов, расчетах за коммунальные услуги, оплате различных штрафов, проведении расчетов в интернете за электронные услуги или Интернет-магазины и т.д. Технология проведения платежей с помощью электронных денег является достаточно простой, при этом получатели получает платеж практически мгновенно.

Расчет электронными деньгами аналогичен аналогичным операциям с наличным оборотом, так как в обеих случаях платеж может быть не персонифицирован.

Определим основные преимущества использования электронных денег [13]:

1. Доступность – для любого пользователя доступна возможность по открытию электронного счета и использования его в каких-либо местах, в независимости от местонахождения денег в текущий момент.

2. Скорость, что предполагает оплату платежей посредством электронных денег в течение считанных секунды. Момент проведения платежа может быть зафиксирован электронными системами, что снижает воздействие человеческого фактора.

3. Фактор мобильности - в данном случае местонахождение владельцев электронных счетов не имеет значения, для доступа к электронным кошелькам необходимо наличие соединения с Интернетом, компьютеров, а в некоторых случаях специализированных программ.

4. Фактор безопасности, что предполагает - защиту от хищений, подделок, изменений номинала в процессе передачи различного рода данных, а также в процессе проведения транзакций возможно обеспечение средствами криптографии и электронными средствами аутентификации. Таким образом, данная защита более эффективна, чем физическая защита наличного оборота.

5. Легкость – проведение платежных операций не требует от пользователей дополнительных специальных знаний, причем установка при необходимости, программного обеспечения, а так же

сама работа с электронными счетами является интуитивно понятной для пользователей различной квалификации.

6. Возможность делимости и объединяемости - при проведении платежей не появляется необходимости выдавать сдачу. Нет необходимости физического пересчёта денег, данная функция переносится на инструменты хранения или платежный инструментарий.

7. Возможность портативности - величина сумм не определяется габаритами или весовыми размерами денежной массы, как в случае с наличными деньгами. Нет необходимости пересчета электронных денег, а также не нужно производить их упаковку, перевозку и организовывать специальные хранилища;

8. Эмиссия электронных денег имеет минимальную стоимость – нет необходимости в чеканке монет и печати банкнот, использования металлов, бумаги, краски и т.д. Электронные деньги имеют идеальную сохраняемость - не теряют своих качеств со временем. Идеальная качественная однородность - отдельные экземпляры электронных денег не имеют уникальных свойств.

К преимуществам электронных денег относятся возможности владельцев по получению и выдаче кредитов. Также к достоинствам цифровых денег относятся свойства мультивалютности и многобанковости.

Таким образом, электронные деньги, имея самостоятельное обращение, являются достаточно привязанными к бумажным эквивалентам. Для любого времени суток есть возможность обмена их на рублевые или валютные эквиваленты, а так же осуществление обратных процедур. Свои кошельки пользователи могут пополнять с использованием предоплаченных карт, таких как WebMoney или Яндекс. Деньги, а так же через перечисление денежных средств со своих банковских счетов или через проведение банковской операции.

Основным недостатком использования электронных денег является то, что электронные счета гарантированны 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.

Другим недостатком является то, что электронные деньги можно использовать только в рамках тех систем, в рамках которых они эмитированы. Также электронные деньги не являются

общепринятым платежным средством, которое обязательно к приему. Из-за этого все платежи, которые совершаются при помощи электронных денег, можно использовать через набор, который предоставляется оператором системы, проведение произвольных платежей в рамках системы невозможно. Это является значительным ограничителем применения электронных денег достаточно специфическими случаями. При этом развитие систем достаточно расширило ассортимент видов проводимых платежных операций.

Кроме того, осуществление переводов средств из одного кошелька в кошелек другой системы может представлять собой достаточно неудобную и дорогостоящую операцию, подобный перевод является более дорогим, чем перевод внутри платежной системы.

Несмотря на отличную портативность, системы электронных денег нуждаются в применении специальных инструментов хранения и обращения, а в случаях физического уничтожения носителей электронных денег, восстановление информации и счета является практически 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.

2.ТЕХНИЧЕСКИЕ И ИНСТРУМЕНТАЛЬНЫЕ СРЕДСТВА ЭЛЕКТРОННЫХ ПЛАТЕЖЕЙ

2.1 Общая характеристика электронных платежных систем

К основным этапам развития электронных платежных систем следует отнести:

- использование телеграфа для передачи платежных поручений (с 1880-х годов, компания Western Union);
- использование средств электронной связи для передачи данных о платежах (с 1980-х г., компания eCash);
- использование средств всемирной сети для проведения платежей (с 1990-х г.г.).

К разновидностям электронных денег относят:

Электронные кошельки на базе smart-карт. Такие карты имеют привязку к банковским счетам и представляют собой определенную сумму, которой пользователь карты, распоряжается. Наиболее известные платёжные системы на этой базе: Visacash, ecash, proton. Такие системы позволяют проводить оплату интернет-приобретений, хранить денежные средства в нескольких валютах и для управления этой системой можно использовать телефонную связь. К уязвимости данного способа платежа можно отнести возможную сомнительную законность проводимых платежных операций.

Электронные платежи на базе сетей. Для электронных систем такого денежного оборота необходима установка определенного программного обеспечения. Такие программы являются бесплатными и с развитием способностей мобильных аппаратов, созданы и мобильные приложения таких систем. В основном, ЭПС на базе сетей выбирают пользователи, имеющие дело с заработком в интернете, приобретающие товары через интернет магазины или же фирмы, которые желают расширить формы принятия оплаты за свои услуги.

Существуют также другие классификации электронных денег, которые определяют тип анонимности, государственный и не государственный вид и так далее.

С развитием интернет-технологий электронные кошельки получили широкое распространение.

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».

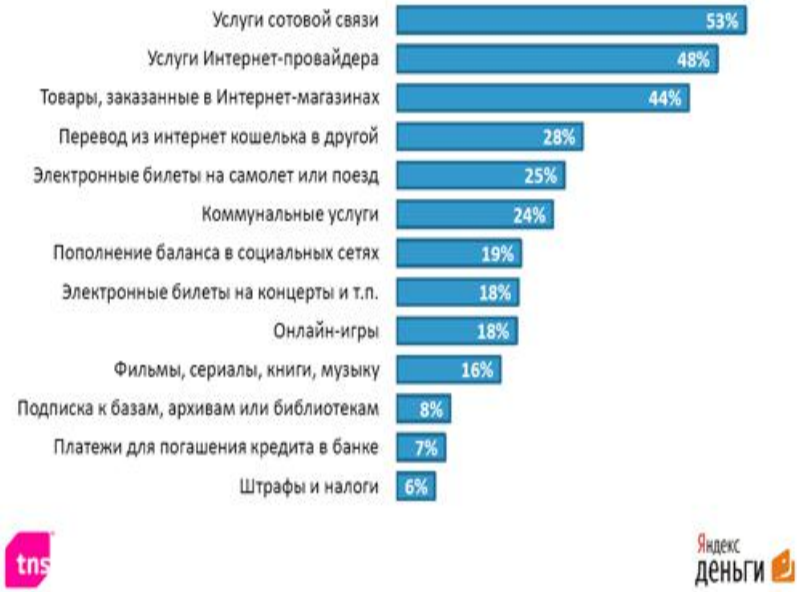

Рисунок 1 - Диаграмма основных направлений использования электронных кошельков на примере системы «Яндекс.Деньги»

Вторым по популярности платежным сервисом в условиях РФ является Киви – кошелек.

Компания основана в 2007г.

Основные возможности данной платежной системы сходны с аналогичными в «Яндекс.Деньги».

Компанией также выпускаются пластиковые карты для проведения платежей с технологией бесконтактной оплаты. Банк, курирующий работу системы – ЗАО «Киви-Банк».

В связи с ужесточением законодательства РФ в области работы с платежами – в обеих системах введены ограничения на платежи не идентифицированных пользователей (до 15000 руб. в сутки), что снизило вероятность использования систем для проведения противозаконных операций.

В настоящее время широкое развитие получили электронные кошельки, интегрированные с аккаунтами в социальных сетях. При этом они пока еще имеют ограниченный функционал, но область их использования постоянно растет.

Так, в настоящее время приобретают популярность сервисы «Одноклассники.Деньги», «Деньги.Mail.ru», основной функционал

которых – это проведение переводов и оплата сервисов на соответствующих сайтах.

На рисунке 2 показана диаграмма оборота денежных средств российскими платежными системами.

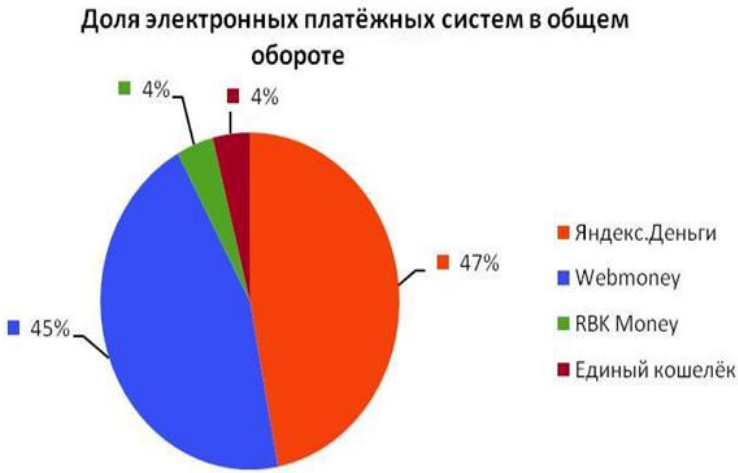

Рисунок 2 - Доля электронных платежных систем в общем обороте

На рисунке 3 показана диаграмма использования электронных кошельков при расчетах с фрилансерами.

Рисунок 3 - Диаграмма использования электронных кошельков при расчетах с фрилансерами

Динамика использования систем электронных денег в России по годам приведена на рисунке 4.

Рисунок 4 - Динамика использования систем электронных денег в России по годам

Таким образом, в России в настоящее время на рынке электронных денег удерживают лидерство системы «Киви» и «Яндекс.Деньги».

Далее рассмотрим платежные системы, используемые пользователями КНР.

1.Alipay 支付宝(самая большая и известная платежная система Китая) была создана в 1999 году и предполагалась как посредник между денежными манипуляциями между двумя другими компаниями, но в 2004 году, уже уверенная в этих делах, группа по развитию, предложила создать собственную ПС.

По мнению многих пользователей, компанией предлагаются действительно выгодные условия сотрудничества: бесплатная

регистрация, отсутствие процентов на вывод средств. При этом существуют некоторые лимиты по выводу средств, о чем сообщается пользователю в процессе регистрации.

Торговая площадка Алиэкспресс сотрудничает с Алипей и создает специальную версию Али кошелька, для более доступной оплаты товаров с этой площадки и других площадок с AlibabaGroup.

Форма авторизации в системе Alipay приведена на рисунке 5.

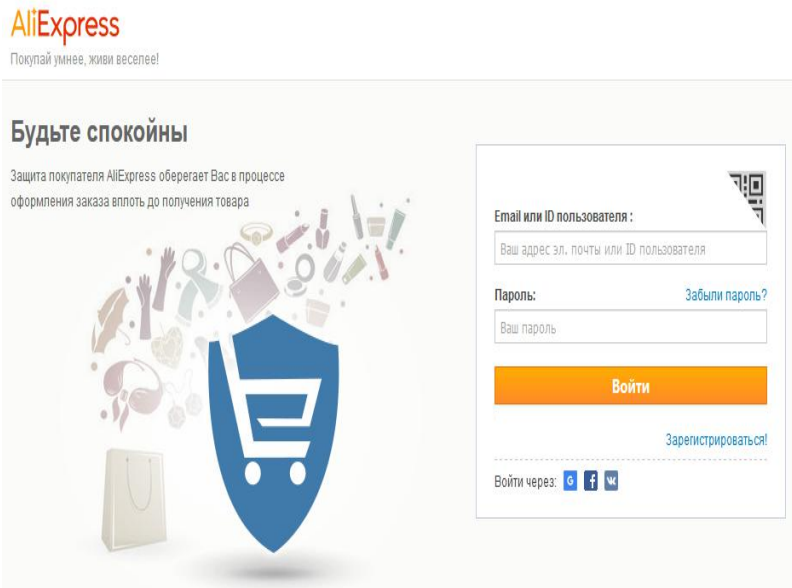

Рисунок 5 - Форма авторизации в системе Alipay

2. Tenpay 财付通

Менее популярная платежная система. Одним из ее недостатков является проблема в процессе регистрации. Имеются ограничения на набор символов в аутентификационных данных.

Данную систему оптимально использовать при оплате услуг в Китайском сегменте Интернета.

Главная форма сайта Tenpay приведена на рисунке 6.

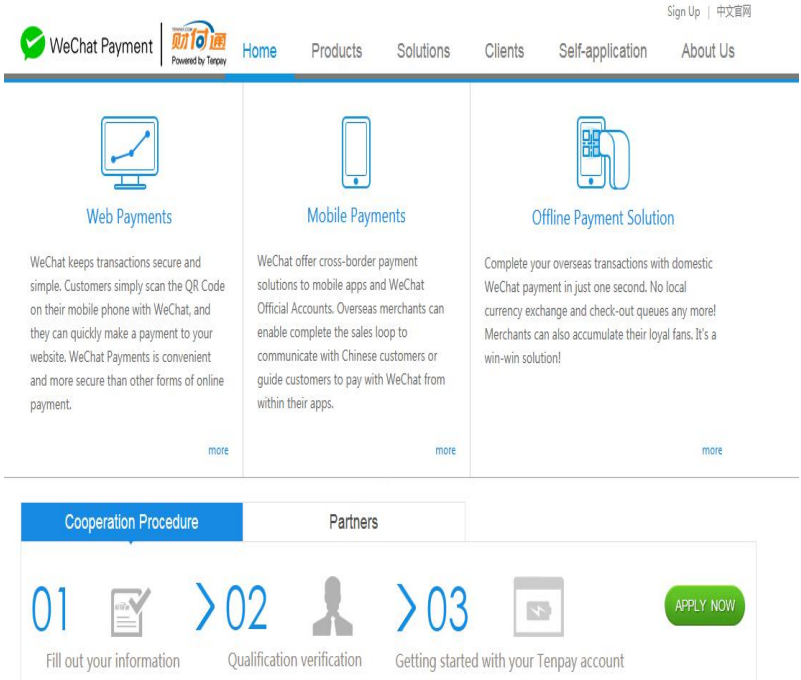

Рисунок 6 - Главная форма сайта Tenpay

3. UnionPay 银联

UnionPay была основана в 2002 году как национальная платёжная система, которая остаётся, по сей день единственной государственной ПС, с поддержкой Центрального банка КНР. В первую очередь надо сказать, что система больше координирована на выпуск пластиковых карт, нежели на оборот денег на базе сетей.

На российском рынке система UnionPay впервые работает с 2007 года. Российские держатели таких карт в моукт проводить оплату интернет услуг и покупок, проводитьобналичивание средства. Операции вывода денег на карту запрещены на уровне законодательства. В настоящий момент данные вопросы проходят стадию урегулирования.

В 2013 году ЮнионПэй стала российской платежной системой, об этом свидетельствует ее занесение в реестр платежных систем России.

Что касается развития системы на базе сетей, то оно есть, но не столь успешно по сравнению с пластиковыми картами.

К главным преимуществамиспользования электронных платежных системявляются:

Возможности без проведения безналичных оплат, переводов и прочих денежных манипуляций.

Операции, связанные с денежными переводами с электронных кошельков, проводятся мгновенно в отличие от банковских или почтовых переводов.

Денежные манипуляции производятся не выходя из дома. Доступны возможности мгновенной регистрации и начала использования системы.

Системы постоянно совершенствуют уровень защищённости при проведении платежей. При соблюдении требований безопасности, вероятность стать жертвой кибермошенничества минимальна.

Диаграмма рейтинга платежных агрегаторов приведена на рисунке 7.

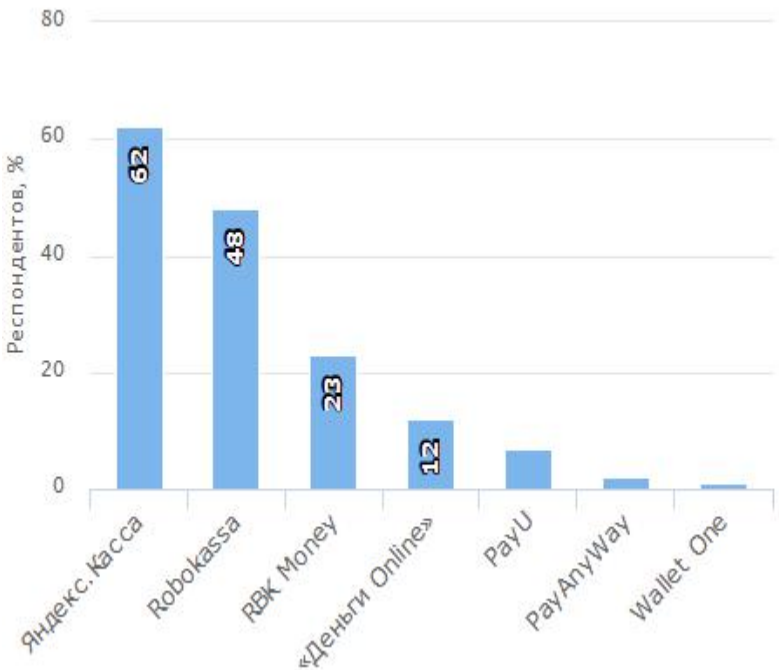

Рисунок 7 - Диаграмма рейтинга платежных агрегаторов

Рейтинг популярности электронных платежных систем по состоянию на 2016 г. приведен на рисунке 8 [22].

Рисунок 8 - Рейтинг популярности электронных платежных систем по состоянию на 2016 г

Платежи с использованием электронных кошельков предполагают меньшую комиссию, либо ее отсутствие.

Возможность ведения статистики по совершенным операциям.

2.2. Оценка рисков при использовании электронных денег

Одним из главных рисков, связанных с работой электронных платежных систем, является риск потери денежных средств, хранящихся в платежных системах.

Риски могут быть обусловлены следующим факторами:

- взлом учетных записей на платежных сервисах;
- активность вредоносного ПО;
- ввод платежной информации на фишинговых сайтах;
- непродуманную политику защиты учетной записи, допускающую ее взлом.

Источниками рисков для электронных кошельков являются:

- неквалифицированные действия самих пользователей;
- активность вредоносных систем;
- ошибки в работе платежных систем, приводящие к ошибкам при проведении платежей и нарушениям безопасности учетных записей.

В силу большого 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 использовать оптимальные настройки 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 аккакунтов 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.

3. МЕТОДЫ ЗАЩИТЫ ОТ РИСКОВ ПРИ РАБОТЕ С ЭЛЕКТРОННЫМИ ДЕНЬГАМИ

3.1. Алгоритмы использования систем безопасности при использовании электронных денег

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.

Основными способами защиты при проведении электронных платежей являются [14]:

- наличие платежного пароля к системе;
- наличие многофакторной аутентификации в системе;
- подтверждение платежа посредством СМС;
- введение лимитов на проведение платежей в течение суток, либо проведение усиленной аутентификации при проведении платежей большими суммами;
- введение системы идентификации пользователя.

Также для проведения электронных платежей необходимо наличие защищенных каналов связи, позволяющих защититься от сетевых атак при проведении транзакций, наличие выделенных защищенных соединений с серверами банков, наличие стандартных систем защиты (антивирусные системы, систем физической защиты, криптографические системы, системы аутентификации и разграничения доступа)

К снижению степени защищенности средств, находящихся в электронных кошельках можно отнести:

- привязка электронных кошельков к ящикам электронной почты или аккаунтам в социальных сетях;
- привязка электронных кошельков только к номерам мобильных телефонов;
- привязка систем электронных платежей к сайтам-партнерам, не обеспечивающим безопасность проведения платежа;
- организационные ошибки в системе восстановления доступа;
- отсутствие многофакторной аутентификации.

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

Таблица 1- Анализ защищенности платежных систем

Критерий защищенности	Яндекс. Деньги	Киви	Сбербанк. Онлайн	ePayments
Платежный пароль	+	-	-	+
Многофакторная аутентификация	-	-	+	+
Подтверждение платежа через СМС	+	+	+	+
Суточные лимиты	При отсутствии идентификации пользователя	При отсутствии идентификации пользователя	+	При отсутствии идентификации пользователя
Наличие системы идентификации	+	+	Производится специалистами Банка	+
Возможность входа в систему напрямую из стороннего приложения	+	-	-	-
Возможность перехода к платежам из системы сайтов-партнеров	+	+	-	-
Возможность аппаратной аутентификации	-	-	+	-
Привязка банковских карт	+	+	+	-

Таким образом, как показано в таблице 1, многие платежные системы, создавая удобства при проведении платежей через возможность прямого перехода к оплате со сторонних сайтов, прямой аутентификации в системе из почтовых ящиков и социальных сетей, пренебрегают требованиями безопасности и возлагают на пользователей системы вопросы обеспечения безопасности своих платежных аккаунтов. Тем самым пользователи платежных систем стараются не хранить большие суммы в электронных кошельках, ограничиваясь суммой на проведение небольших операций расчетов в Интернет-магазинах или других сервисов.

В рамках оценки уровня защищенности платежных систем определим возможный сценарий взлома электронных платежных систем на примере системы «Яндекс. Деньги». Данная схема имела широкую реализацию в 2012г.

1. Взлом почтовых ящиков пользователей посредством вредоносного ПО (как правило, электронные почтовые ящики защищены лишь посредством паролей).
2. Перехват управления почтовыми ящиками, смена пароля, отслеживание сумм на счетах Яндекс. Деньги.
3. Обращение в службу поддержки с целью смены привязки к номеру телефона. Изучив содержимое почтового ящика, злоумышленники могут ответить на вопросы службы поддержки, связанные с идентификацией пользователя.
4. Смена платежного пароля
5. Вывод средств, как правило, на счета мобильных телефонов с предварительно приобретенными для данных целей Сим-карт.

Главной уязвимостью системы Сбербанк-Онлайн является привязка к номеру сотового телефона и возможность вывода средств злоумышленником при получении доступа к сотовому номеру. Так, нередко возникают случаи, когда пользователи, отказавшись от номера Сим-карт и расторгнув договор с сотовым оператором, забывают отключить услугу «Мобильный Банк». Сотовые операторы по прошествии полугода продают сим-карту другому пользователю, который может получить доступ ко счетам предыдущего владельца. При этом на тот момент отсутствовали суточные лимиты вывода денег и пользователи лишались всех сумм, хранившихся в электронных кошельках.

Главной уязвимостью системы «Киви-Кошелек» также является привязка к сотовому номеру. При этом для аутентификации в системе также требуется ввод пароля, но пароли, как правило, пользователи запоминают в кэше браузера.

Наиболее защищенной системой с точки зрения безопасности является система e-payments, аутентификация и проведение платежей в которых требует знание паролей входа в систему, СМС-подтверждения и платежного пароля, что минимизирует риск взлома учетной записи. Но в силу того, что данный платежный сервис является новым в условиях РФ и в нем еще не реализована возможности оплаты услуг популярных сервисов, он не имеет достаточного распространения.

Таким образом, наименее защищенной платежной системой из рассмотренных является система Яндекс.Деньги. Наиболее безопасной – e.payments.

Вместе с этим, пользователям платежных систем необходимо принимать максимум мер по обеспечению безопасности своих учетных записей, как-либо связанных с платежными сервисами. Основными мерами предосторожности являются:

- сохранение паролей в тайне и хранение их в недоступных местах;
- пароли, связанные с платежными системами, не следует сохранять в кэше браузера;
- необходимо обеспечить достаточную сложность паролей (длина более 8 символов, наличие символов в разных регистрах, а также обязательное наличие наряду с буквенными символами цифровых);
- на компьютерах, имеющих доступ к платежным системам, необходимо наличие антивирусных систем защиты от сетевых угроз, а также систем дополнительной защиты браузеров (например, AdBlock);
- своевременное обновление операционных систем.

Ряд современных платежных систем для проведения аутентификации пользователей использует специализированые электронные ключи, на которых записываются закрытые сертификаты электронных подписей. Ключи, как правило, настроены на доступ из определенных программных продуктов, связанных с платежными системами, что исключает хищение закрытых ключей в удаленном режиме. Примером таких платёжных систем является сервис онлайн банкинга Россельхозбанка.

При работе с платежными системами, использующими криптографические системы, необходимо принятие ряда мер по обеспечению сохранности электронных ключей, к которым следует отнести:

- хранение ключей доступа в недоступных местах, исключающих их хищение;

- принятие мер по исключению несанкционированного доступа к компьютерам, на которые установлены криптографические системы через усиленную аутентификацию, возможно, через авторизацию по сертификату;

- использование аппаратного электронного ключа только при работе с платежной системой.

Преимуществом использования электронного ключа при аутентификации в платежной системе является исключение угроз, связанных с удаленным взломом аккаунта в платежной системе в силу того, что аппаратный электронный ключ находится на стороне пользователя. Недостатком использования системы является то, что при выходе из строя электронного ключа необходимы дополнительные временные и денежные затраты на восстановление ключа. Также генерация электронного ключа является затратным по времени процессом и требует визита клиента в банк, что исключает использование системы удаленными клиентами.

3.2. Перспективы развития систем безопасности при использовании электронных денег

Ситуация на банковском рынке требует постоянного повышения качества банковского обслуживания и гибкого взаимодействия с клиентом в условиях высокой конкуренции между кредитными организациями. С каждым годом подвергаются изменению не только традиционные банковские продукты, но и все более глубоко внедряются нетрадиционные – электронные банковские услуги.

Для развития электронного банкинга в последнее время складываются наиболее благоприятные условия. С каждым днем все большее количество людей доверяют электронным банковским услугам, в особенности активные пользователи сети Интернет. Это связано не только с повышением уровня безопасности операций проводимых с помощью электронных каналов связи, но и с более активным внедрением в жизнь современного человека различных технических новшеств.

Электронные банковские продукты сегодня могут использоваться в качестве общего многоцелевого эффективного платежного средства. Предоставляя широкий круг электронных банковских операций, эти продукты становятся реальной заменой бумажных банкнот в небольших розничных операциях, а в перспективе – и в более крупных масштабах.

Современные тенденции электронных банковских услуг позволяют объединить электронные деньги и банковские карты и проводить уже более разнообразные операции с помощью сети Интернет.

Вполне очевидно, что электронные средства оплаты и электронные банковские услуги вполне способны вытеснить традиционные, потому что эти сервисы предлагаю более удобные, быстрые, функциональные и мобильные способы оплаты [15].

Одним из перспективных направлений развития электронного банковского обслуживания является использование одноразовых паролей для идентификации клиента. Но качественно новые изменения в электронный банкинг обещает внести использование биометрических данных для аутентификации клиента. В инновационных банках мира биометрические технологии будут испытываться в пилотном режиме в ближайшее время. Эти системы основываются на распознавании отпечатков пальцев, голоса, лица, сердечного ритма и многое другое [11].

Согласно исследованиям ведущих аналитических агентств «BiometricsforBanking; Market&TechnologyAnalysis, AdoptionStrategies&Forecasts 2015–2020», биометрические технологии в банковской сфере будут использовать свыше миллиарда человек к 2017 году.

Основатель «GoodeIntelligence» Алан Гуд, утверждает, что в последнее время в мире создаются наиболее благоприятные условия для использования биометрической идентификации клиента, как с технической стороны, так и с правовой. Это является причиной возрастающего интереса к данному виду идентификации клиента среди банков, и внедрению наиболее удобных методов биометрической верификации на более высоком уровне.

Агентство «GoodeIntelligence» прогнозирует, что в конце 2015 – начале 2016 года уже 450 миллионов клиентов банков будут совершать операции в банковской сфере посредством биометрии. К примеру, в таких операциях как снятие наличных в банкоматах, идентификация личности в телефонном разговоре с оператором, а также авторизация в мобильном банковском приложении.

К тому же агентство выявляет тенденции, составляющие будущее процесса распознавания клиента банка:

- более тесное объединение с системой выявления мошенничества, включая использование поведенческого биометрического анализа;

- мобильная, предусматривающая несколько способов применения биометрическая верификация клиента;

- ассиметрия скорости внедрения (региональная неравномерность) [22].

В исследовании агентства упоминается также о том, что в ближайшие годы финансовые индустрии стран Европы, Китая и Северной Америки перейдут на использование национальных идентификационных систем, использующие биометрические данные для идентификации клиента. Регуляторы в свою очередь будут указывать на необходимость использования двух- или многофакторные биометрические системы, а также биометрических банковских карт национальной идентификационной системы. Банкоматы с биометрической идентификацией будут распространятся, как в тех регионах, где они уже используются, так и в тех, где единственным способом верификации клиента является ПИН-код. Кроме того, будет широко использоваться биометрический функционал современных смартфонов.

По прогнозам компании «JavelinStrategy&Research», будет внедрятся такая система распознавания клиента по биометрическим данным, которая использует для идентификации электро-кардиограмму человека. Это такие же уникальные биометрические данные как отпечаток пальца или голос человека. Компания «Bionym» разработала браслет, который по встроенному в него датчику распознает владельца по электрокардиограмме и передает сигнал с паролем, подтверждающим личность, на различные устройства, используя протокол «Bluetooth». Технологическая революция в электронной банковской сфере произойдет также, когда для идентификации клиентов банков будет использоваться портативный сканер ДНК.

Согласно данным исследования, проведенного компанией «PewResearchCentre», каждый третий взрослый житель Соединенных Штатов Америки используется в своей повседневной жизни мобильный банкинг, и сравнивая этот показатель с данными 2011 года, можно сказать, что темпы роста этого показателя равны практически 100%.

По данным Платежного Совета Великобритании, в ближайшие годы жители этой страны все более активно будут использовать электронные деньги и использовать электронные банковские услуги, а вот количество операций с наличностью и в офисах банков значительно сократится. Согласно данным Совета, через десять лет количество операций с наличными деньгами сократится на треть – с

21 миллиарда в 2012 году до примерно 14 миллиардов в 2022 году. Количество операций с чеками упадет еще более значительно. Согласно прогнозам, что количество операций с использованием чеков снизится с 477 миллионов в 2012 году до 186 миллионов в 2022 году.

Ситуация с банковскими картами складывается в прямо противоположном направлении, количество операций с пластиковыми картами вырастет на 75%. Так, в 2012 году таких операций было осуществлено в количестве 10 миллиардов, а уже к 2022 году этот показатель составит порядка 17 миллиардов. Причем наиболее часто используемыми пластиковыми картами будут дебетовые карты, которые будут носить определяющий характер в данной сфере.

Транзакции с использованием систем мобильного банкинга и Интернет-банкинга вырастет с 356 миллионов операций 2012 года до почти полутора миллиарда в 2022 году. Согласно данным экспертов, во многих развитых странах такой показатель как степень использования наличных денег с каждым годом снижается примерно на 2-7%.

Сравнительный анализ электронного банкинга в России и за рубежом позволяет сказать, что за рубежом данный показатель значительно выше в несколько раз. Уже больше 10 лет как в развитых странах основная движущая сила развития банковской сферы это электронный банкинг. То, что российский банковский сектор значительно отстает от зарубежного, может привести к тому, что российские банки не смогут конкурировать с зарубежными.

В Российской Федерации электронного банкинга находится на начальном уровне. И хотя в абсолютных показателях ситуация меняется в положительную сторону, в банках было открыто больше 30 миллионов счетов с доступом через сеть Интернет, по которым в 2014 году проводились безналичные платежи. Если рассматривать ситуацию в целом, лишь одна треть всех открытых счетов в этом году была открыта с доступом к Интернет-банкингом, в то время как в развитых странах этот показатель достигает более 96%.

При условии сохранения клиентоориентированности российских систем Интернет-банкинга в крупнейших банках страны к 2020 году можно ожидать значительного упрощения интерфейса таких систем вместе с расширением их функциональности. Основной сдерживающий фактор - проблема безопасности вместе с переходом на использование более защищенных протоков «HTPPS» практически решена, за исключением проблем повышения информационной грамотности населения.

Согласно данным аналитической компании «J'son&PartnersConsulting» к 2017 году рынок электронных банковских услуг в России может вырасти более чем в три раза [16]. Этому причиной могут послужить стремление как клиентов, так и самих банков, а также государства к развитию и распространению электронного банкинга. Клиенты в целях экономии времени требуют формирования более качественного и удобного способа оказания банковских услуг, а банки находят системы электронных банковских услуг, как способ снижения затрат, повышения комиссионных доходов и качества услуг. Государство в свою очередь, в стремлении увеличить безналичный денежный оборот также заинтересовано в развитии систем электронного банкинга, в том числе и Интернет-банкинга.

На сегодняшний день наиболее перспективными игроками на российском рынке банковских услуг являются такие банки как: Сбербанк России, ВТБ-24, Райффазенбанк, Альфа Банк, Банк Русский Стандарт, а также Тинькофф Банк. Эти кредитные организации наиболее активно внедряют электронные банковские услуги на российском финансовом рынке, они учитывают складывающие потребности клиентов и стараются предложить новейшие продукты в сфере электронного банковского обслуживания. Самые популярные системы интернет-банкинга России - Сбербанк Онлайн, Альфа-Клик, Телебанк ВТБ24, а также сервисы Банка Тинькофф и Банка Русский Стандарт. На их долю приходится 58 % пользователей глобальной сети Интернет и 87 % пользователей интернет-банкинга страны. Что касается клиентского проникновения, то тут лучшие результаты показывают Сбербанк России, Банк Авангард и Ситибанк. Их системами электронного банковского обслуживания через Интернет пользуются 65 – 66 % клиентов.

3.3. Основные особенности реализации VPN на основе OpenVPN

Работа с электронными деньгами, как правило, предполагает необходимость использования сетевых соединений. При проведении платежей с использованием средств Интернета необходимо принятие мер по защите сетевых соединений. Одним из методов защите сетей является создание туннелированных каналов (VPN).

Сетевая защита при проведении платежей с использованием электронных денег обеспечивается с использованием технологий VPN.

VPN представляет собой логическую сеть, создаваемую поверх другой сети, например Internet. Несмотря на то, что сетевые соединения производятся с использованием публичных сетей и небезопасных протоколов, где используется шифрование производится создание закрытых от посторонних каналов обмена данными. С помощью VPN-технологий можно проводить объединение, например, нескольких офисов организации в корпоративную сеть, в которой используются для соединения неподконтрольные каналы.

По своей сути VPN имеет многие свойства выделенных линий, при этом развертывание производится в пределах общедоступных сетей, например, Интернета. С использованием технологий туннелирования производится транслирование пакетов данных через общедоступные сети как по обычному двухточечному соединению. Каждой паре «отправитель–получатель данных» проводится установление своеобразного туннеля – безопасного логического соединения, позволяющего инкапсулировать данные одного протокола в пакеты другого. Основными составляющими туннеля являются :

- Инициаторы;
- маршрутизируемые сети;
- туннельные коммутаторы;
- туннельные терминаторы.

Технология функционирования VPN не противоречит основным принципам передачи данных в сетях. Так, при установленном удалённом со стороны клиента посылаются на сервер потоки пакетов стандартного протокола PPP. В случае организации виртуальных выделенных линий между локальными сетями их маршрутизаторы также обмениваются пакетами PPP. Тем не менее, принципиально новым моментом является пересылка пакетов через безопасный туннель, организованный в пределах общедоступной сети.

С использованием туннелирования возможно организовать передачу пакетов одного протокола в логических средах, использующих другие протоколы. В результате появляются возможности решение проблем взаимодействия нескольких разнородных сетей, начиная с необходимости обеспечения целостности и конфиденциальности передаваемых данных и заканчивая преодолением несоответствий внешних протоколов или схем адресации.

Существующая сетевая инфраструктура корпорации может быть подготовлена к использованию VPN как с помощью

программного, так и с помощью аппаратного обеспечения. Организацию виртуальной частной сети можно сравнить с прокладкой кабеля через глобальную сеть. Как правило, непосредственное соединение между удаленным пользователем и оконечным устройством туннеля устанавливается по протоколу PPP.

Существуют следующие принципы классификации VPN-сетей :

- по типам используемых сред;
- по способам реализации;
- по назначению;
- по типам протоколов.

По виду используемой среды VPN-сети подразделяются на :

Защищённые VPNсети. Наиболее распространённый вариант приватных частных сетей. Его использование позволяет создавать надежные и защищенные подсети на основе ненадёжных сетей, как правило, Интернета. Примером защищённых VPN являются: IPSec, OpenVPN и PPTP.

Доверительные VPNсети. Используются в случаях, когда передающую среду можно считать надёжной и необходимо решить лишь задачу создания виртуальной подсети в рамках большей сети. Вопросы обеспечения безопасности становятся неактуальными. Примерами подобных VPN решении являются: MPLS и L2TP. Таким образом, данные протоколы перекладывают задачу обеспечения безопасности на другие, например L2TP, как правило, используется в паре с IPSec.

В рамках данной работы проведем анализ архитектуры VPN-сетей на основе OpenVPN. Проведем рассмотрение данной технологии.

Основными компонентами OpenVPNявляются:

- сервер OpenVPN;
- удостоверяющий центр;
- клиенты OpenVPN;
- сертификаты;
- публичные ключи;
- приватные ключи;
- списки отозванных сертификатов;
- файл Джиффи-Хелмана;
- статический ключ.

OpenVPN — представляет собой свободную реализацию технологии виртуальных частных сетей (VPN), содержащую открытый исходный код для реализации зашифрованных каналов вида точка-точка или соединений между серверами и клиентами. Она

позволяет проводить установление соединений между компьютерами, находящимися за NAT и сетевыми экранами, без необходимости изменения их настроек. Распространение OpenVPN производится под лицензией GNU GPL.

Целью GNU GPL является предоставление пользователям прав на копирование, модифицирование и распространение (в том числе на коммерческой основе) программных продуктов, а также гарантия получения подобных прав и для пользователей.

По контрасту с GPL, лицензии проприетарного ПО «очень редко дают пользователю такие права и обычно, наоборот, стремятся к их ограничению, например, запрещая восстановление исходного кода».

Согласно лицензионной политике OpenVPN по применению лицензии GNU GPL (эти разъяснения приложены к размещённому на сайте разработчика тексту лицензии), лицензия должна в электронной форме присоединяться к компьютерным программам.

Таким образом, лицензионная политика разработчиков OpenVPN имеет ряд преимуществ перед проприентарным ПО, к которому относится большинство систем подобного рода.

ПО OpenVPN проводит передачу данных по сети с использованием протоколов UDP или TCP с применением драйверов TUN/TAP. Протоколы UDP и драйвер TUN позволяют проводить подключение к серверу OpenVPN со стороны клиентов, расположенных за NAT.

Для OpenVPN - соединения производится выбор произвольного порта, дает возможность для преодоления ограничений файерволов, через которые производится доступ из локальной сети в Интернет (при наличии таких ограничений).

Технологии обеспечения безопасности и шифрования в OpenVPN реализованы с помощью библиотеки OpenSSL и протокола транспортного уровня TransportLayerSecurity (TLS). Вместо OpenSSL в новых версиях OpenVPN используется библиотека PolarSSL.

В OpenSSL может использоваться симметричная и ассиметричная криптография.

В первом случае процесс передачи данных на все узлы сети начинается с использования одинакового секретного ключа. При этом появляется проблема безопасности при передаче данного ключа через небезопасный Интернет.

Во втором случае для каждого из участников процесса обмена данными используются два ключа — публичный (открытый) и приватный (секретный). Публичные ключи используются в процессе

шифрования данных, а приватные — при расшифровке. Основой технологии шифрования является сложный математический аппарат. Выбранные в SSL/TLS алгоритмы шифрования с использованием публичных ключей обеспечивают возможность расшифровки только с помощью приватных ключей.

Приватные ключи являются секретными, и должны находиться в пределах узла, где они были созданы. Публичные ключи должны передаваться всем сторонам файлового обмена.

Безопасность передачи информации предполагает необходимость идентификации сторон, принимающих участие в файловом обмене. В иных случаях сеть может быть подвергнута «атакам посредников» (ManintheMiddle, MITM). Данный тип атаки предполагает возможность подключения злоумышленника к каналам передачи данных и их прослушивания. Злоумышленники также могут вмешиваться, проводить удаление или изменение данных.

Для обеспечения аутентификации (проверки подлинности пользователей) протоколы TLS используют инфраструктуру публичных ключей (PublicKeyInfrastructure, PKI) и технологии асимметричной криптографии.

Необходимо иметь в виду, что расшифровка данных без использования приватных ключей также возможно, например, с использованием методов последовательного перебора. Хотя данный метод и требует значительных вычислительных ресурсов, это является вопросом времени, в течение которого можно провести расшифровку данных.

Хотя размер ключа влияет на длительность процесса расшифрования, никакие ключи не дают гарантий полной безопасности данных. Кроме того, существует вероятность похищения уже расшифрованных данных и ключей за счет уязвимостей и закладок в операционной системе или прикладном ПО, а также в аппаратном обеспечении серверов и рабочих станций.

Технология OpenVPNпредполагает возможности нескольких видов аутентификации:

- вход с помощью предустановленного ключа, что является наиболее простым методом;
- вход по сертификату;
- с использованием пары «логин - пароль».

Необходимым компонентом, даже в случае аутентификации через логин-пароль является сертификат сервера.

Сертификаты выпускаются удостоверяющим центром.

Заверение сертификата, как правило, проводит аккредитованная доверенная организация. Эта организация выполняет роль удостоверяющего центра.

При создании открытого ключа для публичного использования, в качестве удостоверяющего центра могут выступать аккредитованные коммерческие или государственные организации. Данная организация проводит публикацию собственного открытого ключа, доступного всем.

Существует большое количество коммерческих организаций, оказывающих услуги по выпуску сертификатов, пригодных, например, для создания HTTPS-сайтов, для цифровой подписи сообщений электронной почты или документов, для систем мгновенного обмена сообщениями, такими как Jabber. Выдача данных сертификатов производится выдаются на ограниченный срок и является платной услугой.

Но для сетей VPN, создаваемых для своей компании, есть возможность самостоятельного создания своего удостоверяющего центра CA и выпуска так называемых самоподписанных сертификатов. Конечно, доверие к данным сертификатам не будет выходить за пределы организации, но во-первых, этого будет вполне достаточно, а во-вторых, самоподписанные сертификаты совершенно бесплатны.

Самоподписанные сертификаты в технологиях Open VPN играют роль публичных ключей, с использованием которых узлы сети Open VPN будут проводить шифрование данных. Для расшифровки данных в данном случае используются приватные ключи.

Создание сертификатов производится в соответствии со стандартом X.509. Данный стандарт определяет форматы данных и процедуры распределения открытых ключей с помощью сертификатов, снабженных электронными подписями.

Технологии OpenVPNмогут быть реализованы на различных платформах.

1.Для FreeBSD:

- обновление портов с использованием команд:

portsnapfetch

portsnapextract

- синхронизация по времени между узлами сети:

ntpdate 1.pool.ntp.org

- Установка утилиты Easy-RSA

- Конфигурирование сервера

Файлы конфигурации сервера OpenVPN при его установке в ОС FreeBSD необходимо размещать в каталоге /usr/local/etc/openvpn.

mkdir /usr/local/etc/openvpn

- Добавление пользователей с использованием команды adduser;
- Запускагентов:

openvpn_enable="YES"

openvpn_configfile="/usr/local/etc/openvpn/server.conf"

- Установка SQID

cd /usr/ports/www/squid33

make install clean

2. Для ОС Windows

Этапы работы:

- установка GUIOpenVPN;
- создание запросов на сертификат;

cdC:\ProgramFiles\OpenVPN\easy-rsa

init-config.bat

clean-all

- получение сертификата;
- создание конфигурационного файла;
- запуск GUIOpenVPN.

3.4 Использование антивирусных систем при работе с электронными деньгами

Работа с электронными деньгами предполагает использование компьютерной техники, что связано с необходимостью обеспечения систем антивирусной защиты. Приведем обзор антивирусных решений для обеспечения защиты электронных кошельков.

Существует большое количество различных антивирусных программ как российских, так и зарубежных производителей.

Проведем анализ наиболее распространенного антивирусного ПО.

Рассмотрим более подробно такие антивирусные решения, как:

1. KasperskyEndPoint Security 10;
2. Dr. WebSecurity Space 10;
3. Panda Antivirus;
4. NOD 32.

При выборе того или иного антивирусного решения в условиях информационных систем предприятий необходимо учитывать следующие критерии:

- функциональность (статистика противодействия активности вредоносного ПО);
- совместимость с архитектурой информационной системы предприятия;
- наличие корпоративных версий;
- наличие средств централизованного администрирования;
- степень замедления системы;
- системные требования;
- стоимость.

Из всех рассмотренных антивирусов наиболее наименьшую стоимость имеетPanda Antivirus, а наибольшую -NOD 32.

Решения от Kaspersky, DrWeb, Nod32 имеют корпоративные версии, включающие возможности централизованного управления, PandaАнтивирус не предоставляет возможности реализации корпоративных решений.

Все виды рассмотренного программного обеспечения предлагают надежную защиту всех видов вредоносного программного обеспечения. Проверка файлов в таких программах, как Dr. Web, NOD 32, осуществляется при запуске системы, а вот Антивирус Касперского проверяет файлы в момент обращения к ним. KasperskyEndPointSecurity, NOD 32 в отличие от всех остальных обладают продвинутой системой проактивной защиты, основанной на алгоритмах эвристического анализа; возможностью защиты паролем и, тем самым, возможностью защиты программы от вирусной активности, нацеленной на разрушение АВЗ. Кроме этого,Kaspersky EndPoint Security обладает поведенческим блокиратором. Panda Antivirus, в отличие от остальных рассмотренных, не поддерживает блокировку подозрительных веб-страниц или защиту личных данных. Все указанные виды антивирусного ПО обладают возможностью автоматического обновления сигнатур и планировщик задач. Кроме этого, указанные антивирусные решения полностью совместимы с современными версиями операционных систем.

В рамках выполнения данной работы мной было проведено исследование корпоративных версий антивирусного ПО на компьютере с конфигурацией, приведенной в таблице 2. Результаты тестирования приведены в таблице 3.

Таблица 2 - Конфигурация компьютера для тестирования антивирусного ПО

Процессор	IntelCore i5 650 3.2 ГГц
Материнская плата	ASUS P7H55M
Видеокарта	NVIDIA GeForse 210
Оперативная память	4096 MB
Жесткий диск №1	WD CWD 10EARS 00Y5B1
Жесткий диск №2	Hitachi HDP725040GLA360
Операционная система	Microsoft Windows 7 x86

Таблица 3 - Результаты тестирования антивирусного ПО

	Касперский	Nod32	Dr.WEB
Влияние на время загрузки ОС, сек	10,05	9,85	12,28
Замедление системы,%	11	14	18
Использование ОЗУ, КБ	112028	116331	130616
Использование системного кэша, КБ	174982	40248	270716
Время сканирования файлов, мин	4:09	4:13	14:32
Загрузка CPU при сканировании, %	85	30	35
Использование ОЗУ при сканировании файлов, КБ	2684575	2917154	2769985
Использование системного кэша при сканировании файлов, КБ	882044	1189388	1687355
Влияние на копирование файлов, сек	25	32	42

Kaspersky EndPoint Security

ФайловыйАнтивирус

Осуществляет контроль файловой системы компьютеров. Проводит проверку всех открываемых, запускаемых и сохраняемых файлов, находящихся на компьютерах пользователей, а также загружаемых из Интернета. Прикаждом обращении к файлу производится перехват антивирусоми проверка на наличие известных вредоносных программ. Дальнейшая работа с файлами возможна только в тех случаях, когда не определены признаки заражения файла

или проведено успешноеих лечение. При невозможности лечения файлов проводится их удаление, либо помещение в карантин [16].

С помощью почтового антивируса проводится проверка всех пользовательских входящих и исходящих почтовых сообщений. Также проводится анализ электронных писем на наличие вредоносных программ. Работа с почтоввм отправлением будет доступна адресату только в тех случаях, если в нем не содержаться опасные объекты. Также, компонентом проводится анализ почтовых сообщений на наличие фишинг-мошенничества.

Также компонентами системы антивирусной защиты являются [3]:

- Web-антивирус (проводит анализ скриптов, выполняемых при загрузке Web-страниц);
- IM-антивирус (контроль активности мессенджеров);
- Контроль активности программ (анализ работы установленного ПО на наличие вредоносных функций);
- Сетевой экран (обеспечение безопасности работы в Интернете);
- Проактивная защита (анализ поведения программ, на основе которого определяется степень их потенциальной вредоносности);
- Модуль защиты от сетевых атак (проводится анализ трафика на предмет наличия сетевых атак);
- Анти-спам (поддержка функционала почтовых клиентов и серверов на наличие нежелательной почты)

К корпоративным решениям лаборатории Касперского относят:

- Агент администрирования (обеспечивает связь сервера антивирусной защиты с рабочими станциями);
- Консоль Администратора (Управление антивирусной защитой).

Dr. Web

Данная система имеет возможность установки на зараженные компьтеры. Начиная с версии 8.0, установка осуществляется посредством нового защищенного инсталлятора, противодействующего основным типам вредоносных программ, что позволяет проводить корректную установку антивируса на зараженную систему. В ходе установки производится обновление антивирусных баз и исполняемых компонент системы.

Система использует технологию OriginsTracing, содержащую алгоритмы несигнатурного детектирования вредоносного ПО, дополняющую традиционные технологии сигнатурного поиска и эвристического анализатора, дает возможности для значительного

повышения уровня детектирования ранее неизвестных вирусов. Система также может использоваться и в мобильных версиях приложения.

Модуль Anti-rootkit API (ArkAPI), использует универсальные технологии по нейтрализации угроз. С помощью данной системы проводится нейтрализация угроз с помощью всех компонент антивирусной системы. Так же применяется в лечащих утилитах Dr.WebCureIt!.

Модуль Dr. Web Shield представляет собой механизм борьбы с руткитами, реализованный в форме драйвера. С его использованием обеспечивается низкоуровневый доступ к вирусным объектам, скрывающимся в модулях и системных файлах операционных систем.

Также система включает корпоративные решения, аналогичные программам от Касперского, а также облачные сервисы, позволяющие проводить проверки системы в режиме онлайн.

Panda Antivirus

Антивирус Panda Cloud функционирует с использованием вычислительных способностей локальных компьютеров и удалённых серверов Panda Security. Облачные технологии, используемые системой, основаны на функциях Collective Intelligence, собирающих, анализирующих, категоризирующих и выполняющих лечение файлов. Все определения вредоносных объектов проводятся именно на удалённых серверах, что избавляет пользователей от необходимости загружать обновления антивирусных баз. На компьютерах пользователей работают эвристические анализаторы и инструменты для постоянного сканирования, имеющие следующие уровни приоритета:

- Модуль мгновенного сканирования, проверяющий все активные процессы, программы и файлы.
- Модуль сканирования с упреждающей выборкой — антивирусом откладывается сканирование файлов, загруженных из сети Интернет или с внешних носителей, но не запущенных пользователем, на то время, пока не совершатся рутинные действия с высоким приоритетом. Если пользователь начнёт работать с данными файлами, то они будут перенесены в категорию для мгновенного сканирования.
- Фоновое сканирование — антивирус в фоновом режиме сканирует все файлы системы, пока пользователь не работает с компьютером.

При сканировании антивирус может создавать особые кэши, которые позволяют при повторном сканировании значительно сократить время проверки компьютера.

NOD32

Сканер по запросу, который можно запустить вручную для проверки отдельных файлов или разделов диска. Этот модуль также может быть запущен в часы с наименьшей загрузкой с помощью планировщика.

InternetMONitor (IMON)

Резидентный сканер, работающий на уровне Winsock и препятствующий попаданию зараженных файлов на диски компьютера. Данный модуль проверяет HTTP-трафик и входящую почту, получаемую по протоколу POP3.

Данный модуль в версиях 2.x может конфликтовать с некоторыми службами Windows Server и с некоторыми межсетевыми экранами (например, Kerio WinRoute). При установке система исследуется на возможность конфликтов и, если существует вероятность конфликта, выводится сообщение, предлагающее отключить этот компонент.

E-mailMONitor (EMON)

Дополнительный модуль для проверки входящих/исходящих сообщений через интерфейс MAPI, например, в Microsoft Outlook и Microsoft Exchange.

Document MONitor (DMON)

Использует запатентованный интерфейс Microsoft API для проверки документов Microsoft Office (включая Internet Explorer).

Состав версии 4.x

Модуль защиты от вирусов и шпионских программ

В этом модуле используется ядро сканирования на основе технологии ThreatSense. Ядро Threat Sense оптимизировано и улучшено в соответствии с требованиями новой архитектуры ESET Smart Security.

Персональный брандмауэр

Персональный брандмауэр отслеживает весь трафик между защищаемым компьютером и другими компьютерами сети.

Модуль защиты от нежелательной почты

Модуль защиты от нежелательной почты ESET фильтрует нежелательную почту, повышая уровень безопасности системы и удобство использования обмена данными по электронной почте.

Прочие компоненты:

ESET SysRescue

ESET SysRescue позволяет пользователям создавать загрузочный носитель CD, DVD или USB с программой ESET SmartSecurity, который может запускаться независимо от операционной системы. Он предназначен главным образом для работы с трудноудаляемыми вирусами.

ESET SysInspector

Когда для отправки запроса в службу поддержки клиентов используется раздел «Справка и поддержка», можно добавить снимок состояния компьютера в ESET SysInspector.

Защита документов

Функция защиты документов сканирует документы MicrosoftOffice перед их открытием, а также проверяет файлы, автоматически загружаемые браузером InternetExplorer, например элементы MicrosoftActiveX.

Составверсии 5.x

ESET Live Grid

Обеспечивают надежную защиту от Интернет-угроз и вредоносных программ в режиме реального времени.

ParentalControl

Защищает Вашу семью от потенциально нежелательного веб-контента, блокируя определенные категории веб-сайтов.

EnhancedMediaControl

Автоматическое сканирование всех USB-носителей, карт памяти, CD/DVD-дисков. Блокировка медиа носителей в зависимости от типа носителя, производителя, размера и других параметров.

Advanced HIPS Functionality

Позволяет настраивать поведение системы в целом и каждой её части. Пользователи могут установить правила для системной регистрации, процессов, приложений и файлов.

GamerMode

Обеспечивает автоматический переход в «беззвучный» режим во время работы в полноэкранном режиме.

Рассмотрев функциональность антивирусного программного обеспечения, можно сделать выводы:

- наиболее оптимальным решением для реализации корпоративной антивирусной защиты является KasperskyEndPointSecurity. Данное решение определено по параметрам функционирования данного решения (степень загруженности системы, времени проверки файлов, количеством сигнатур, требования к аппаратному обеспечению, наличие средств администрирования и централизованного

управленияKasperskySecurityCenter и наличия реализованных в них возможностях, что приведено в таблице 3);

- в качестве дополнительного антивирусного решения оптимально использование решений от DrWeb. Достоинством данного решения помимо стандартных антивирусных сервисов – это выпуск системы проверки системы DrWebCureIt, наличие корпоративных решений и системы централизованного управления АВЗ;

- решения на основе PandaАнтивирус не подходят для использования в информационных системах предприятий, так как не предоставляют возможности централизованного управления системой АВЗ.

ЗАКЛЮЧЕНИЕ

В данной работе рассмотрены вопросы обеспечения безопасности при проведении электронных платежей и использования электронных денег. Актуальность данной работы обусловлена тем, что в связи с распространением телекоммуникационных технологий возрастает объем платежей, проводимых дистанционно с использованием электронных средств. В настоящее время электронные кошельки используются для решения множества задач, к которым относятся:

- оплата счетов;
- оплата услуг в Интернете;
- денежные переводы;
- привязка к банковским картам.

Системы, использующие электронные платежи, в целом являются менее затратными по сравнению с традиционными технологиями денежного обращения, но при этом для внедрения электронных платежных систем требуется обеспечение безопасности проведения платежных операций.

В рамках данной работы проведено решение следующих задач:

- 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.

В рамках данной работы дана оценка уровню защищенности в наиболее распространённых платежных системах, проведена формулировка основных видов уязвимостей. Также в ходе анализа технологий работы с электронными кошельками было проведено сравнение платежных систем России и Китая. Было показано, что электронные кошельки в этих странах имеют схожий функционал, но при этом ограничено их использование на территориях других стран. Также имеются ограничения в соответствии с законами государств.

Также показано, что для обеспечения сохранности средств в электронных кошельках необходимо соблюдения требований безопасности не только со стороны платежных операторов, но и самими пользователями. В связи с этим необходимо повышения уровне грамотности пользователей в области технологий информационной безопасности.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Электронные платежные системы в России // TAdviser портал выбора технологий и поставщиков. URL: http://www.tadviser.ru/index.php/ (дата обращения: 20.03.2017).

2. Количество банковских карт в России // Статистика национальной платежной системы сайта. URL: http://www.cbr.ru/statistics/print.aspx?file=p_sys/sheet013.html (дата обращения: 10.04.2017).

3. Количество пользователей Сбербанк-Онлайн // Анализ сайта. URL: http://www.my-sberbank.ru/chislo-polzovatelej-servisa-sberbank-onlajn-prevysilo-6-millionov-chelovek.html (дата обращения: 07.04.2017).

4. Особенности работы банков с пластиковыми картами // Особенности анализа работы банка с пластиковыми картами. URL: http://www.bankir.ru/publikacii/20121112/osobennosti-analiza-raboty-banka-s-plastikovymi-kartami-10002526/ (дата обращения: 28.03.2017).

5. Популярные платежные системы России и Китая // Электронные платёжные системы сайта. URL: http://www.web-klik.ru/elektronnye-platyozhnye-sistemy/#i-2 (дата обращения: 31.03.2017).

6. Бабаш, А. В. Информационная безопасность. Лабораторный практикум: Учебное пособие / А. В. Бабаш, Е. К. Баранова, Ю. Н. Мельников. М.: КноРус, 2013. 136 с.

7. Баймакова, И. А. Обеспечение защиты персональных данных / И. А. Баймакова. М.: Изд-во 1С-Паблишинг, 2010. 216 с.

8. Гафнер, В. В. Информационная безопасность: Учебное пособие / В. В. Гафнер. - Рн/Д: Феникс, 2010. 324 с.

9. Гашков, С. Б. Криптографические методы защиты информации / С. Б. Гашков, Э. А. Применко, М. А. Черепнев. М.: Академия, 2010. 304 с.

10. Герасименко, В. А. Основы защиты информации / В. А. Герасименко, А. А. Малюк. М.: МИФИ, 1997. 271 с.

11. Грибунин, В. Г. Комплексная система защиты информации на предприятии / В. Г. Грибунин, В. В. Чудовский. М.: Академия, 2009. 416 с.

12. Громов, Ю. Ю. Информационная безопасность и защита информации: Учебное пособие / Ю. Ю. Громов, В. О. Драчев, О. Г. Иванова. М.: Форум, 2010. 384 с.

13. Емельянова, Н. З. Защита информации в персональном компьютере / Н. З. Емельянова, Т. Л. Партыка, И. И. Попов. М.: Форум, 2009. 368 с.

14. Ефимова, Л. Л. Безопасность проведения платежей Российский и зарубежный опыт: Монография / Л. Л. Ефимова, С. А. Кочерга. М.: ЮНИТИ-ДАНА, 2013. 239 с.

15. Завгородний, В. И. Комплексная защита в компьютерных системах: Учебное пособие / В. И. Завгородний, Н. А. Егоров. М.: Логос ПБОЮЛ, 2001. 264 с.

16. Грекул, В. И. Проектирование информационных систем / В. И. Грекул, Г. Н. Денищенко, Н. Л. Коровкина. М.: ИНТУИТ.ру, 2013. 135 с.

17. 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.

18. 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.

19. Днепров, А. Г. Microsoft SQL Server 2008. Самоучитель / А. Г. Днепров, М.: Финансы и статистика, 2012. 361 с.

20. Емельянова, Н. З. Защита информации в персональном компьютере / Н. З. Емельянова, Т. Л. Партыка, И. И. Попов. М.: Форум, 2013. 368 с.

21. Обзор агрегаторов для приема платежей // Платежные системы сайта. URL: https://www.habrahabr.ru/company/web_payment_ru/blog/265349/ (дата обращения: 16.03.2017).

22. Рейтинг платежных систем 2016 // Рейтинги платежных инструментов. URL: http://www.tagline.ru/payment-systems-rating/ (дата обращения: 21.03.2017).

23. Электронные кошельки // Обзор популярных платежных систем. URL: http://www.user-life.ru/internet/elektronnye-koshelki-obzor-populyarnyx-platezhnyx-sistem.html (дата обращения: 28.03.2017).