МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

по выполнению лабораторных работ
по дисциплине «Методы и средства защиты информации в банковских системах»
для студентов направления подготовки
10.03.01 «Информационная безопасность»
Направленность (профиль)
«Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности»

Ставрополь
2026

СОДЕРЖАНИЕ:

ВВЕДЕНИЕ

Целью изучения дисциплины «Методы и средства защиты информации в банковских системах» является формирование у студентов способностей решать профессиональные задачи по обеспечению информационной безопасности в банковских системах путем применения современных методов и средств защиты информации, а также приобретение набора общепрофессиональных компетенций будущего бакалавра по направлению подготовки 10.03.01 «Информационная безопасность».
Задачами дисциплины являются:

1. Раскрытие сущности и значения информационной безопасности в банковских системах, их места в системе национальной безопасности.
2. Определение теоретических, концептуальных, методологических, организационных и технических основ обеспечения безопасности информации в автоматизированных банковских системах.

Перечень планируемых результатов обучения по дисциплине (модулю), соотнесённых с планируемыми результатами освоения образовательной программы

Код, формулировка компетенции	Код, формулировка индикатора	Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций, индикаторов
ПК-1 Способен обеспечивать защиту от несанкционированного доступа сооружений и средств связи сетей электросвязи (за исключением сетей связи специального назначения) в процессе их эксплуатации (06.030 В)	ИД-1$_{ПК-1}$ Способен проводить мониторинг функционирования СССЭ, защищённости от НСД сооружений и СССЭ	определяет способы мониторинга функционирования беспроводных СССЭ и оценки их защищенности от НСД к информации

ПЛАНЫ ЛАБОРАТОРНЫХ РАБОТ

Тема 1. Базовые понятия дисциплины. Банковская система Российской Федерации.

Лабораторная работа №1-2.

Вербальное и графическое моделирование виртуального банка
Формируемые компетенции: ПК-1.
Теоретическая часть

Задание 1. Замыслить и вербально описать виртуальный банк.

Задание 2. Замыслить и разработать организационную структуру виртуального банка.

***Задание 3*.** Замыслить и составить план здания виртуального банка (не менее 2-х этажей).

Пример оформления отчета по работе

Название банка: ООО «Пантеон»

Сфера деятельности: универсальный банк, занимающийся обслуживанием физических и юридических лиц.

Количество и расположение зданий, помещений: одно здание, 2 этажа, включая помещения: операционный зал для обслуживания физических лиц; помещение для кассовых операций; помещение операторов; офис начальника операционного отдела; отдел службы безопасности; главное хранилище; зал для обслуживания инкассаторских операций; помещение охраны; офис директора; офис зам. директора; юридический отдел; отдел обслуживания крупных юридических лиц; IT отдел; серверная; конференц-зал; экономический и статистический отдел; бухгалтерский отдел; служебное помещение для сотрудников.

Адрес: Ставропольский край, г. Ставрополь, ул. Ленина, 25

План здания представлен на рисунках 1 и 2.

Развитая информационная система с высокой степенью распределённости: множество банкоматов и POS-терминалов; сервер баз данных Oracle; файловый сервер; коммуникационное оборудование Cisco; программные и аппаратные средства аутентификации. Система видеонаблюдения. Система охранной сигнализации.

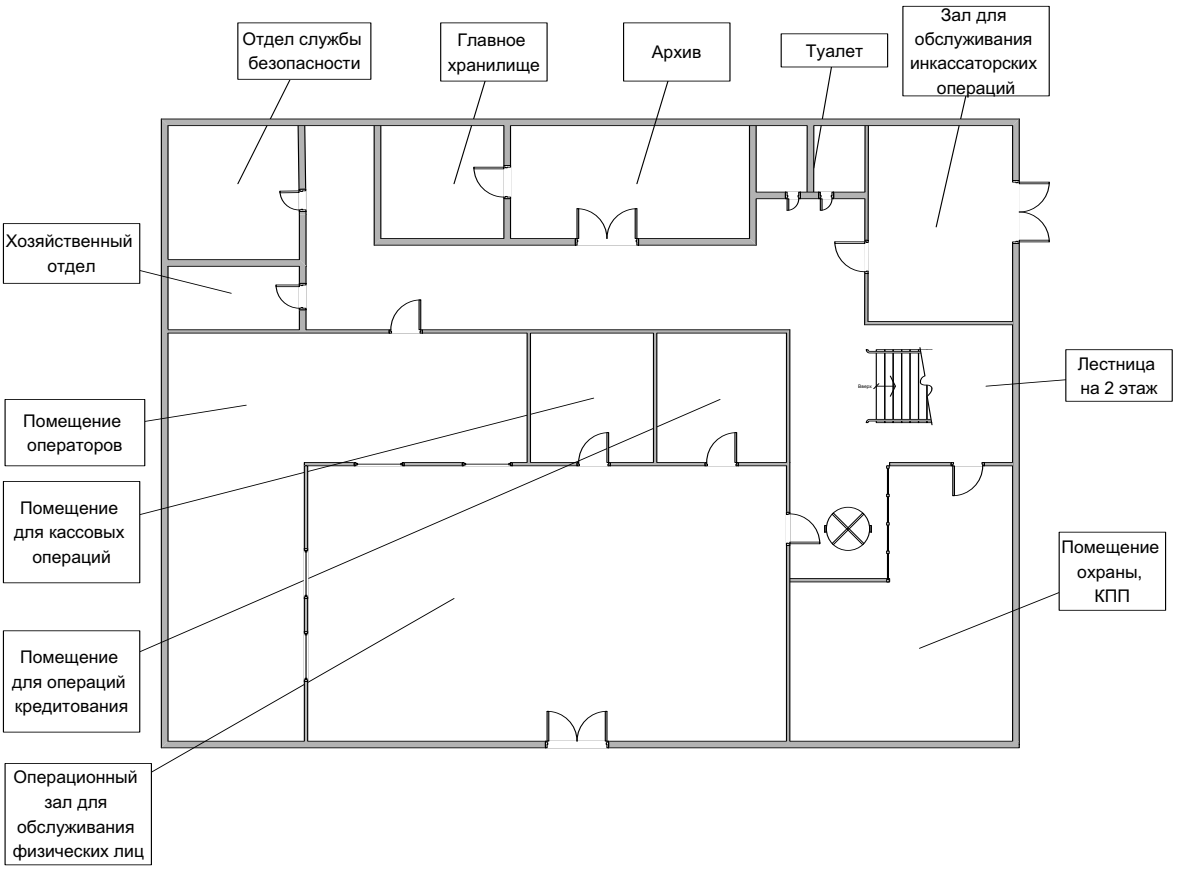

Рисунок 1 – План первого этажа

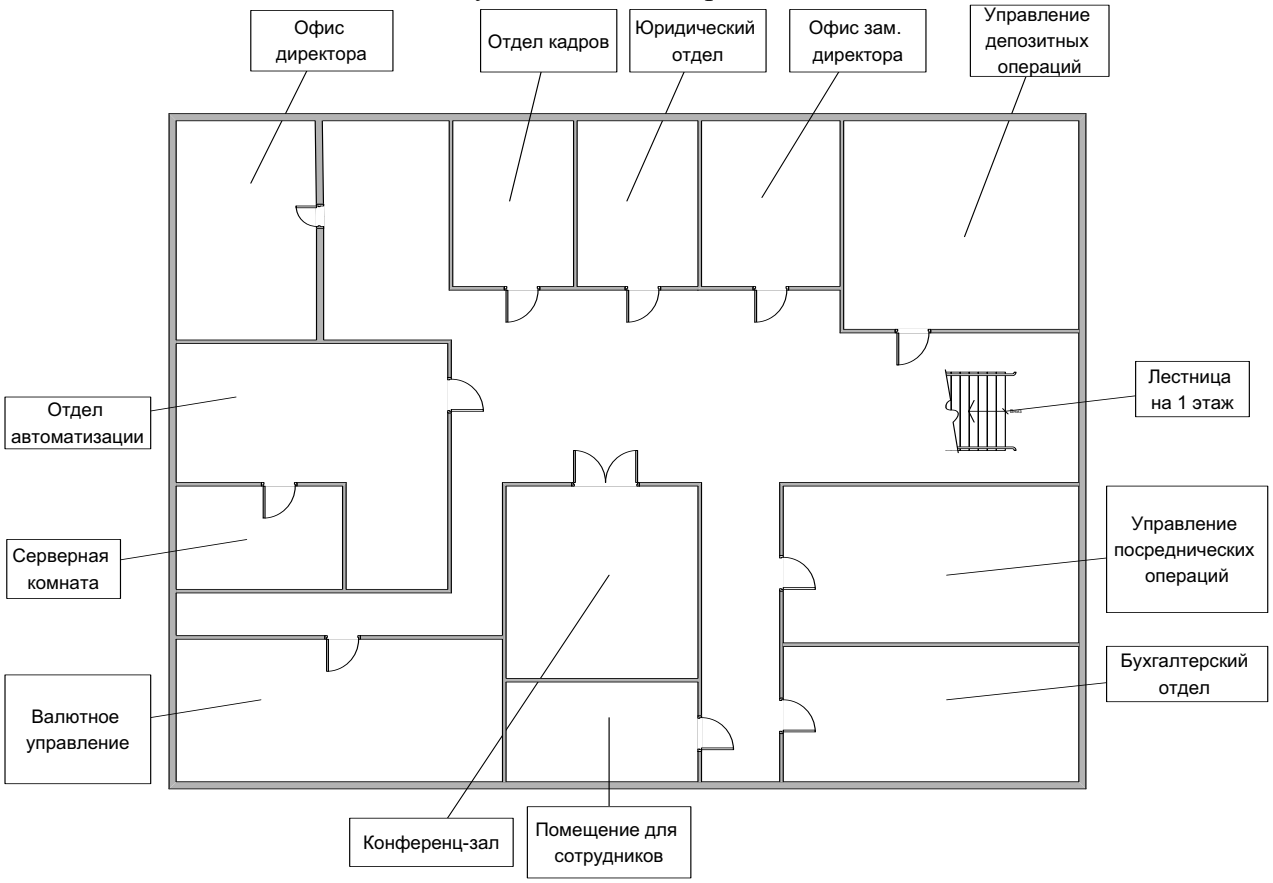

Рисунок 2 – План второго этажа

Рисунок 3 – Организационная структура банка

Список литературы, рекомендуемый к использованию по данной теме.
Основная: 1-3

Тема 2. Электронная коммерция и платежные системы.

Лабораторная работа № 3-4.

Структурное моделирование виртуальной автоматизированной банковской системы

Формируемые компетенции: ПК-1.

Теоретическая часть:

Задание 1. Замыслить и вербально описать автоматизированную банковскую систему виртуального банка.

Зздание 2. Замыслить и разработать структурную схему автоматизированной банковской системы виртуального банка.

Пример оформления отчета по работе

Автоматизированная банковская система (АБС) — комплекс программного и технического обеспечения, направленный на автоматизацию банковской деятельности.

Виртуальная автоматизированная банковская система банка ООО «Пантеон» включает распределенную локальную сеть, состоящую из отдельных компьютеров сотрудников банка, подсоединённых к общей сети банка коммутаторами, которые в свою очередь присоединены к главному серверу обработки банковских операций при помощи маршрутизатора. В данной системесервер обработки банковских операций подсоединён к серверу базы данных, содержащий все данные о сотрудниках, клиентах и документацию организации, и к серверу резервного копирования данных для обеспечения безотказной работы банка. Выход в сеть интернет осуществляется от главного сервера обработки банковских операций защищаемый усиленным брандмауэром.

Отдел службы безопасности имеет свою закрытую локальную сеть без доступа к сети интернет для защиты от хакерских атак, включающую сервер службы безопасности, содержащий разграничительную систему доступа, записи камер наблюдения и журналы учета всех операций с конфиденциальными данными.

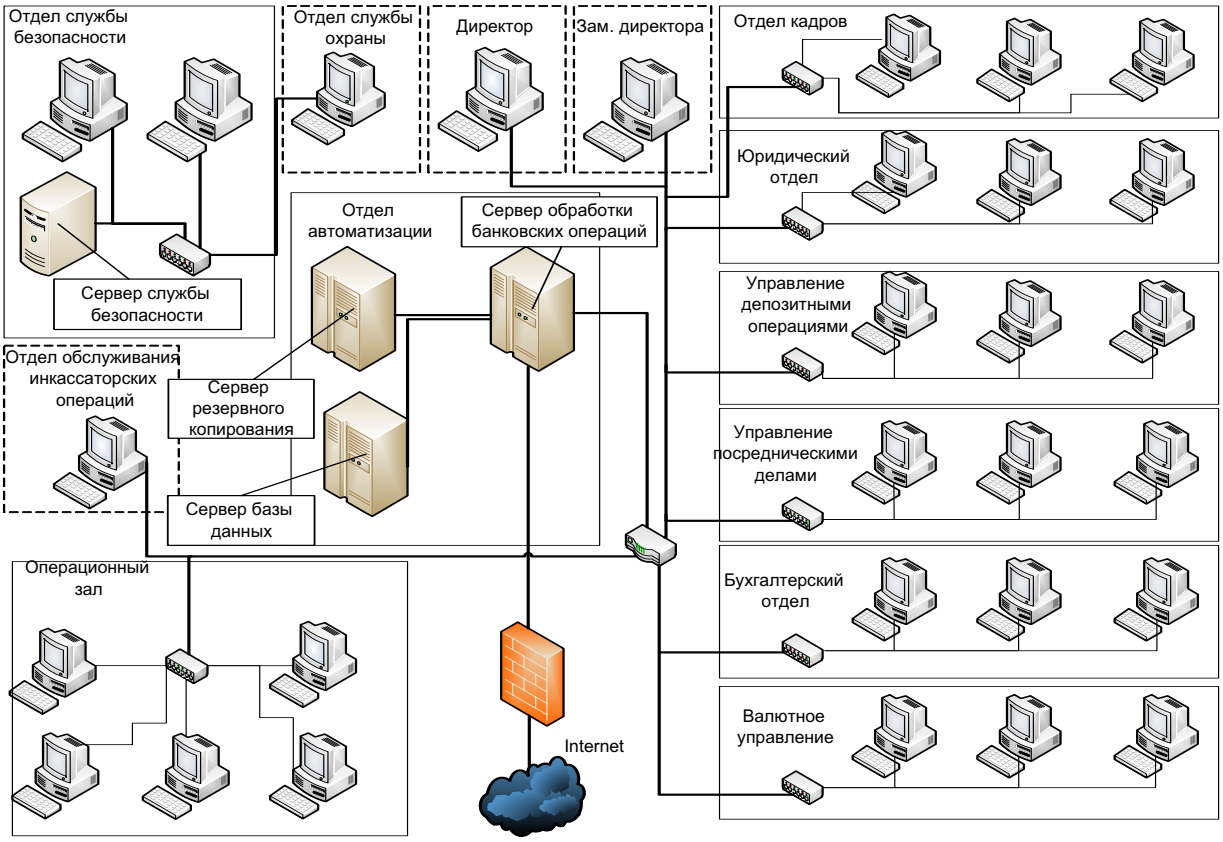

Рисунок 1 – Структурная схема автоматизированной банковской системы

Список литературы, рекомендуемый к использованию по данной теме.
Основная: 1-3

Тема 3. Проблемы безопасности в банковской сфере

Лабораторная работа № 5-6.

Информационное моделирование автоматизированных банковских операций

Формируемые компетенции: ПК-1.

Теоретическая часть:

Задание 1. Вербально описать и составить алгоритм реализации банковской операции – открытие платежной карты.

Задание 2. Вербально описать и составить алгоритм реализации первичной банковской операции – пополнение/удержание.

Задание 3. Вербально описать и составить алгоритм реализации внутренней банковской операции – снятие наличных денег через банкоматы.

Задание 4. Вербально описать и составить алгоритм реализации операции – электронных платежей в торгово-сервисной точке.

Пример оформления отчета по работе

1) ***Открытие платежной карты*** осуществляется в отделениях банка, где происходит прием первичных документов. При этом проверяют исходные данные на правильность и корректность заполнения всех форм, после чего программой «Филиал» формируется первичный номер карточки со статусом «Новая карта». Далее документы (заявление клиента, паспортные данные, анкета) направляются в службу безопасности банка, где происходит проверка на платежеспособность. В конце операционного дня происходит передача пакета данных (файл из программы «Филиал»). По получению данных из службы безопасности банка статус карточки изменяется на «Действующая» и проходит процесс персонализации, после чего карточка передается в отделение банка для передачи клиенту.

Рисунок 1- Открытие платежной карты

2) ***Первичные операции: пополнение/удержание*** совершаются в отделениях банка. Клиент вносит (снимает) денежные средства, на основании данной операции

формируется первичный документ «Приходный ордер» (или расходный ордер при снятии денег, например, при отказе в выдаче карточки), который вводится в банковскую систему (БС) и модуль «Филиал». Далее информация передается из модуля «Филиал» в модуль «Эмитент», с одновременной передачей бумажного носителя «Приходный/Расходный ордер» - происходит контроль информации путем сравнения данных, введенных в БС, сверка контрольных сумм по пакетам и в программе «Филиал» с приходным ордером. В случае правильности введенной информации происходит текущая обработка полученных данных, в течение которой изменяют и корректируют остатки по карточкам держателей, а также происходит архивация проведенных операций и данных.

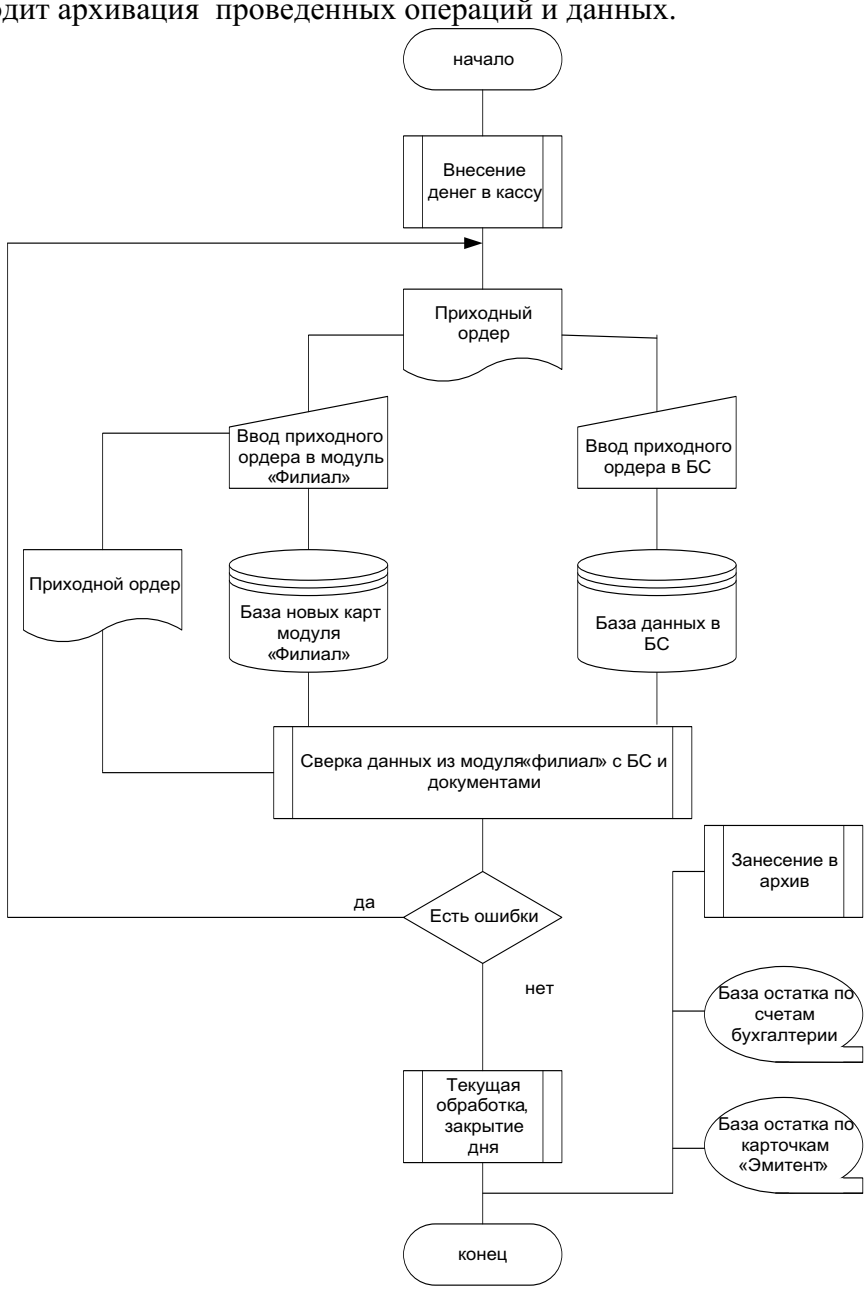

Рисунок 2 - первичные операции: пополнение/удержание

3) ***Операции «снятие наличных денег через банкоматы***, тип «внутренние». Под внутренними подразумеваются операции, совершенные по карточке банка в банкомате или ПОС терминале того же банка. После ввода карточки в банкомат и совершения всех необходимых операций запрос поступает в модуль авторизации, в котором определяется принадлежность карточки: «своя» или «чужая» и принадлежность карточки платежной системе. Если карточка «чужая», происходит перенаправление запроса в сеть платежной системы. Если карточка «своя», т.е.банка, то проверяется остаток, если остаток позволяет, блокируется запрошенная сумма на счете до момента подтверждения снятия денег. В

банкомат отсылается подтверждение о возможности выдачи денег, после этого происходит процесс выдачи денег банкоматом. Если выдача прошла удачно, отправляется подтверждение операции, в этом случае блокированные деньги списываются и операция считается законченной. При этом корректируется база остатков по счетам и карточкам. После закрытия операционного дня в процессинговом центре происходит формирование бухгалтерских проводок по данным операциям, которые экспортируются в общую банковскую систему.

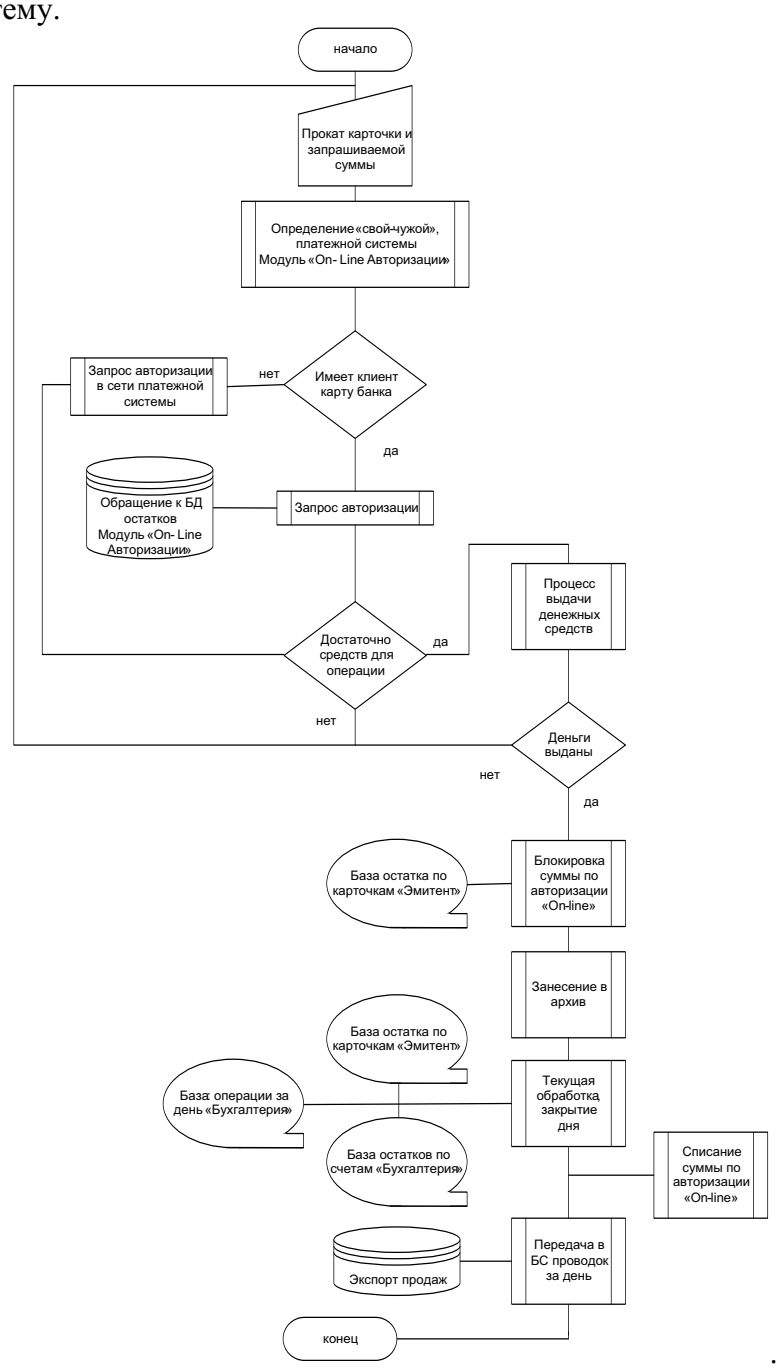

Рисунок 3- операции «снятие наличных денег через банкоматы, тип «внутренние»

4) ***Операции в торгово-сервисной точке***, тип «у нас» и Операции в торгово-сервисной точке, тип «чужие» выполняются аналогично процессу выдачи наличных средств через банкоматы, за исключением времени прихода подтверждения, которое может составлять несколько дней.

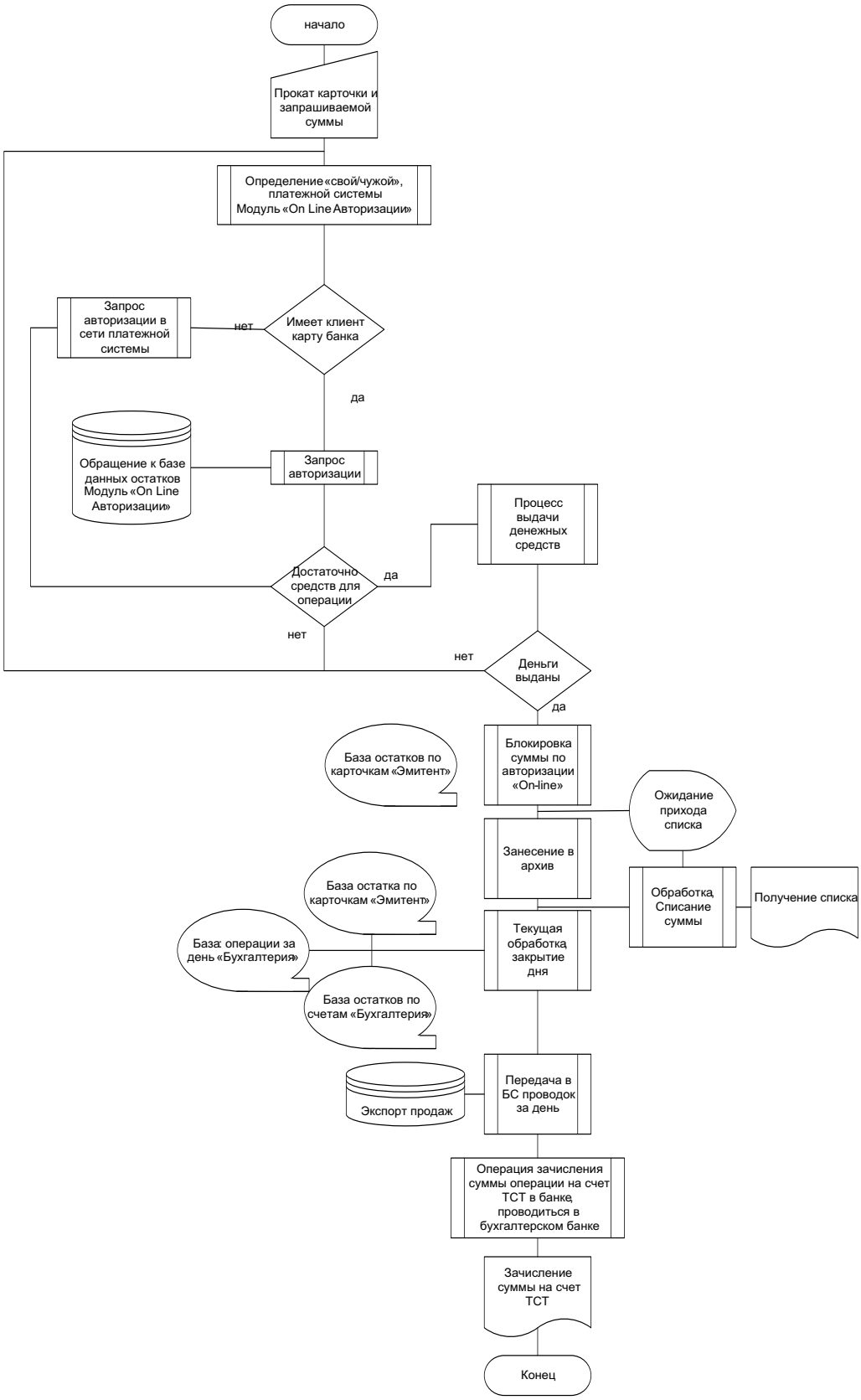

Рисунок 4 - операции в торгово-сервисной точке, тип «у нас»

Список литературы, рекомендуемый к использованию по данной теме.

Основная: 1-3

Тема 4. Анализ рисков в банковской сфере

Лабораторная работа № 7-8.

Разработка модели угроз информации в виртуальном банке

Формируемые компетенции: ПК-1.

Теоретическая часть:

Задание 1. Вербально описать общий подход к составлению Отраслевой модели угроз для виртуального банка.

Задание 2. Вербально описать исходные данные для отраслевой модели угроз применительно к своему виртуальному банку.

Задание 3. Формализовано в виде таблицы описать отраслевую модель угроз для виртуального банка.

Задание 4. Разработать графическую модель проникновения злоумышленника в серверную комнату, определить критический путь и рассчитать вероятность проникновения злоумышленника в серверную комнату.

Пример оформления отчета по работе

Общий подход к составлению Отраслевой модели угроз

1. Угрозы безопасности персональных данных (ПДн) при их обработке в информационных системах персональных данных (ИСПДн) организаций БС РФ - это:

- угроза нарушения доступности ПДн;
- угроза нарушения целостности ПДн;
- угроза нарушения конфиденциальности[1] (неправомерное использование) ПДн, в том числе за счет хищения отчуждаемых машинных носителей с несанкционированно копированной информацией.

2. Отраслевая модель угроз содержит систематизированный перечень актуальных угроз безопасности ПДн при их обработке в ИСПДн, источников актуальных угроз безопасности ПДн, уровней реализации угроз безопасности ПДн, типов материальных объектов среды обработки ПДн (далее – актуальные угрозы безопасности ПДн).

Актуальная угроза безопасности ПДн – угроза безопасности ПДн, риск реализации которой не является допустимым для организации БС РФ по результатам проведения оценки рисков нарушения безопасности персональных данных, обрабатываемых в ИСПДн.

3. Отраслевая модель угроз содержит единые исходные данные по актуальным для организации БС РФ угрозам безопасности ПДн, связанным с несанкционированным, в том числе случайным, доступом в ИСПДн с целью ознакомления, изменения, копирования, неправомерного распространения ПДн или деструктивных воздействий на элементы ИСПДн и обрабатываемых в них ПДн с целью уничтожения или блокирования ПДн.

В рамках настоящей Отраслевой модели угроз под доступом к ПДн понимается ознакомление с ПДн, их обработка, в частности, копирование, модификация или уничтожение ПДн (в соответствии с Руководящим документом «Защита от несанкционированного доступа к информации. Термины и определения», Гостехкомиссия России.- М.: Воениздат,-1992).

К несанкционированному доступу (НСД) к ПДн при их обработке в ИСПДн, в частности, относится:

доступ к ПДн или действия с ПДн, нарушающие установленные права и (или) правила разграничения доступа с использованием штатных средств, предоставляемых ИСПДн;

несанкционированное воздействие на ресурсы ИСПДн, осуществляемое с использованием вредоносных программ (вредоносного кода).

Исходные данные Отраслевой модели угроз

1. Категории ПДн:

категория 1 – персональные данные, отнесенные в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее – Федеральный закон «О персональных данных») к специальным категориям персональных данных;

категория 2 – персональные данные, отнесенные в соответствии с Федеральным законом «О персональных данных» к биометрическим персональным данным;

категория 3 – персональные данные, которые не могут быть отнесены к категории 1, категории 2 или категории 4;

категория 4 - персональные данные, отнесенные в соответствии с Федеральным законом «О персональных данных» к общедоступным или обезличенным персональным данным.

2. Перечень основных источников угроз безопасности ПДн:

– неблагоприятные события природного и техногенного характера;

– террористы, криминальные элементы;

– компьютерные злоумышленники, осуществляющие целенаправленные деструктивные воздействия, в том числе использование компьютерных вирусов и других типов вредоносных кодов и атак;

– поставщики программно-технических средств, расходных материалов, услуг и т.п.;

– подрядчики, осуществляющие монтаж, пуско-наладочные работы оборудования и его ремонт;

– сотрудники организации БС РФ, являющиеся легальными участниками процессов в ИСПДн и действующие вне рамок предоставленных полномочий;

– сотрудники организации БС РФ, являющиеся легальными участниками процессов в ИСПДн и действующие в рамках предоставленных полномочий.

3. Уровни информационной инфраструктуры, на которых возможна реализация угроз безопасности ПДн:

- физический уровень;
- сетевой уровень;
- уровень сетевых приложений и сервисов;
- уровень операционных систем;
- уровень систем управления базами данных;
- уровень банковских технологических процессов и приложений.

Отраслевая модель угроз

Отраслевая модель угроз безопасности ПДн (Таблица) содержит обобщенное описание угроз безопасности ПДн для каждой категории ПДн, включающее:

– источник угрозы безопасности ПДн;

– угроза безопасности ПДн;

– уровень реализации угрозы безопасности ПДн;

– типы материальных объектов среды обработки ПДн (далее – типы объектов среды).

Таблица 1. Отраслевая модель угроз безопасности ПДн

№ п/п	Источник угрозы безопасности ПДн	Уровень реализации угрозы безопасности ПДн	Типы объектов среды	Угроза безопасности ПД
1	2	3	4	5
	ПДн категории 1, ПДн категории 2			
1	**Компьютерные злоумышленники, осуществляющие целенаправленное деструктивное воздействие**	**Сетевой уровень**	**Маршрутизаторы, коммутаторы, концентраторы**	**Нарушение целостности**
2				**Нарушение доступности**
3		**Уровень сетевых приложений и сервисов**	**Программные компоненты передачи данных по компьютерным сетям (сетевые сервисы)**	**Нарушение целостности**
4				**Нарушение доступности**
5		**Уровень операционных систем**	**Файлы данных с ПДн**	**Нарушение конфиденциальности**
6				**Нарушение целостности**
7				**Нарушение доступности**
8		**Уровень систем управления базами данных**	**Базы данных с ПДн**	**Нарушение конфиденциальности**
9				**Нарушение целостности**
10				**Нарушение доступности**
11		**Уровень банковских технологических приложений и сервисов**	**Прикладные программы доступа и обработки ПДн, автоматизированные рабочие места ИСПДн**	**Нарушение конфиденциальности**
12				**Нарушение целостности**
13	**Поставщики программно-технических средств, расходных материалов, услуг и т.п. и подрядчики, осуществляющие монтаж, пуско-наладочные работы оборудования и его ремонт**	**Уровень операционных систем**	**Файлы данных с ПДн**	**Нарушение конфиденциальности**
14				**Нарушение целостности**
15		**Уровень систем управления базами данных**	**Базы данных с ПДн**	**Нарушение конфиденциальности**
16				**Нарушение целостности**
17		**Уровень банковских технологических приложений и сервисов**	**Прикладные программы доступа и обработки ПДн, автоматизированные рабочие места ИСПДн**	**Нарушение конфиденциальности**
18				**Нарушение целостности**
19		**Физический уровень**		**Нарушение конфиденциальности**

№ п/п	Источник угрозы безопасности ПДн	Уровень реализации угрозы безопасности ПДн	Типы объектов среды	Угроза безопасности ПД
1	2	3	4	5
20	**Сотрудники, действующие в рамках предоставленных полномочий**		**Линии связи, аппаратные и технические средства, сервера, физические носители информации**	**Нарушение целостности**
21		**Сетевой уровень**	**Маршрутизаторы, коммутаторы, концентраторы**	**Нарушение конфиденциальности**
22				**Нарушение целостности**
23				**Нарушение доступности**
24		**Уровень сетевых приложений и сервисов**	**Программные компоненты передачи данных по компьютерным сетям (сетевые сервисы)**	**Нарушение конфиденциальности**
25				**Нарушение целостности**
26				**Нарушение доступности**
27		**Уровень операционных систем**	**Файлы данных с ПДн**	**Нарушение конфиденциальности**
28				**Нарушение целостности**
29				**Нарушение доступности**
30		**Уровень систем управления базами данных**	**Базы данных с ПДн**	**Нарушение конфиденциальности**
31				**Нарушение целостности**
32				**Нарушение доступности**
33		**Уровень банковских технологических приложений и сервисов**	**Прикладные программы доступа и обработки ПДн, автоматизированные рабочие места ИСПДн**	**Нарушение конфиденциальности**
34				**Нарушение целостности**
35				**Нарушение доступности**
36	**Сотрудники, действующие вне рамок предоставленных полномочий**	**Уровень операционных систем**	**Файлы данных с ПДн**	**Нарушение конфиденциальности**
37				**Нарушение целостности**
38		**Уровень систем управления базами данных**	**Базы данных с ПДн**	**Нарушение конфиденциальности**
39				**Нарушение целостности**
40		**Уровень банковских технологических приложений и сервисов**	**Прикладные программы доступа и обработки ПДн,**	**Нарушение конфиденциальности**
41				**Нарушение целостности**

№ п/п	Источник угрозы безопасности ПДн	Уровень реализации угрозы безопасности ПДн	Типы объектов среды	Угроза безопасности ПД
1	2	3	4	5
			автоматизированные рабочие места ИСПДн	
	ПДн категории 3			
42	**Компьютерные злоумышленники, осуществляющие целенаправленное деструктивное воздействие**	**Сетевой уровень**	**Маршрутизаторы, коммутаторы, концентраторы**	**Нарушение целостности**
43				**Нарушение доступности**
44		**Уровень сетевых приложений и сервисов**	**Программные компоненты передачи данных по компьютерным сетям (сетевые сервисы)**	**Нарушение целостности**
45				**Нарушение доступности**
46		**Уровень операционных систем**	**Файлы данных с ПДн**	**Нарушение конфиденциальности**
47				**Нарушение целостности**
48				**Нарушение доступности**
49		**Уровень систем управления базами данных**	**Базы данных с ПДн**	**Нарушение конфиденциальности**
50				**Нарушение целостности**
51				**Нарушение доступности**
52	**Сотрудники, действующие в рамках предоставленных полномочий**	**Физический уровень**	**Линии связи, аппаратные и технические средства, сервера, физические носители информации**	**Нарушение конфиденциальности**
53				**Нарушение целостности**
54		**Сетевой уровень**	**Маршрутизаторы, коммутаторы, концентраторы**	**Нарушение конфиденциальности**
55				**Нарушение целостности**
56				**Нарушение доступности**
57		**Уровень сетевых приложений и сервисов**	**Программные компоненты передачи данных по компьютерным сетям (сетевые сервисы)**	**Нарушение конфиденциальности**
58				**Нарушение целостности**
59				**Нарушение доступности**
60		**Уровень операционных систем**	**Файлы данных с ПДн**	**Нарушение конфиденциальности**
61				**Нарушение целостности**
62				**Нарушение доступности**

№ п/п	Источник угрозы безопасности ПДн	Уровень реализации угрозы безопасности ПДн	Типы объектов среды	Угроза безопасности ПД
1	2	3	4	5
63		**Уровень систем управления базами данных**	**Базы данных с ПДн**	**Нарушение конфиденциальности**
64				**Нарушение целостности**
65				**Нарушение доступности**
66		**Уровень банковских технологических приложений и сервисов**		**Нарушение конфиденциальности**
67				**Нарушение целостности**
68				**Нарушение доступности**
69	**Сотрудники, действующие вне рамок предоставленных полномочий**	**Уровень операционных систем**	**Файлы данных с ПДн**	**Нарушение конфиденциальности**
70				**Нарушение целостности**
71				**Нарушение доступности**
72		**Уровень систем управления базами данных**	**Базы данных с ПДн**	**Нарушение конфиденциальности**
73				**Нарушение целостности**
74		**Уровень банковских технологических приложений и сервисов**	**Прикладные программы доступа и обработки ПДн, автоматизированные рабочие места ИСПДн**	**Нарушение конфиденциальности**
75				**Нарушение целостности**
	ПДн категории 4			
76	**Компьютерные злоумышленники, осуществляющие целенаправленное деструктивное воздействие**	**Уровень операционных систем**	**Файлы данных с ПДн**	**Нарушение целостности**
77				**Нарушение доступности**
78		**Уровень систем управления базами данных**	**Базы данных с ПДн**	**Нарушение целостности**
79				**Нарушение доступности**
80	**Сотрудники, действующие в рамках предоставленных полномочий**	**Уровень операционных систем**	**Файлы данных с ПДн**	**Нарушение целостности**
81				**Нарушение доступности**
82			**Базы данных с ПДн**	**Нарушение целостности**

№ п/п	Источник угрозы безопасности ПДн	Уровень реализации угрозы безопасности ПДн	Типы объектов среды	Угроза безопасности ПД
1	2	3	4	5
83		**Уровень систем управления базами данных**		**Нарушение доступности**
84		**Уровень банковских технологических приложений и сервисов**	**Прикладные программы доступа и обработки ПДн, автоматизированные рабочие места ИСПДн**	**Нарушение целостности**
85				**Нарушение доступности**
86	**Сотрудники, действующие вне рамок предоставленных полномочий**	**Уровень операционных систем**	**Файлы данных с ПДн**	**Нарушение целостности**
87		**Уровень систем управления базами данных**	**Базы данных с ПДн**	**Нарушение целостности**
88		**Уровень банковских технологических приложений и сервисов**	**Прикладные программы доступа и обработки ПДн, автоматизированные рабочие места ИСПДн**	**Нарушение целостности**

Проведя анализ модели угроз информационной безопасности банка, мы пришли к выводу, что наиболее опасной угрозой нарушения конфиденциальности информации является доступ злоумышленника к серверу базы данных конфиденциальной информации, а именно к серверной комнате.

Модель проникновения злоумышленника в серверную комнату изображена на рисунке 1.

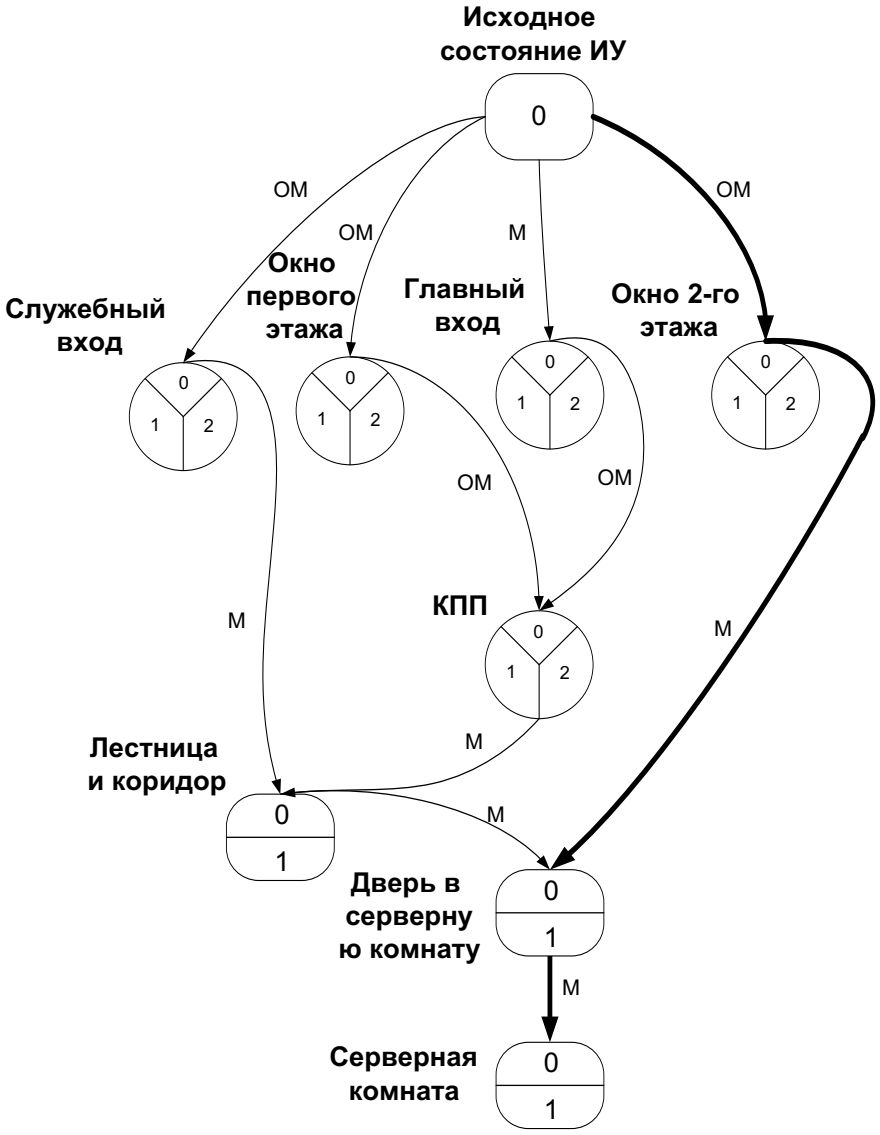

Рисунок 1 – Модель проникновения злоумышленника в серверную комнату

При условии, что значения вероятностей: очень малая (ОМ) равна 0,05, малая (М) равна 0,01 , средняя равна 0,1, то критический путь вероятности проникновения злоумышленника в серверную комнату равен

$P_{пр} = 0,05*0,01*0,01=0,000005$.

Список литературы, рекомендуемый к использованию по данной теме.

Основная: 1-3

Тема 5. Политика безопасности в банковской сфере

Лабораторная работа № 9-10.

Разработка системы физической защиты для объекта информатизации виртуального банка

Формируемые компетенции: ПК-1.

Теоретическая часть:

Задание 1. Графически на планах этажей здания виртуального банка разместить точки доступа и технические средства системы контроля и управления доступа. Вербально обосновать размещение технических средств системы контроля и управления доступа.

Задание 2. Графически на планах этажей здания виртуального банка разместить технические средства системы охранно-пожарной сигнализации. Вербально обосновать выбор и размещение технических средств системы охранно-пожарной сигнализации.

Задание 3. Графически на планах этажей здания виртуального банка разместить видеокамеры системы охранного телевидения. Вербально обосновать выбор типа и размещение видеокамер системы охранного телевидения.

Пример оформления отчета по работе

Система физической защиты виртуального банка включает в себя подсистемы разграничения доступа, пожарной сигнализации и видеонаблюдения. На плане этажей представлено размещение камер видеонаблюдения для мониторинга действий посетителей и сотрудников банка, датчики движения, магнитный замок с возможностью удаленной активации, устройства считывателя персональных карт сотрудников и устройства считывателя персональных карт с вводом пароля.

Помимо представленных на плане устройств обязательными являются датчики пожарной безопасности для каждой комнаты, детекторы разбитого стекла и решетки для каждого окна в здании. Все данные с датчиков выводятся на экран в помещении охраны и записываются на сервер в отделе службы безопасности.

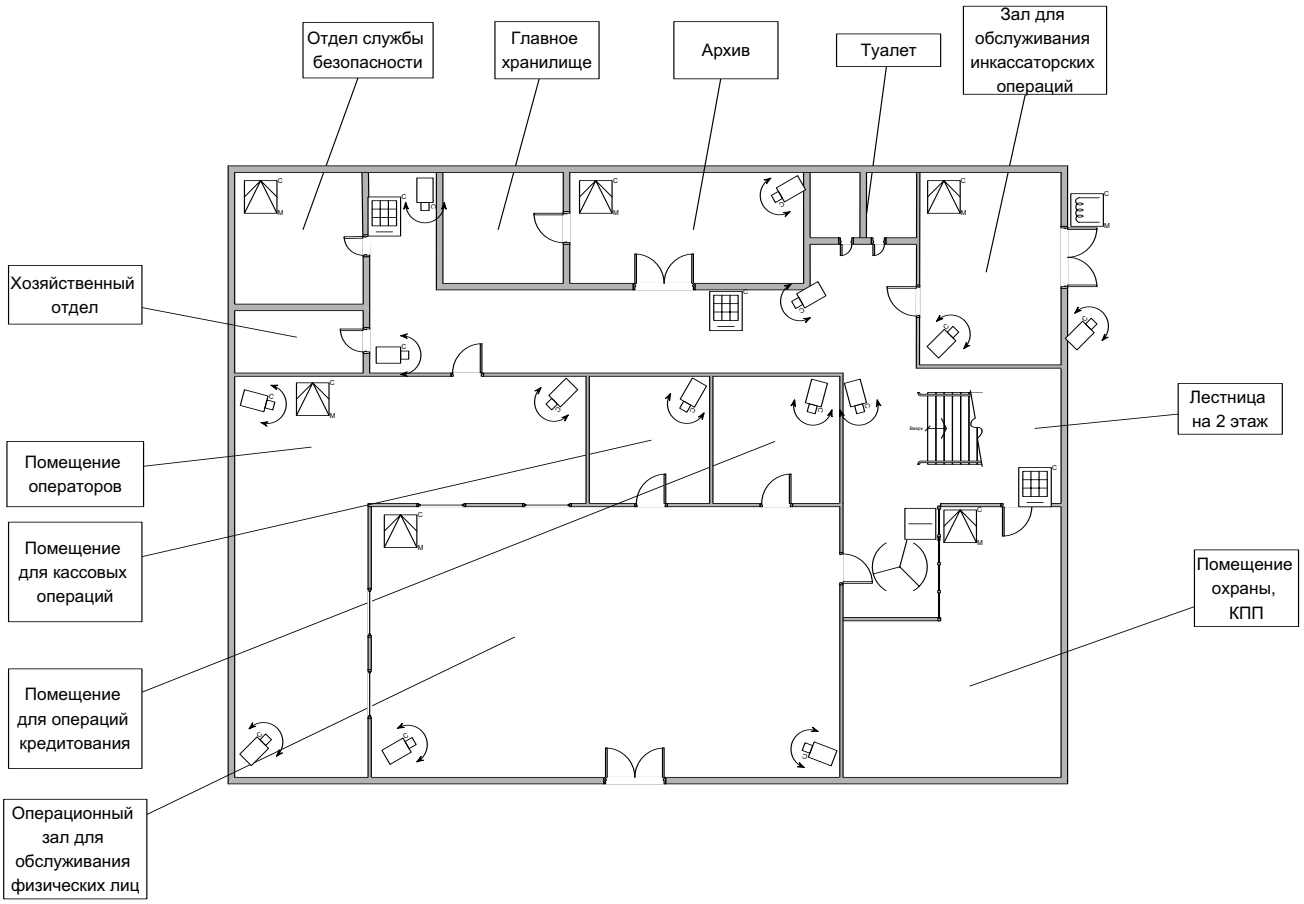

Рисунок 1 – План 1 этажа

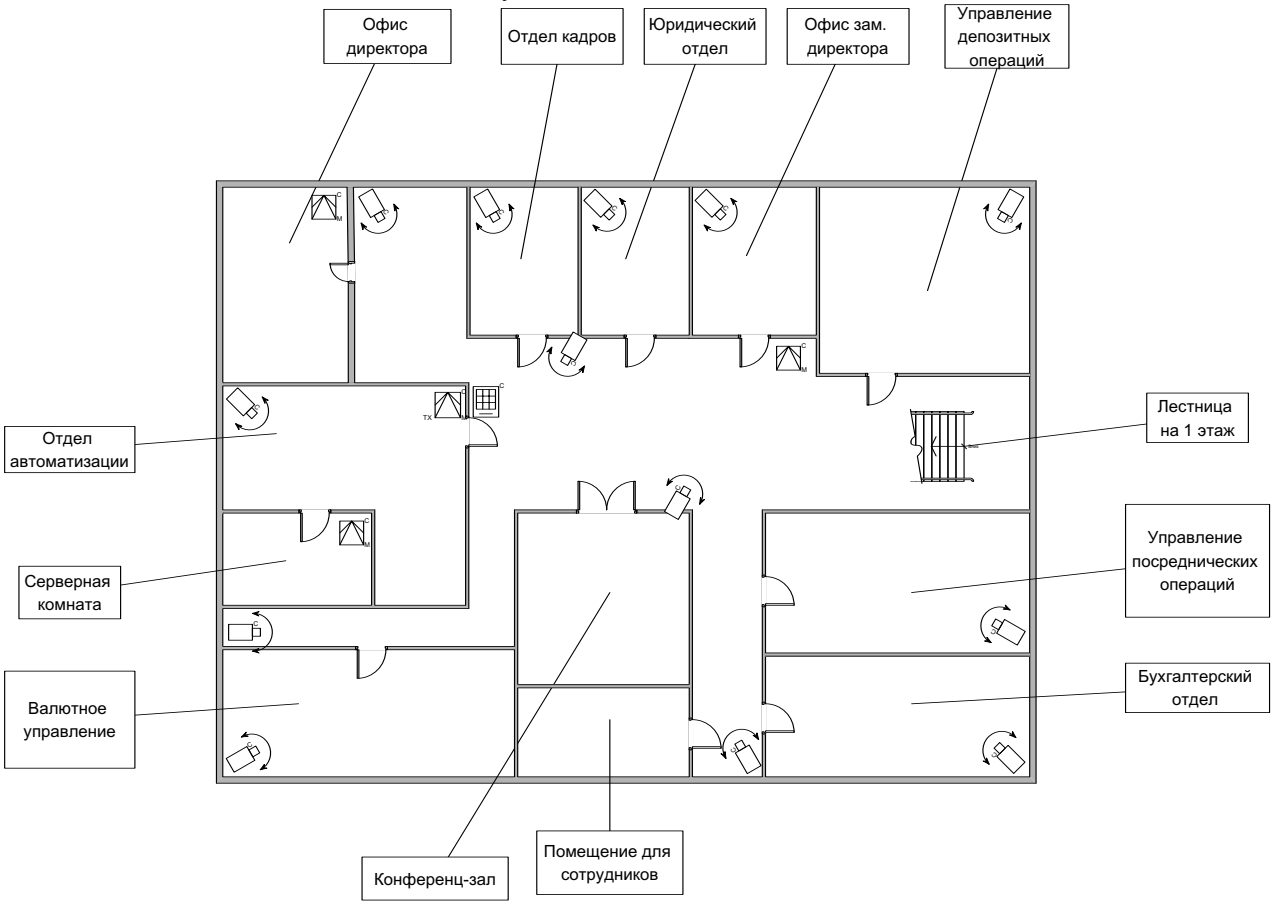

Рисунок 2 – План 2 этажа

Рисунок 3 – Условные обозначения

Список литературы, рекомендуемый к использованию по данной теме.

Основная: 1-3

Тема 6. Управление защитой банковских операций и автоматизированной банковской сети

Лабораторная работа № 11-12.

Разработка политики безопасности виртуального банка

Формируемые компетенции: ПК-1.

Теоретическая часть:

Учебные вопросы:

1. Разработка замысла политики безопасности виртуального банка.
2. Документальное оформление политики безопасности виртуального банка.

СОДЕРЖАНИЕ ЗАНЯТИЯ

Задание 1. Замыслить и вербально описать политику безопасности своего виртуального банка, при этом отразить следующее:

1) Общие положения.

2) Необходимые термины и определения.

3) Приведенные обозначения и сокращения.

4) Цели и задачи обеспечения информационной безопасности.

5) Существующие модели угроз и нарушителей информационной безопасности банка.

6) Систему информационной безопасности:

– общие принципы обеспечения информационной безопасности;

– требования к системе информационной безопасности;

– порядок защиты программно-технических комплексов автоматизированной системы банка;

– принципы обеспечения безопасности баз данных;

– особенности обеспечения безопасности на рабочих станциях пользователей.

7) Систему безопасного функционирования технических средств и информационных ресурсов банка.

8) Порядок категорирования защищаемых ресурсов:

– общие положения;

– категории защищаемых ресурсов;

– разработка перечней защищаемых ресурсов.

9) Управление доступом к информационным ресурсам автоматизированных систем:

– управление доступом пользователей, в том числе: регистрацию пользователей; идентификацию и аутентификацию пользователей; управление привилегиями;

– аудит и протоколирование в автоматизированной системе банка;

– обязанности пользователей, в том числе по использованию паролей; по обеспечению антивирусной защиты.

10) Администрирование автоматизированной системы банка:

– разделение обязанностей;

– защита баз данных;

– резервное копирование и архивирование данных;

– формирование, хранение и распределение ключевой информации;

– организация учета и хранения защищаемых носителей информации;

11) Планирование бесперебойной работы автоматизированной системы:

– доступность системы;

– порядок тестирования и эксплуатации элементов автоматизированной системы.

12) Этапы создания системы защиты информации автоматизированной системы банка.

13) Ответственность за нарушение политики информационной безопасности.

Задание 2. Документально оформить разработанную политику безопасности виртуального банка.

Пример оформления отчета по работе

1. Общие положения

1.1. Настоящий документ определяет основные направления политики информационной безопасности, цели и задачи, принципы ее организации, функционирования и правовые основы. Описывает виды угроз банковским активам и ресурсы, подлежащие защите, а также комплекс организационно-технических мер по защите автоматизированной системы Банка от несанкционированного доступа к циркулирующей в ней информации и незаконного вмешательства в процесс ее функционирования.

1.2. Требования настоящего документа распространяются на все структурные подразделения и пользователей Автоматизированной системы ООО КБ «ПАНТЕОН».

1.3. Перечень мер по реализации Политики информационной безопасности, а также структура управления системой защиты информации и ответственность должностных лиц могут варьироваться в соответствии с особенностями построения и организацией Автоматизированной системы Банка, с целью достижения разумного компромисса между защищенностью, удобством работы и стоимостью системы защиты информации.

%1.%2. Положения данной Политики разработаны согласно рекомендациям Стандарта Банка России СТО БР ИББС-1.0-2008.

2. термины и определения

Автоматизированная система Банка **–** система, реализующая банковские платежные технологические процессы, банковские информационные технологические процессы, процессы жизненного цикла автоматизированных банковских систем в целом

Автоматизированная банковская система **–** автоматизированная система, реализующая банковский технологический процесс или его часть

Банковский технологический процесс **–** технологический процесс, содержащий операции по изменению и (или) определению состояния банковской информации, используемой при функционировании или необходимой для реализации банковских услуг

%1. Обозначения и сокращения

АС	автоматизированная система
АБС	автоматизированная банковская система
АРМ	автоматизированное рабочее место
БС	банковская система
ИБ	информационная безопасность
ИР	информационные ресурсы
ЛВС	локальная вычислительная сеть-
МЭ	межсетевой экран
НСД	несанкционированный доступ
НРД	нерегламентированные действия в рамках предоставленных полномочий
ОС	операционная система
ПЭМИН	побочные электромагнитные излучения и наводки
РС	рабочая станция
СЗИ	система защиты информации
СЗИ НСД	средства защиты информации от

	несанкционированного доступа
СКЗИ	средство криптографической защиты информации
СМИБ	система менеджмента информационной безопасности
СПД	система передачи данных
СУБД	система управления базами данных
ТС	телекоммуникационные системы
ЭЦП	электронная цифровая подпись
ЭВМ	электронно-вычислительная машина

4. ЦЕЛИ И ЗАДАЧИ ОБЕСПЕЧЕНИЯ ИБ

4.1. Целью обеспечения информационной безопасности Банка является сохранение конфиденциальности, целостности и доступности информации.

Конфиденциальность информации обеспечивается в случае предоставления доступа к данным только авторизованным лицам,

целостность – в случае внесения в данные исключительно авторизованных изменений,

доступность – при обеспечении возможности получения доступа к данным авторизованным лицам в нужное для них время.

4.2. Основными задачами обеспечения ИБ являются:

- защита от угроз утечки, утраты и несанкционированной модификации;
- нейтрализация последствий от реализованных угроз;
- обеспечение соответствия законодательству и стандартам.

5. Модели угроз и нарушителей информационной безопасности БАНКА

5.1. Угроза информационной безопасности АС Банка – совокупность условий и факторов, создающих опасность несанкционированного доступа к информации, циркулирующей в автоматизированной системе, а также возможные последствия воздействий нарушителя на АС Банка, непредотвращение, необнаружение и неликвидация которого может привести к ухудшению заданных качественных характеристик функционирования АС Банка или нарушению ее работоспособности, а также искажению и утечке информации.

5.2. В соответствии со Стандартом Банка России СТО БР ИББС-1.0-2008 п.6.2. информационная инфраструктура АС Банка, обеспечивающая реализацию банковских технологий, может быть представлена в виде иерархии следующих основных уровней:

- физического (линии связи, аппаратные средства и пр.);
- сетевого (сетевые аппаратные средства: маршрутизаторы, коммутаторы, концентраторы и пр.);
- сетевых приложений и сервисов;
- операционных систем;
- систем управления базами данных;
- банковских технологических процессов и приложений;
- бизнес-процессов организации.

Главной целью злоумышленника является получение контроля над активами на уровне бизнес-процессов. Прямое нападение на уровне бизнес-процессов более эффективно для злоумышленника и опаснее для Банка, чем нападение, осуществляемое через нижние уровни, требующее специфических опыта, знаний и ресурсов (в т.ч. временных) и поэтому менее эффективное по соотношению "затраты/получаемый результат". Определение конкретных объектов защиты осуществляется на каждом из уровней информационной инфраструктуры.

%1.%2. Основными угрозами информационной безопасности автоматизированной системы, принятыми в Банка на основании п. 6.6. Стандарта БР СТО БР ИББС-1.0-2008 являются:

– неблагоприятные события природного, техногенного и социального характера;

– террористы и криминальные элементы;

– зависимость от поставщиков / провайдеров / партнеров / клиентов;

– сбои, отказы, разрушения / повреждения программных и технических средств;

– работники Банка, реализующие угрозы ИБ с использованием легально предоставленных им прав и полномочий (внутренние нарушители ИБ);

– работники Банка, реализующие угрозы ИБ вне легально предоставленных им прав и полномочий, а также субъекты, не являющиеся работниками Банка, но осуществляющие попытки НСД и НРД (внешние нарушители ИБ);

– несоответствие требованиям надзорных и регулирующих органов, действующему законодательству.

5.3.1. Источники угроз на физическом, сетевом уровнях и уровне сетевых приложений:

– внешние источники угроз: лица, распространяющие вирусы и другие вредоносные программы, хакеры и иные лица, осуществляющие несанкционированный доступ (НСД);

– внутренние источники угроз, реализующие угрозы в рамках своих полномочий и за их пределами (персонал, имеющий права доступа к аппаратному оборудованию, в том числе сетевому, администраторы сетевых приложений и т.п.);

– комбинированные источники угроз: внешние и внутренние, действующие совместно и/или согласованно.

5.3.2. Источники угроз на уровнях операционных систем, систем управления базами данных, банковских технологических процессов:

– внутренние, реализующие угрозы в рамках своих полномочий и за их пределами (администраторы ОС, администраторы СУБД, пользователи банковских приложений и технологий, администраторы ИБ и т.д.);

– комбинированные источники угроз: внешние и внутренние, действующие в сговоре.

5.3.3. Источники угроз на уровне бизнес-процессов:

– внутренние источники, реализующие угрозы в рамках своих полномочий и за их пределами (авторизованные пользователи и операторы АБС, представители менеджмента организации и пр.);

– комбинированные источники угроз: внешние (например, конкуренты) и внутренние, действующие в сговоре.

5.3.4. Угрозы, связанные с природными и техногенными катастрофами и террористической деятельностью.

5.4. В соответствии с требованиями к обеспечению информационной безопасности автоматизированной системы Банка определены следующие модели угроз:

– преднамеренные программно-технические воздействия с целью нарушения целостности (уничтожения, искажения) информации в процессе ее обработки, передачи и хранения в АС Банка;

– нарушения санкционированной доступности информации в АС Банка, за счет нарушения работоспособности программного обеспечения, коммуникационного оборудования и маршрутизаторов АС Банка или их перепрограммирования (дефекты, сбои, аварии и отказы аппаратно-программных комплексов);

– утечка и искажение конфиденциальной информации за счет несанкционированного доступа к ней через технические средства АС Банка, утечка конфиденциальной информации по техническим каналам;

– разглашение конфиденциальной информации и неправомерные действия со стороны лиц, имеющих право доступа к конфиденциальной информации и реализующих угрозы в рамках своих полномочий и за их пределами.

5.5. Основными критическими элементами средств автоматизации АС Банка (в порядке убывания их важности) являются:

– сервера баз данных и приложений;

– коммуникационное оборудование (компоненты) системы передачи данных (маршрутизаторы, концентраторы, модемы);

– специализированные АРМ с установленными СКЗИ;

– рабочие станции пользователей Банка.

5.6. Объектами защиты средств автоматизации являются:

– программно-технический комплекс АС Банка в целом как автоматизированная система, обрабатывающая конфиденциальную информацию;

– сервера баз данных и приложений;

– специализированных АРМ с установленными СКЗИ;

– рабочие станции конечных пользователей АС Банка;

– каналы связи, посредством которых осуществляется информационный обмен в АС Банка;

– помещения, в которых располагается серверная часть программно-технических комплексов и рабочие станции конечных пользователей (в зависимости от обрабатываемой информации).

5.7. Система информационной безопасности АС Банка строится в соответствии с определенным характером угроз и основных элементов системы, на которые эти угрозы распространяются, а также с учетом требований Стандарта БР СТО БР ИББС-1.0-2008 по обеспечению информационной безопасности организаций банковской системы Российской Федерации.

6. Система информационной безопасности БАНКА

6.1. Общие принципы обеспечения информационной безопасности

6.1.1. Своевременность обнаружения проблем, потенциально способных повлиять на бизнес - цели Банка.

6.1.2. Прогнозируемость развития проблем, что подразумевает выявление причинно-следственных связей возможных проблем и построение на этой основе точного прогноза их развития.

6.1.3. Адекватная оценка степени влияния выявленных проблем на бизнес - цели Банка.

6.1.4. Адекватность защитных мер, т.е. выбирать защитные меры, адекватные моделям угроз и нарушителей, с учетом затрат на реализацию таких мер и объема возможных потерь от выполнения угроз.

6.1.5. Эффективность защитных мер, т.е. эффективно реализовывать принятые защитные меры.

6.1.6. Использование опыта при принятии и реализации решений, т.е. накапливать, обобщать и использовать как свой опыт, так и опыт других банков на уровнях принятия решений и их исполнения.

6.1.7. Непрерывность принципов безопасного функционирования, т.е. обеспечение непрерывности реализации принципов безопасного функционирования.

%1.%2.%3. Контролируемость защитных мер, т.е. применение только тех защитных мер, правильность работы которых может быть проверена, при этом регулярно

оценивается адекватность защитных мер и эффективность их реализации с учетом влияния защитных мер на бизнес — цели.

6.2. Требования к системе информационной безопасности

Требования к СИБ формируются для следующих областей:

– назначение и распределение ролей, обеспечение доверия к персоналу;
– обеспечение ИБ на стадиях жизненного цикла АБС;
– защиты от НСД и НРД, управления доступом и регистрацией всех действий в АБС, в телекоммуникационном оборудовании, автоматических телефонных станциях и т.д.;
– антивирусной защиты;
– использования ресурсов сети Интернет;
– использования СКЗИ;
– защиты банковских платежных и информационных технологических процессов.

6.2.1. Назначение и распределение ролей, обеспечение доверия к персоналу.

6.2.1.1. Знание своих клиентов и служащих. Необходимо обладать информацией о своих клиентах, тщательно подбирать персонал, вырабатывать и поддерживать корпоративную этику, что создает благоприятную доверительную среду для деятельности Банка по управлению активами.

6.2.1.2. Формирование ролей осуществляется на основании существующих бизнес-процессов Банка и проводиться с целью исключения концентрации полномочий и снижения риска инцидентов ИБ, связанных с потерей информационными активами свойств доступности, целостности или конфиденциальности.

6.2.1.3. Фактически сложившиеся права и полномочия персонала Банка не являются основанием при формировании ролей.

6.2.1.4. Должны быть определены роли, связанные с деятельностью по обеспечению ИБ. Руководство Банка осуществляет координацию своевременности и качества выполнения ролей, связанных с обеспечением ИБ.

6.2.1.5. Все работники Банка должны давать письменное обязательство о соблюдении конфиденциальности, приверженности правилам корпоративной этики, включая требования по недопущению конфликта интересов. При взаимодействии с внешними организациями и клиентами требования по обеспечению ИБ должны регламентироваться положениями, включаемыми в договоры (соглашения) с ними.

6.2.2.Обеспечение ИБ на стадиях жизненного цикла АБС.

ИБ АБС должна обеспечиваться на всех стадиях жизненного цикла АБС, автоматизирующих банковские технологические процессы, с учетом интересов всех сторон, вовлеченных в процессы жизненного цикла (разработчиков, заказчиков, поставщиков продуктов и услуг, эксплуатирующих и надзорных подразделений Банка). Ввиду отсутствия в Банке подразделения по разработке собственного ПО, рассматриваются следующие стадии жизненного цикла:

– приемка и ввод в действие;
– эксплуатация;
– сопровождение и модернизация;
– снятие с эксплуатации.

6.2.2.1. Ввод в действие, эксплуатация и сопровождение (модернизация), снятие с эксплуатации АБС осуществляются под контролем службы информационной безопасности.

6.2.2.2.На стадии сопровождения (модернизации) при любом внесении изменения в АБС должны проводиться процедуры проверки функциональности, результаты которой должны документально фиксироваться.

6.2.2.3. На стадии снятия с эксплуатации должны быть документально определены и выполняться процедуры, обеспечивающие удаление информации,

несанкционированное использование которой может нанести ущерб бизнес-деятельности организации, и информации, используемой средствами обеспечения ИБ.

6.2.3. Антивирусная защита.

6.2.3.1.На всех рабочих станциях пользователей и серверах АС Банка устанавливаются лицензионные средства антивирусной защиты.

6.2.3.2. Производится постоянный антивирусный контроль программ и файлов данных на рабочих станциях и серверах АС Банка.

6.2.3.3.Обновления антивирусных баз производится ежедневно, в автоматическом режиме.

6.2.3.4.Сотрудники службы информационной безопасности регулярно проводят аудит сообщений антивирусных средств.

6.2.4.Защита от НСД и НРД, управление доступом.

6.2.4.1. В Банке должны быть документально определены и утверждены руководством, выполняться и контролироваться процедуры идентификации, аутентификации, авторизации, управления доступом, контроля целостности, регистрации событий и действий. Процедуры управления доступом должны исключать возможность «самосанкционирования». Результаты контроля процедур должны документироваться.

6.2.4.2. Должен быть документально определен перечень информационных активов (их типов). Права доступа работников и клиентов организации Банка к данным активам должны быть документально зафиксированы.

6.2.4.3. В составе АБС должны применяться встроенные защитные меры.

6.2.4.4. Порядок доступа работников Банка в помещения, в которых размещаются объекты среды информационных активов, должен быть регламентирован во внутренних документах, а его выполнение должно контролироваться.

6.2.4.5. Работа всех пользователей АБС осуществляется под уникальными учетными записями.

6.2.5. Использование сети Интернет.

Сеть Интернет используется Банком для:

- ведения дистанционного банковского обслуживания;
- информационно-аналитической работы в интересах Банка;
- обмена электронными сообщениями, например, почтовыми.

Использование сети Интернет в неустановленных целях запрещено.

6.2.6. Использование СКЗИ.

6.2.6.1. СКЗИ должны быть сертифицированы уполномоченным государственным органом, либо реализованы на основе рекомендованных уполномоченным государственным органом алгоритмов, либо алгоритмов, определенных условиями договора с контрагентом (клиентом) Банка.

6.2.6.2. СКЗИ используются АС банка для:

- обмена информацией с региональным управлением Банка России;
- обмена информацией с управлением РосФинМониторинга;
- обмена информацией с клиентами по системе удаленного банковского обслуживания;
- обмена информацией с прочими организациями, в случаях, когда использование СКЗИ установлено законодательством РФ.

6.2.6.3. ИБ процессов изготовления и хранения ключевых документов СКЗИ обеспечивается комплексом технологических, организационных, технических и программных мер и средств защиты.

6.2.7. Защита банковских платежных и информационных технологических процессов.

6.2.7.1. Комплекс мер по обеспечению ИБ банковского платежного и информационного технологического процесса должен предусматривать:

– защиту платежной информации от искажения, фальсификации, переадресации, несанкционированного уничтожения, ложной авторизации электронных платежных сообщений;

– доступ работника Банка только к тем ресурсам банковского платежного технологического процесса, которые необходимы ему для исполнения должностных обязанностей или реализации прав, предусмотренных технологией обработки платежной информации;

– контроль (мониторинг) исполнения установленной технологии подготовки, обработки, передачи и хранения платежной информации;

– аутентификацию входящих электронных платежных сообщений;

– двустороннюю аутентификацию автоматизированных рабочих мест (рабочих станций и серверов), участников обмена электронными платежными сообщениями;

– возможность ввода платежной информации в АБС только для авторизованных пользователей;

– контроль, направленный на исключение возможности совершения злоумышленных действий (двойной ввод, сверка, установление ограничений в зависимости от суммы совершаемых операций и т.д.);

– восстановление платежной информации в случае ее умышленного (случайного) разрушения (искажения) или выхода из строя средств вычислительной техники;

– сверку выходных электронных платежных сообщений с соответствующими входными и обработанными электронными платежными сообщениями при осуществлении межбанковских расчетов;

– доставку электронных платежных сообщений участникам обмена.

6.2.7.2.Должна осуществляться и быть регламентирована процедура восстановления всех реализованных программно-техническими средствами функций по обеспечению ИБ платежной информации. Регламентирующие документы должны быть согласованы со службой либо лицом, отвечающим в Банке за обеспечение ИБ.

6.3. Защита программно-технических комплексов АС БАНКА

6.3.1. Предотвращение или существенное затруднение реализации потенциальных угроз безопасности АС Банка обеспечивается реализацией следующих функций безопасности:

– резервирование и восстановление ресурсов независимо на всех уровнях АС Банка – для компенсации угроз, связанных с выходом из строя технических средств Банка, защиты от уничтожения, изменения информации, а также обеспечения устойчивости к критическим ситуациям, связанным с уничтожением информации;

– обеспечение защиты конфиденциальной информации при помощи алгоритмов специального преобразования данных – для предотвращения перехвата потенциальным злоумышленником защищаемой информации при передаче ее по внешним каналам передачи данных;

– система идентификации и аутентификации – для предотвращения несанкционированного доступа к информационным ресурсам АС Банка потенциального злоумышленника;

– ведение аудита на различных уровнях АС Банка для реализации системы ответственности за нарушения политики безопасности;

– применение специальных программно-технических средств – для разграничения АС Банка, сетей общего пользования и глобальных сетей, а также логического разделения серверного сегмента АС Банка и остальной корпоративной сети Банка.

6.4. Обеспечение безопасности баз данных

6.4.1. Функции безопасности системы защиты информации Банка в части обеспечения безопасности баз данных АС Банка направлены на:

– защиту баз данных АС Банка от несанкционированных внешних запросов (атак);

– защиту доступности и целостности информации, хранящейся в базах данных АС Банка.

6.4.2 Защита баз данных АС Банка достигается путем:

– распределенного резервирования, что решается в АС Банка с помощью дисковых массивов и оборудования архивного хранения данных;

– установления регламента подключения пользователей к АС Банка для получения информации из баз данных;

– ведения аудита на уровне доступа к базе данных – позволяет установить систему ответственности за нарушения политики безопасности.

6.5. Особенности обеспечения безопасности на рс пользователей

6.5.1. Вся информация в АС Банка хранится централизованно в базах данных и обрабатывается на серверах АС Банка. Поэтому, основной упор при реализации системы защиты информации Банка в части защиты рабочих станций делается на защищенное взаимодействие клиентских мест АС Банка с серверами.

6.5.2. Необходимыми функциями защиты при взаимодействии РС пользователей с серверами являются:

– идентификация и аутентификация пользователей при доступе к базам данных АС Банка;

– ограничение доступа рабочих станций пользователей к информационным ресурсам АС Банка;

6.5.3. Кроме того, необходимыми функциями защиты рабочих станций пользователей Банка являются:

– защита от несанкционированного доступа к информации на РС Банка;

– защита от преднамеренных программных воздействий, в том числе вирусов.

7. система безопасного функционирования технических средств и информационных ресурсов Банка

7.1. Основой для реализации системы защиты информации Банка является построение на базе защищенной операционной системы, реализующей механизмы разграничения прав доступа, аутентификации и аудита, и другого программного обеспечения, единой структуры управления СЗИ, которая, осуществляет поддержку Политики информационной безопасности АС Банка и контроль за ее выполнением.

7.2. Управление информационной безопасностью реализуется техническими мерами на базе функций защиты информации, предоставляемых штатными средствами операционных систем, средств системы управления базами данных и дополнительных сертифицированных программно-аппаратных средств и организационными мерами, направленными на предотвращение разглашения, несанкционированного уничтожения и модификации конфиденциальной информации.

7.3. Корпоративная сеть может включать имеющиеся у Банка локальные сети, доступные ресурсы глобальных (включая Интернет) и ведомственных телекоммуникационных сетей, телефонные и выделенные каналы связи, средства стационарной, спутниковой и мобильной радиосвязи и др. При этом в полной мере может использоваться уже имеющееся оборудование (компьютеры, сервера, маршрутизаторы, коммутаторы, межсетевые экраны и т.д.).

7.4. Безопасность коммуникаций и технических средств, безопасность и достоверность информационных ресурсов в корпоративной сети, взаимодействующей с внешними техническими средствами и информационными ресурсами, достигается путем создания в телекоммуникационной инфраструктуре корпоративной сети интегрированной защищенной среды, включающей:

– Систему комплексной сетевой защиты, основанную на применении сертифицированных программных межсетевых экранов, что позволяет добиться наиболее оптимальной и эффективной степени защиты ресурсов и информации в корпоративной сети

от посягательств, исходя из важности информационного объекта и требуемой надежности защиты.

– Распределенную систему регистрации о наличии санкционированных объектов в корпоративной сети, об их IP-адресах и местоположении, обеспечивающую в любой момент времени полную информированность любого объекта корпоративной сети всей необходимой информацией для возможности автоматического установления соединений с другими объектами.

– Систему электронной цифровой подписи и шифрования информации на прикладном уровне, обеспечивающую достоверность и юридическую значимость документов и совершаемых действий, а также систему управления ключами, включающую подсистему распределения симметричных ключей и подсистему асимметричного распределения ключей.

– Безопасную для локальной сети систему организации каналов доступа отдельных компьютеров локальной сети к открытым ресурсам внешних сетей (включая Интернет) и отдельных компьютеров внешних сетей к открытым ресурсам локальной сети.

– Систему контроля и управления связями, правами и полномочиями объектов АС Банка, обеспечивающую автоматизированное управление политиками безопасности в корпоративной сети.

– Систему межсетевого взаимодействия, обеспечивающую организацию связи между разными подсетями банка путем взаимного согласования между администрациями сетей допустимых межобъектных связей и политик безопасности.

7.5. Для защиты АС Банка используются функции защиты от несанкционированного доступа, реализованные в ОС серверов и рабочих станций, функции защиты баз данных, реализованные в СУБД, функции защиты, реализованные в прикладном программном обеспечении, а также дополнительные сертифицированные программно-аппаратные средства защиты информации.

7.6. Защита серверов АС Банка обеспечивается выполнением следующих требований:

7.6.1. Серверная часть АС Банка находится в защищаемом помещении для исключения возможности несанкционированного в него проникновения посторонних лиц.

7.6.2. Для защиты серверной части АС Банка все сервера приложений, сервера баз данных, установленные в Банка, находятся в одной защищенной подсети.

7.7.Защита рабочих станций пользователей, составляющих клиентскую часть АС Банка, обеспечивается системой защиты от несанкционированного доступа, базирующейся на штатных средствах операционной системы.

8. Категорирование защищаемых ресурсов

8.1. Общие положения

Категорирование ресурсов АС Банка является необходимым элементом организации работ по обеспечению информационной безопасности АС Банка, целями которого является:

−создание нормативно-методической основы для дифференцированного подхода к защите ресурсов АС Банка, (информации, задач, специализированных АРМ, рабочих станций);

−выработка типовых решений по принимаемым организационным мерам защиты и распределению аппаратно-программных средств защиты для различных категорий рабочих станций АС Банка.

8.2. Категории защищаемых ресурсов

8.2.1. Ресурсы АС Банка делятся на 2 класса:

−информационные ресурсы;

−аппаратные ресурсы.

8.2.2. Исходя из необходимости обеспечить различные уровни защиты разных видов информации (не содержащей сведений, составляющих государственную тайну), хранимой

и обрабатываемой в организации, вводятся следующие категории информационных ресурсов.

8.2.2.1. Категории конфиденциальности:

«Строго конфиденциальная» — информация, являющаяся конфиденциальной в соответствии с требованиями действующего законодательства (банковская тайна, персональные данные), а также информация, ограничения на распространение которой введены решениями руководства организации (коммерческая тайна), разглашение которой может привести к тяжким финансово-экономическим последствиям для организации, вплоть до банкротства (нанесению тяжкого ущерба жизненно важным интересам клиентов, корреспондентов, партнеров или сотрудников).

«Конфиденциальная» — информация, не отнесенная к категории «строго конфиденциальная», ограничения на распространение которой вводятся решением руководства организации в соответствии с предоставленными ему как собственнику (уполномоченному собственником лицу) информации действующим законодательством правами, разглашение которой может привести к убыткам и потере конкурентоспособности организации (нанесению ущерба интересам клиентов, корреспондентов, партнеров или сотрудников).

«Открытая» — информация, обеспечения конфиденциальности (введения ограничений на распространение) которой не требуется.

8.2.2.2. Категории целостности:

«Высокая» — к данной категории относится информация, несанкционированная модификация (искажение, подмена, уничтожение) или фальсификация (подделка) которой может привести к нанесению значительного прямого ущерба организации, целостность и аутентичность (подтверждение подлинности источника) которой должна обеспечиваться гарантированными методами (средствами электронной цифровой подписи), в соответствии с обязательными требованиями действующего законодательства, приказов, директив и других нормативных актов.

«Низкая» — к данной категории относится информация, несанкционированная модификация, подмена или удаление которой может привести к нанесению незначительного косвенного ущерба организации, ее клиентам, партнерам или сотрудникам, целостность которой должна обеспечиваться в соответствии с решением руководства в соответствии с требованиями действующего законодательства, приказов, директив и других нормативных актов.

«Нет требований» — к данной категории относится информация, к обеспечению целостности (и аутентичности) которой требований не предъявляется.

8.2.2.3. Категории доступности:

В зависимости от периодичности решения функциональных задач и максимально допустимой задержки получения результатов вводится четыре требуемых категории доступности информации.

«Беспрепятственная доступность» — доступ к задаче должен обеспечиваться в любое время (задача решается постоянно, задержка получения результата не должна превышать нескольких секунд или минут).

«Высокая доступность» — доступ должен осуществляться без существенных задержек по времени (задача решается ежедневно, задержка получения результата не должна превышать нескольких часов).

«Средняя доступность» — доступ может обеспечиваться с существенными задержками по времени (задача решается раз в несколько дней, задержка получения результата не должна превышать нескольких дней).

«Низкая доступность» — задержки по времени при доступе к задаче практически не лимитированы (задача решается с периодом в несколько недель или месяцев, допустимая задержка получения результата — несколько недель).

8.2.3. Для обеспечения уровнями безопасности различных видов аппаратных ресурсов, используемых в Банке, вводятся следующие категории.

8.2.3.1. Категории отказоустойчивости:

«Высшая» — к данной категории относятся критически важные аппаратные средства, (Сервер СУБД и дисковые массивы, содержащие базу данных АБС, сервер - контроллер домена, файловый сервер, сервера банковских технологических процессов, маршрутизаторы, коммутаторы, межсетевые экраны). К высшей категории отказоустойчивости относятся также компьютеры с установленными средствами криптографической защиты информации.

«Средняя» — к данной категории относятся рабочие станции пользователей. Непрерывность банковских технологических процессов обеспечивается наличием резервных рабочих станций.

«Низшая» — к данной категории относятся концентраторы и офисная техника.

8.2.3.2. Категории доступа:

«Строго ограниченный» — физический доступ к данной категории средств вычислительной техники регламентируется приказами руководства Банка, инструктивными и регламентирующими документами. К данной категории относятся ЭВМ с установленными средствами криптографической защиты информации, сервер СУБД и дисковые массивы, содержащие базу данных АБС, сервер - контроллер домена, файловый сервер, сервера банковских технологических процессов, маршрутизаторы, коммутаторы, межсетевые экраны.

«Ограниченный» — к данной категории относятся рабочие станции пользователей и средств вычислительной техники, доступ к которым регламентируется должностными инструкциями сотрудников Банка и «Положением о предоставлении сотрудникам Банка доступа к информационным ресурсам и регистрации действий пользователей при их работе в АС Банка».

8.2.4. Каналы связи, используемые в технологических банковских процессах, не категорируются. Для обеспечения непрерывности банковских процессов необходимо предусмотреть резервирование каналов связи.

8.3. Разработка Перечней защищаемых ресурсов

8.3.1. В ходе выполнения работ по категорированию защищаемых ресурсов АС Банка составляется «Перечень информационных ресурсов АС Банка, в котором отражаются категории задач, решаемых в рамках банковских процессов автоматизированной системы, и «Перечень средств вычислительной техники АС Банка, устанавливающий категории средств вычислительной техники автоматизированных банковских и информационных систем и определяющий типовые средства защиты.

8.3.2. После проведения работ по категорированию средств вычислительной техники АС Банка в «Паспорта рабочих мест» вносятся записи о категории рабочей станции. ЭВМ должны быть оснащены средствами защиты информации в соответствии с установленной категорией.

8.3.3. В случае изменения требований к категориям информационных ресурсов АС Банка и/или изменения категории РС, (при изменении набора решаемых на РС задач, изменения категорий решаемых на РС задач и изменении состава пользователей РС) производится пересмотр «Перечня информационных ресурсов АС Банка» и «Перечня вычислительной техники АС Банка».

9. Управление доступом к информационным ресурсам автоматизированных систем

9.1. Управление доступом пользователей

9.1.1. Регистрация пользователей

Регистрация и подключение пользователей к АС Банка происходит в соответствии с «Положением о предоставлении сотрудникам Банка доступа к информационным

ресурсам и регистрации действий пользователей при их работе с АБС, ЛВС и сети Интернет».

9.1.2. Идентификация и аутентификация пользователей

Идентификация и аутентификация пользователей АС Банка проводится при включении рабочей станции – штатными средствами защиты ОС, либо использованием функций сертифицированных средств защиты от НСД, установленных на рабочей станции;

9.1.3. Управление привилегиями

Администратором АБС для каждого пользователя определяются и устанавливаются полномочия на вызов транзакций, а также на конкретные действия внутри транзакций, в соответствии с должностными обязанностями. Если пользователь делает попытку вызвать транзакцию или выполнить действие внутри транзакции, на которые у него нет полномочий, он получает соответствующее сообщение от системы.

Каждому пользователю разрешено выполнение только тех функций и работа с теми объектами системы, на которые он имеет полномочия в соответствии со своими должностными обязанностями при работе в АС Банка, зафиксированными в служебных записках на подключение к АС Банка.

9.2. Аудит и протоколирование в АС БАНКА

9.2.1. Аудит и протоколирование в АС Банка необходимы для удовлетворения правовых требований в случае возникновения спорных ситуаций, мониторинга защиты системы и отслеживания событий безопасности.

9.2.2. Аудит и протоколирование могут осуществляться штатными средствами операционных систем, прикладного программного обеспечения или специализированными программами.

9.2.3. При осуществлении данных процедур учитывается категорийность защищаемого ресурса, важность и значимость регистрируемого события, особенности используемого программного обеспечения, требований Стандарта ЦБР СТО БР ИББС-1.0-2006, договорных отношений, регламентирующих и инструктивных документов Банка.

9.2.4. Журналы аудита и протоколирования подлежат периодическому архивированию и хранению в соответствии с требованиями нормативных документов. Доступ к этим журналам определяется системой полномочий.

9.3. Обязанности пользователей

9.3.1. Использование паролей

9.3.1.1. Пароли должны держаться в тайне, то есть запрещается сообщать их другим людям или вставлять в тексты программ.

9.3.1.2. При несоблюдении правил использования паролей, установленных в «Положении о предоставлении сотрудникам Банка доступа к информационным ресурсам и регистрации действий пользователей при их работе с АБС, ЛВС и сети Интернет», пользователи несут ответственность в соответствии с п.15 настоящего документа.

9.3.2. Обеспечение антивирусной защиты

9.3.2.1. На всех рабочих станциях пользователей АС Банка устанавливаются средства антивирусной защиты.

9.3.2.2. Производится постоянный антивирусный контроль программ и файлов данных на рабочих станциях АС Банка.

9.3.2.3. Обновления антивирусных баз производится ежедневно, в автоматическом режиме.

9.3.2.4. Сотрудники должны немедленно информировать службу информационной безопасности Банка об обнаруженных вирусах, изменениях в конфигурации или сбоях при работе компьютера или приложений.

9.3.2.5. Лица, ответственные за обеспечение защиты информации и пользователи должны соблюдать требования «Инструкции по организации антивирусной защиты автоматизированной системы Банка.

10. Администрирование АС Банка

10.1. Разделение обязанностей

10.1.1. Администрирование АС Банка (регистрация пользователей, назначение прав доступа и проч.) осуществляют сотрудники отдела информационных технологий Банка, наделенные функциональными правами администраторов соответствующих подсистем.

10.1.2. Контрольные функции и аудит возлагаются на службу информационной безопасности.

10.1.3. Администраторы АС Банка имеют полномочия только на выполнение администраторских задач в системе.

10.2. Защита баз данных

10.2.1. За защиту данных на уровне базы данных отвечает специалист отдела информационных технологий, ответственный за администрирование СУБД.

10.2.2. Для доступа к базе данных используются только встроенные средства системы АС Банка.

10.2.3. Для доступа к базе данных запрещено пользоваться стандартной учетной записью пользователя АС Банка. Для прямого доступа к базе данных необходимо создать специальных пользователей с соответствующими правами доступа.

10.2.4. Сервера приложений в тестовой системе не имеют прямого доступа к продуктивным данным.

10.3. Резервное копирование и архивирование данных

10.3.1. Для бесперебойной работы АС Банка и возможности восстановления ее функционирования после аварийных ситуаций, обеспечивается сохранность архивов базы данных и системных журналов.

10.3.2. Комплекс программно-аппаратных средств системы АС Банка поддерживает функции ежедневного резервного копирования данных и хранения недельного объема накопленных изменений данных. Максимально допустимый объем потери данных при авариях и сбоях не должен превышать дневного объема изменений данных на каждом рабочем месте системы.

10.3.3. Электронные носители информации с архивами баз данных хранятся в соответствии с требованиями п.10.5.3. Хранение архивов баз данных осуществляется в защищаемых помещениях, удаленных от мест расположения серверов АС Банка.

10.4. Формирование, хранение и распределение ключевой информации

10.4.1. Система формирования, хранения и распределения ключевой информации решает задачи надежной аутентификации данных и пользователей, закрытие данных, гарантирование их целостности при транспортировке по сети передачи данных.

10.4.2. Формирование, хранение и распределение ключевой информации осуществляется в соответствии с «Положением по работе со средствами криптографической защиты информации, использующимися в системах электронного документооборота».

10.5. Организация учета и хранения защищаемых носителей информации

10.5.1. При организации учета и хранения защищаемых носителей информации, в том числе, электронных носителей информации с архивами баз данных, должен проводиться учет всех защищаемых носителей информации с помощью их маркировки.

10.5.2. Учет защищаемых носителей информации должен проводиться в журнале с регистрацией их выдачи/приема.

10.5.3. Электронные носители информации с архивами баз данных хранятся в защищаемых помещениях для исключения возможности бесконтрольного или несанкционированного проникновения посторонних лиц.

11. планирование бесперебойной работы

11.1. Доступность системы

11.1.1. После введения АС Банка в эксплуатацию, все компоненты системы должны быть доступны в соответствии с регламентом работы Банка.

11.1.2. Резервное копирование систем осуществляется ежедневно.

11.1.3. Время восстановления после сбоя в системе 4 часа.

11.1.4. Максимальное время недоступности базы данных в штатном режиме функционирования не должно превышать 20 минут.

11.1.5. Для обеспечения бесперебойного функционирования АС Банка предусмотрено резервирование систем обработки и хранения данных, а также возможность сбора данных аудита о трафике в сети и его анализа.

11.1.6. Резервное оборудование и процедуры перехода на аварийный режим работы необходимо тестировать ежегодно.

11.1.7. Обеспечение бесперебойного функционирования АС Банка производиться в соответствии с Планом действий, направленным на обеспечение непрерывности деятельности и (или) восстановление деятельности в случае возникновения непредвиденных обстоятельств ООО КБ «ПАНТЕОН».

11.2. Порядок тестирования и эксплуатации элементов Ас

11.2.1. Соблюдение полного технологического цикла функционирования АС Банка обеспечивается наличием двух программных сред: тестовой и продуктивной. Для обеспечения доступности, бесперебойной работы и снижения загрузки серверов обеспечивается разделение серверных частей тестовой и продуктивной систем. Сервера в тестовой системе не должны иметь доступа к продуктивным данным.

11.2.2. Все изменения в продуктивную систему должны вноситься после того, как администратор системы проверит правильность запроса на перенос настроек.

11.2.3. При тестировании системы не должны использоваться продуктивные данные.

11.2.4. В продуктивной системе не должно быть пользователей с правами разработки, изменения и отладки программ.

11.2.5. Для организации процесса обучения должна существовать отдельная система, не использующая продуктивные данные АС Банка.

12. Этапы создания системы защиты информации АС Банка

12.1. Реализация системы защиты информации АС Банка строится на использовании организационно-распорядительных и программно-технических мер. К организационно-распорядительным мерам можно отнести:

−построение схемы взаимодействия подразделений банка по вопросам информационной безопасности АС;

−разработку и/или совершенствование нормативно-методических и организационно-распорядительных документов по вопросам защиты информации АС;

−назначение лиц, ответственных за информационную безопасность;

−категорирование защищаемых ресурсов АС;

−разработку эксплуатационной документации на объект информатизации и средства защиты информации;

−подготовку и обучение персонала правилам работы с СЗИ АС Банка;

−аттестацию объекта информатизации на соответствие требованиям безопасности информации.

12.2. Техническая реализация системы защиты АС Банка состоит из следующих основных этапов:

−Построение защищенной сети серверного сегмента АС Банка и настройки штатных средств защиты операционных систем серверов и СУБД на предмет сетевой безопасности.

−Защита рабочих станций пользователей АС Банка с применением программно-аппаратных средств защиты информации от несанкционированного доступа.

13. ответственность за нарушение Политики информационной безопасности

13.1. Действующее законодательство РФ позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией.

13.2. Уголовным Кодексом РФ установлена ответственность за незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или

банковскую тайну (ст.183 УК РФ), за неправомерный доступ к компьютерной информации (ст.272 УК РФ), за создание, использование и распространение вредоносных программ для ЭВМ (ст.273 УК РФ), за нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст.274 УК РФ).

13.3. В соответствии со ст. 139 Гражданского кодекса работники, разгласившие служебную или коммерческую тайну вопреки трудовому договору, обязаны возместить причиненные убытки.

Приложение 1
к Политике информационной безопасности
ООО КБ «ПАНТЕОН»

Перечень документов Банка по информационной безопасности.

1. Положение о предоставлении сотрудникам Банка доступа к информационным ресурсам и регистрации действий пользователей при их работе в АБС, ЛВС и сети Интернет
2. Положение по работе со средствами криптографической защиты информации использующимися в системах электронного документооборота Банка
3. Инструкция по организации антивирусной защиты автоматизированной системы Банка
4. Инструкция по обеспечению информационной безопасности при использовании ресурсов сети Интернет
5. Инструкция по использованию системы дистанционного банковского обслуживания Банка
6. План действий, направленный на обеспечение непрерывности деятельности и (или) восстановление деятельности в случае возникновения непредвиденных обстоятельств
7. Положение о службе информационной безопасности

Список литературы, рекомендуемый к использованию по данной теме.

Основная: 1-3.

Тема 7. Управление защитой банковских операций и автоматизированной банковской сети

Лабораторная работа № 13-14.

Разработка механизмов защиты платежной системы виртуального банка

Формируемые компетенции: ПК-1.

Теоретическая часть:

Задание 1. Разработать и вербально описать систему POS.

Задание 2. Разработать и вербально описать механизмы обеспечения безопасности систем POS.

Задание 3. Разработать и вербально описать механизмы обеспечения безопасности электронных платежей через сеть Internet.

Пример оформления отчета по работе

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ СИСТЕМ POS

Системы POS (Point-Of-Sale), обеспечивающие расчеты продавца и покупателя в точке продажи, получили широкое распространение в развитых странах и, в частности, в США. Системы POS осуществляют проверку и обслуживание дебетовых и кредитных карт покупателя непосредственно в местах продажи товаров и услуг в рамках системы электронных платежей. POS-терминалы, входящие в эти системы, размещаются на различных предприятиях торговли - в супермаркетах, на автозаправочных станциях и т.п.

Обычно POS-терминал бывает также оснащен модемом с возможностью автодозвона. POS-терминал обладает "интеллектуальными" возможностями - его можно программировать. В качестве языков программирования используются язык ассемблера, а также диалекты языков Си и Бейсик. Все это позволяет проводить авторизацию карт с магнитной полосой в режиме реального времени (on-line) и использовать при работе со смарт-картами автономный режим (off-line) с накоплением протоколов транзакций. Эти протоколы транзакций передаются в процессинговый центр во время сеансов связи. Во время этих сеансов POS-терминал может также принимать и запоминать информацию, передаваемую ЭВМ процессингового центра. В основном это бывают стоп-листы.

Схема системы POS приведена на рис.4. Покупатель для оплаты покупки предъявляет свою дебетовую или кредитную карту и вводит значение PIN для подтверждения личности. Продавец, в свою очередь, вводит сумму денег, которую необходимо уплатить за покупку или услуги. Затем в банк-эквайер (банк продавца) направляется запрос на перевод денег. Банк-эквайер переадресует этот запрос в банк-эмитент для проверки подлинности карты, предъявленной покупателем. Если эта карта подлинная и покупатель имеет право применять ее для оплаты продуктов и услуг, банк-эмитент переводит деньги в банк-эквайер на счет продавца. После перевода денег на счет продавца банк-эквайер посылает на POS-терминал извещение, в котором сообщает о завершении транзакции. После этого продавец выдает покупателю товар и извещение.

Следует обратить внимание на тот сложный путь, который должна проделать информация о покупке, прежде чем будет осуществлена транзакция. Во время прохождения этого пути возможны искажения и потеря сообщений.

Для защиты системы POS должны выполняться следующие требования:

Проверка PIN, введенного покупателем, должна производиться системой банка-эмитента. При пересылке по каналам связи значение PIN должно быть зашифровано.

Сообщения, содержащие запрос на перевод денег (или подтверждение о переводе), должны проверяться на подлинность для защиты от замены и внесения изменений при прохождении по линиям связи и обрабатывающим процессорам.

Самым уязвимым местом системы POS являются ее POS-терминалы. В отличие от банкоматов в этом случае изначально предполагается, что POS-терминал не защищен от внешних воздействий. Угрозы для POS-терминала связаны с возможностью раскрытия секретного ключа, который находится в POS-терминале и служит для шифрования информации, передаваемой этим терминалом в банк-эквайер. Угроза раскрытия ключа терминала достаточно реальна, так как эти терминалы устанавливаются в таких неохраняемых местах, как магазины, автозаправочные станции и пр. Потенциальные угрозы из-за раскрытия ключа получили такие названия.

"Обратное трассирование". Сущность этой угрозы состоит в том, что если злоумышленник получит ключ шифрования, то он может пытаться восстановить значения PIN, использованные в предыдущих транзакциях.

"Прямое трассирование". Сущность этой угрозы состоит в том, что если злоумышленник получит ключ шифрования, то он попытается восстановить значения PIN, которые будут использоваться в последующих транзакциях.

Для защиты от угроз обратного и прямого трассирования предложены три метода:

-метод выведенного ключа;

-метод Ключа транзакции;

-метод открытых ключей.

Сущность первых двух методов состоит в том, что они обеспечивают модификацию ключа шифрования передаваемых данных для каждой транзакции. Метод выведенного ключа обеспечивает смену ключа при каждой транзакции независимо от ее содержания. Для генерации ключа шифрования используют однонаправленную функцию от текущего значения ключа и некоторой случайной величины. Процесс получения (вывода) ключа для шифрования очередной транзакции представляет собой известное "блуждание" по дереву. Вершиной дерева рис.5 является некоторое начальное значение ключа I. Чтобы получить ключ с номером S, число S представляют в двоичной форме. Затем при вычислении значения ключа учитывается структура двоичного представления числа S, начиная со старшего разряда. Если L-й двоичный разряд числа S равен 1, то к текущему значению ключа K применяется однонаправленная функция FL (K), где L - номер рассматриваемого двоичного разряда. В противном случае переходят к рассмотрению следующего разряда числа S, не применяя однонаправленной функции. Последняя реализована на основе алгоритма DES. Для получения достаточного быстродействия количество единиц в двоичном представлении числа S обычно ограничивается - их должно быть не более 10. Этот метод обеспечивает защиту только от угрозы "обратного трассирования".

Метод ключа транзакции позволяет шифровать информацию, передаваемую между POS-терминалами и банком-эквайером, на уникальном ключе, который может меняться от транзакции к транзакции. Для генерации нового ключа транзакции используются следующие составляющие:

* однонаправленная функция от значения предыдущего ключа;

* содержание транзакции;

* информация, полученная от карты.

Обеспечение безопасности электронных платежей через сеть Internet

Все большее значение приобретает электронная торговля. Число покупок по банковским картам будет расти по мере создания систем заказов в оперативном режиме Internet. Сегодня Internet может рассматриваться как огромный рынок, способный охватить практически все население планеты Земля.

Под термином "электронная торговля" понимают предоставление товаров и платных услуг через глобальные информационные сети. виды электронной коммерции:

-продажа информации, например подписка на базы данных, функционирующие в режиме on-line.

-электронный магазин, который представляет собой Web-site.

-электронные банки.

Основные методы защиты информации

Традиционный и проверенный способ электронной торговли, который ведет свое начало от обычной торговли по каталогам, представляет собой оплату товаров и услуг кредитной карточкой по телефону. В этом случае покупатель заказывает на Web-сервере список товаров, которые он хотел бы купить, и потом сообщает по телефону номер своей кредитной карточки продавцу коммерческой фирмы. Затем происходит обычная авторизация карты, а списание денег со счета покупателя производится лишь в момент отправки товара по почте или с курьером.

Для того чтобы покупатель - владелец кредитной карточки мог без опасений расплатиться за покупку через сеть, необходимо иметь более надежный, отработанный механизм защиты передачи электронных платежей. Такой принципиально новый подход заключается в немедленной авторизации и шифровании финансовой Информации в сети Internet с использованием схем SSL и SET.

Протокол SSL (Secure Socket Layer) предполагает шифрование информации на канальном уровне.

Протокол "Безопасные электронные транзакции" SET (Secure Electronic Transactions), разработанный компаниями Visa и MasterCard, предполагает шифрование исключительно финансовой информации.

Особенности функционирования протокола SET

Для того чтобы обеспечить полную безопасность и конфиденциальность совершения сделок, протокол SET должен гарантировать непременное соблюдение следующих условий.

1. Абсолютная конфиденциальность информации. Владельцы карточек должны быть уверены в том, что их платежная информация надежно защищена и доступна только указанному адресату. Это является непременным условием развития электронной торговли.

2. Полная сохранность данных. Участники электронной торговли должны быть уверены в том, что при передаче от отправителя к адресату содержание сообщения останется неизменным." Сообщения, отправляемые владельцами карточек коммерсантам, содержат информацию о заказах, персональные данные и платежные инструкции. Если в процессе передачи изменится хотя бы один из компонентов, то данная транзакция не будет обработана надлежащим образом. Поэтому во избежание ошибок протокол SET должен обеспечить средства, гарантирующие сохранность и неизменность отправляемых сообщений. Одним из таких средств является использование цифровых подписей.

3. Аутентификация (установление подлинности) счета владельца карточки. Использование цифровых подписей и сертификатов владельца карточки гарантирует аутентификацию счета владельца карточки и подтверждение того, что владелец карточки является законным пользователем данного номера счета.

4. Владелец карточки должен быть уверен, что коммерсант действительно имеет право проводить финансовые операции с финансовым учреждением. Использование цифровых подписей и сертификатов коммерсанта гарантирует владельцу карточки, что можно безопасно вести электронную торговлю.

Участники системы расчетов и криптографические средства защиты транзакций. Протокол SET изменяет способ взаимодействия участников системы расчетов. В данном случае электронная транзакция начинается с владельца карточки, а не с коммерсанта или эквайера.

Коммерсант предлагает товар для продажи или предоставляет услуги за плату. Протокол SET позволяет коммерсанту предлагать электронные взаимодействия, которые могут безопасно использовать владельцы карточек.

Эквайером (получателем) является финансовое учреждение, которое открывает счет коммерсанту и обрабатывает авторизации и платежи по кредитным карточкам. Эквайера обрабатывает сообщения о платежах, переведенных коммерсанту посредством платежного межсетевого интерфейса. При этом протокол SET гарантирует, что при взаимодействиях,

которые осуществляет владелец карточки с коммерсантом, информация о счете кредитной карточки будет оставаться конфиденциальной.

Правила SET предусматривают первоначальное шифрование сообщения с использованием случайным образом сгенерированного симметричного ключа, который, в свою очередь, шифруется открытым ключом получателя сообщения. В результате образуется так называемый электронный конверт. Получатель сообщения расшифровывает электронный конверт с помощью своего частного (секретного) ключа, чтобы получить симметричный ключ отправителя. Далее симметричный ключ отправителя используется для расшифрования присланного сообщения.

Целостность информации и аутентификации участников транзакции гарантируется использованием электронной цифровой подписи.

Протокол SET вводит новое применение цифровых подписей, а именно использование двойных цифровых подписей. В рамках протокола SET двойные цифровые подписи используются для связи заказа, отправленного коммерсанту, с платежными инструкциями, содержащими информацию о счете и отправленными банку.

Список литературы, рекомендуемый к использованию по данной теме.

Основная: 1-3.

Тема 8. Безопасность платежей в INTERNET

Лабораторная работа № 15-16.

Тема: Разработка алгоритма работы протокола безопасных электронных транзакций
Формируемые компетенции: ПК-1.
Теоретическая часть:

Задание 1. Вербально описать протокол безопасных электронных транзакций SET.

Задание 2. Составить диаграмму реализации протокола безопасных электронных транзакций SET.

Задание 3. Разработать алгоритм протокола безопасных электронных транзакций SET.

Пример оформления отчета по работе

Протокол безопасных электронных транзакций SET

Для операций с кредитными карточками используется протокол SET, разработанный совместно компаниями Visa, MasterCard, Netscape и Microsoft. Полная документация по SET имеет объем около 970 страниц. Данная статья является изложением базовых принципов и понятий. В отличие от SSL протокол SET узкоспециализирован. Целью SET является обеспечение необходимого уровня безопасности для платежного механизма, в котором участвует три или более субъектов. При этом предполагается, что транзакция реализуется через Интернет. В РФ в настоящее время разработано и разрабатывается большое число различных платежных программ, некоторые из них достаточно совершенны. Здесь следует иметь в виду, что если российские торговые компании и банки не хотят оказаться в изоляции, если они не будут учитывать складывающиеся тенденции и стандарты, шансов конкурировать на международном, а вскоре и на отечественном рынке у них не будет. Для этого нужно снять ряд юридических ограничений, действующих в РФ и блокирующих развитие электронной торговли (это касается прежде всего алгоритмов RSA, электронной подписи и т.д.). На базовом уровне SET осуществляет следующие функции:

–аутентификация. Все участники кредитных операций идентифицируются с помощью электронных подписей. Это касается клиента-покупателя, продавца, банкира, выдавшего кредитную карточку, и банкира продавца.

–конфиденциальность. Все операции производятся в зашифрованном виде.

–целостность сообщений. Информация не может быть подвергнута модификации по дороге в противном случае это будет сразу известно.

–подсоединение. SET позволяет подключить к базовому сообщению дополнительный текст и послать его одному из партнеров.

–безопасность. Протокол должен обеспечить максимально возможную безопасность операции, достижимую в имеющихся условиях.

–совместимость. Должна быть предусмотрена совместимость с любыми программными продуктами и с любыми сервис-провайдерами.

–независимость от транспортного протокола. Безопасность операций не должна зависеть от уровня безопасности транспортного протокола. Такие гарантии особенно важны, так как протокол SET ориентирован для работы в Интернет.

На более высоком уровне протокол SET поддерживает все возможности, предоставляемые современными кредитными карточками:

- регистрацию держателя карточки;
- регистрацию продавца;
- запрос покупки;
- авторизацию платежа;

– перевод денег;
– кредитные операции;
– возврат денег;
– отмену кредита;
– дебитные операции.

Окончательная версия протокола SET была выпущена в мае 1997 года. Протокол работает с четырьмя субъектами: владельцем кредитной карточки, банком, эту карточку выпустившим (issuer - эмитент), продавцом (merchant) и банком, где помещен счет продавца (acquirer). Помимо этих функциональных субъектов в процессе обычно (опционно) участвует центры сертификации, в задачу которых входит подтверждение подлинности предъявляемых параметров аутентификации, причем в случае крупных сделок с этими центрами должны взаимодействовать все участники. Основной целью сертификатов является подтверждение того, что присланный общедоступный ключ прибыл от настоящего отправителя, а не от самозванца.

Практика электронной торговли позволяет выделить семь этапов сделки.

Таблица 1 – этапы сделки.

Этап	Действие
1	Владелец карты просматривает позиции каталога продавца: В реальном масштабе времени на WEB-сервере На CD-диске на своей рабочей станции Читая бумажную версию каталога Через поисковую систему посредника
2	Владелец карты выбирает понравившийся товар или услугу.
3	Владельцу карты предоставляется форма заказа, содержащая список позиций, их цены, стоимости доставки, уровни платежей по налогам, возможные скидки и т.д. Такая форма может быть доставлена по сети с сервера продавца или сформирована торговой программой владельца карты. Иногда продавцы предоставляют возможность согласования цены продукта (например, предъявляя карту постоянного покупателя или предоставляя цены конкурентов).
4	Владелец карты выбирает средство платежа. SET предполагает применение различных кредитных и платежных карт.
5	Владелец карты посылает продавцу заполненную форму заказа и платежные инструкции. В данной спецификации предполагается, что заказ и инструкции подписываются владельцем карты электронным образом с привлечением имеющихся в его распоряжении сертификатов.
6	Продавец запрашивает платежную авторизацию от эмитента карты.
7	Продавец посылает подтверждение заказа.
8	Продавец доставляет заказанный товар или услугу
9	Продавец посылает запрос на оплату товара или услуги финансовой организации владельца карты.

Порядок следования этапов при определенных условиях может несколько варьироваться. Спецификация SET определяет функции и технику реализации этапов 5, 6, 7 и 9. Таким образом, работа протокола SET инициализируется владельцем карты. Владельцем карты может быть как частное лицо, так и корпоративный клиент, работающие на своих рабочих станциях.

Многие современные WEB-броузеры поддерживают протокол SET. Что позволяет осуществлять торговлю товарами и услугами с использованием WWW-технологии. Напрашивается вопрос, почему для финансовых операций не использовать протокол SSL, который весьма широко распространен? SSL позволяет безопасно передавать продавцу номер кредитной карточки покупателя, но не способен реализовать многие другие операции, например, проверить этот номер на правильность, проконтролировать, позволено ли данному клиенту пользоваться данной карточкой и т.д.. Конечно, не трудно создать CGI-скрипты, которые решат некоторые из этих проблем, но это не может заменить контроля в реальном масштабе времени, необходимого для некоторых операций. Нельзя утверждать, что в рамках протокола SSL нельзя решить и эти проблемы, но для этого нужно создать достаточно большое число специализированных программ, которые в существующих пакетах пока отсутствуют. Кроме того, нужно думать и о безопасности на стороне сервера. Продавец, получив номер кредитной карточки, может занести его в базу данных. А где гарантия (для покупателя), что эта база данных достаточно хорошо защищена? Таким образом, даже передача номера кредитной карточки посредством SSL не самая лучшая идея. Тем более такая схема позволяет осуществлять подбор номеров кредитных карт. А заботиться об удобствах воров не самое полезное занятие.

Номер кредитной карточки имеет определенную структуру (это не случайное число). Первые четыре цифры - код банка, выпустившего карточку. Последняя цифра представляет собой контрольную сумму номера. Вычисление этой контрольной суммы производится по следующему алгоритму.

Каждая цифра номера умножается на его “вес”. Веса меняются 1,2,1,2. Для карт с четным числом цифр, последовательность весов начинается с 2, в противном случае с 1. Если взвешенное число больше 9, из него вычитается 9. Далее вычисляется сумма по модулю 10. Результат всегда должен получаться равным нулю (с учетом кода контрольной суммы).

Схема взаимодействия субъектов в протоколе SET показана на рис. 1 (взаимодействия с центром сертификации не показаны). Протокол SET помогает реализовать следующие процедуры.

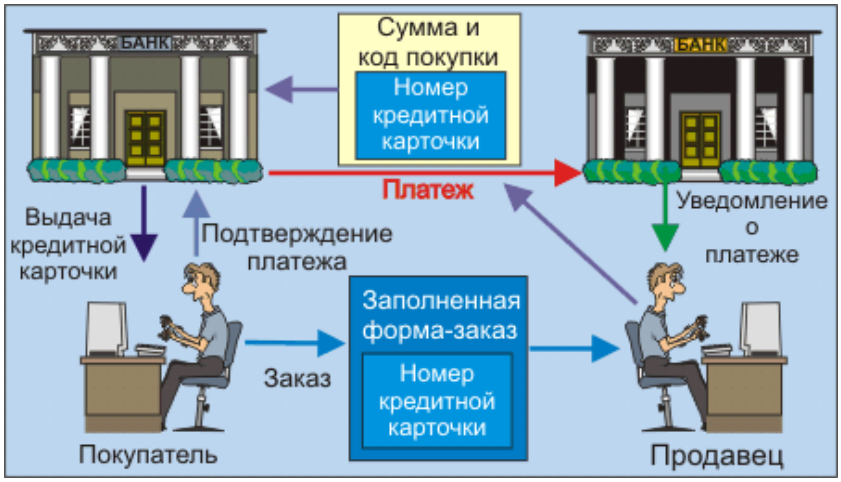

Рисунок 1- Схема взаимодействия субъектов протокола SET

1. Покупатель инициализирует покупку. При этом покупатель выбирает продавца, просматривает его WEB-сайт, принимает решение о покупке, заполняет бланк заказа. Все это делается до вступления в дело протокола SET. Реально взаимодействие участников сделки регламентируется протоколом IOTP. SET начинает свою работу, когда покупатель нажимает

клавишу оплаты. При этом сервер посылает ЭВМ-покупателя сообщение, которое и запускает соответствующую программу. Процедура эта может быть реализована с помощью PHP- или CGI-скрипта, или JAVA-аплета.

2. Программа клиента посылает заказ и информацию об оплате. Для этого формируется два сообщения, одно содержит данные о полной стоимости покупки и номере заказа, второе - номер кредитной карточки покупателя и банковскую информацию. Сообщение о заказе шифруется с использованием симметричного метода (например, DES) и вкладывается в цифровой конверт, где используется общедоступный ключ продавца. Сообщение об оплате шифруется с привлечением общедоступного ключа банка (эмитента кредитной карты). Таким образом продавец не получает доступа к номеру кредитной карточки покупателя. Программа генерирует хэш-дайджест (SHA1) обоих сообщений с использованием секретного ключа покупателя. Это позволяет продавцу и банкиру проконтролировать целостность сообщения, но препятствует прочтению части, ему не предназначенной (например, номера кредитной карты продавцом).

3. Продавец выделяет часть, адресованную банкиру, и направляет ее по месту назначения. Программа SET WEB-сервера продавца генерирует запрос авторизации серверу банка, где находится счет продавца. При формировании запроса авторизации используется электронная подпись продавца, базирующаяся на его секретном ключе, что позволяет однозначно его идентифицировать. Этот запрос шифруется с помощью ключа сессии и вкладывается в цифровой конверт, где используется общедоступный ключ банка.

4. Банк проверяет действительность кредитной карточки, дешифрует запрос авторизации продавца и идентифицирует продавца. После этого осуществляется проверка авторизации покупателя. При этом посылается запрос авторизации, снабженный электронной подписью, банку, выпустившему кредитную карточку.

5. Банк, выпустивший карточку, выполняет авторизацию и подписывает чек, если кредитная карточка покупателя в порядке. Отклик, снабженный соответствующей подписью, посылается банку продавца.

6. Банк продавца авторизует данную операцию, и посылает подтверждение, подписанное электронным образом, WEB-серверу продавца.

7. WEB-сервер продавца завершает операцию, выдавая клиенту подтверждение на экран, и заносит результат операции в соответствующую базу данных.

8. Продавец осуществляет подтверждение выполнения операции своему банку, Деньги покупателя переводятся на счет продавца.

9. Банк, выпустивший карточку, посылает счет покупателю и SET уведомляет покупателя об изменениях на его счету (раз в месяц).

Итак, видно, что каждый шаг реализации протокола SET сопровождается аутентификацией. Это препятствует какому-то внешнему субъекту стать посредником и видоизменять сообщения. Для нормальной работы протокола SET все участники должны зарегистрироваться и снабдить партнеров своим общедоступным ключом.

Протокол SET может использоваться не только в рамках Интернет, но и при заказах по почте или телефону MOTO (Mail Order/Telephone Order).

Рассмотрим диаграмму конечных состояний протокола SET , представленную на рисунке 2.

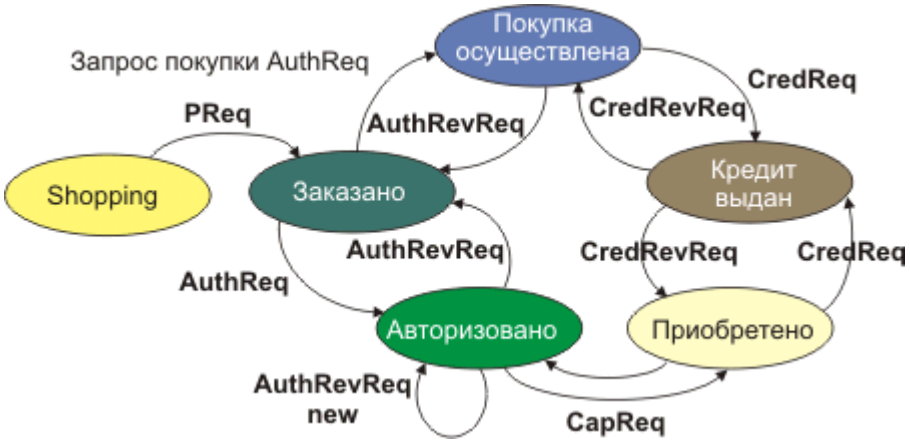

Рисунок 2 – Диаграмма реализации протокола SET

Начальным состоянием покупателя является *shopping*. Когда решение о покупке принято, программой клиента посылается запрос PReq и система переходит в состояние *заказано*. Запрос PReq включает в себя инструкцию OI (Order Instruction) и платежную инструкцию PI. Отклик PRes держателю карты может быть прислан немедленно или с некоторой задержкой. Полученная в отклике информация зависит от состояния протокольной машины (принят заказ, транзакция авторизована и т.д.).

Продавец посылает запрос авторизации платежному серверу, но флаг CaptureNow не устанавливается равным “истинно”, так как запрос оплаты (capture request) будет обработан позже. В состоянии *авторизовано* допускается частичный пересмотр условий сделки, при этом система может вернуться в состояние *заказано* или остаться в состоянии *авторизовано*. Продавец теперь имеет платежное обязательство от эмитента карты, но он должен обработать запрос покупки, для того чтобы получить соответствующую оплату. Запрос CapReq переводит транзакцию в состояние *приобретено* (*Captured* - сделка оплачена) и заказ обрабатывается.

Если поступит запрос отмены сделки, система возвращается в состояние *авторизовано*. Далее владелец карты может запросить кредит. В этом случае обрабатывается запрос кредита, переводя транзакцию из состояния *покупка осуществлена* (sale processed) в состояние *кредит выдан* (credit issued).

Запрос покупки (Sale Request) используется, когда продавец знает, что заказанный товар на складе и может быть поставлен немедленно при наличии авторизации. Этот запрос используется также в случае заказа товара или услуг, доставляемых через Интернет. Когда расчетный центр (Payment Gateway) обрабатывает запрос, происходит переход транзакции в состояние *покупка осуществлена*. С финансовой точки зрения состояния *sale processed* (обработана) и *captured* (оплачена) являются эквивалентными. В случае необходимости возврата денег клиенту, запрос кредита (CredReq) переводит систему в состояние *кредит получен*. Следует учитывать, что реализации некоторых компаний не поддерживают частичный возврат денег (сумма из запроса AuthRevReq копируется в сообщение AuthRevRes).

Когда продавец не может выполнить заказ в полном объеме сразу, он поставляет имеющиеся в наличии товары, а нехватающие заказывает дополнительно. Продавец может предложить клиенту различные схемы оплаты, например, осуществить оплату заказа в несколько этапов, или в случае предоставления Интернет услуг оплата может происходить на регулярной основе раз в месяц без участия самого держателя кредитной карты.

Протокол SET позволяет расчетному центру (Payment Gateway) определять, будет ли продавец получать номер счета владельца карты. Если эмитент карты решает не выдавать эту информацию, продавцу должен быть предоставлен какой-то другой механизм для возвращения сдачи в рамках текущей транзакции.

Список литературы, рекомендуемый к использованию по данной теме.

Основная: 1-3

.

Тема 9. Реализация защищенных платежных систем

Лабораторная работа № 17-18.

Разработка механизмов защиты электронных данных в платежных системах виртуального банка

Формируемые компетенции: ПК-1.

Теоретическая часть:

Задание 1. Разработать и вербально описать электронную платежную систему виртуального банка.

Задание 2. Разработать и вербально описать механизмы защиты электронных данных в электронных пластиковых картах.

Задание 3. Разработать и вербально описать механизм генерации персонального идентификационного номера для электронных пластиковых карт.

Пример оформления отчета по работе

ЭЛЕКТРОННАЯ ПЛАТЕЖНАЯ СИСТЕМА

Электронной платежной системой называют совокупность методов и реализующих их субъектов, обеспечивающих в рамках системы использование банковских пластиковых карт в качестве платежного средства.

Пластиковая карта - это персонифицированный платежный инструмент, предоставляющий пользующемуся этой картой лицу возможность безналичной оплаты товаров и услуг, а также получения наличных средств в банковских автоматах и отделениях банков. Предприятия торговли и сервиса и отделения банков, принимающие карту в качестве платежного инструмента, образуют приемную сеть точек обслуживания карты.

Неавтоматизированная процедура приема платежа с помощью карты сравнительно проста. В первую очередь кассир предприятия должен убедиться в подлинности пластиковой карты. При оплате предприятие должно перенести реквизиты пластиковой карты клиента на специальный чек с помощью копировальной машины-импринтера, занести в чек сумму, на которую была совершена покупка или оказана услуга, и получить подпись клиента.

В последние годы широкую популярность приобрели автоматизированные торговые POS-терминалы (Point-Of-Sale - оплата в точке продажи) и банкоматы. При использовании POS-терминалов нет необходимости в заполнении слипов. Клиент вводит в терминал свой PIN-код (Personal Identification Number - персональный идентификационный номер), известный только ему. Элементы PIN-кода включаются в общий алгоритм шифрования записи на магнитной полосе и служат электронной подписью владельца карты. На клавиатуре POS-терминала набирается сумма сделки.

Для обеспечения надежной работы электронная платежная система должна быть надежно защищена. С точки зрения информационной безопасности в системах электронных платежей существуют следующие уязвимые места:

– пересылка платежных и других сообщений между банком и клиентом и между банками;

– обработка информации внутри организаций отправителя и получателя сообщений;

– доступ клиентов к средствам, аккумулированным на счетах.

Для обеспечения функций защиты информации на отдельных узлах системы электронных платежей должны быть реализованы следующие механизмы защиты:

управление доступом на оконечных системах;

контроль целостности сообщения;

обеспечение конфиденциальности сообщения;

взаимная аутентификация абонентов;
невозможность отказа от авторства сообщения;
гарантии доставки сообщения;
невозможность отказа от принятия мёр по сообщению;
регистрация последовательности сообщений,
контроль целостности последовательности сообщений.

ЭЛЕКТРОННЫЕ ПЛАСТИКОВЫЕ КАРТЫ

Применение POS-терминалов и банкоматов возможно при использовании некоторого носителя информации, который мог бы идентифицировать пользователя и хранить определенные учетные данные. В качестве такого носителя информации выступают пластиковые карты.

Пластиковая карта представляет собой пластину стандартных размеров (85,6x53,9x0,76 мм), изготовленную из специальной, устойчивой к механическим и термическим воздействия пластмассы. Одна из основных функций пластиковой карты - обеспечение идентификации использующего ее лица как субъекта платежной системы. Для этого на пластиковую карту наносят логотипы банка-эмитента и платежной системы, обслуживающей эту карту, имя держателя карты, номер его счета, срок действия карты и т.п. Кроме того, на карте может присутствовать фотографий держателя и его подпись. Алфавитно-цифровые данные - имя номер счета и др. - могут быть эмбоссированы, т.е. нанесены рельефным шрифтом. Это дает возможность при ручной обработке принимаемых к оплате карт быстро перенести данные на чек с помощью специального устройства - импринтера, осуществляющего "прокатывание" карты (аналогично получению второго экземпляра при использовании копировальной бумаги).

По принципу действия различают пассивные и активные пластиковые карты. Пассивные пластиковые карты всего лишь хранят информацию на том или ином носителе. К ним относятся пластиковые карты с магнитной полосой.

Карты с магнитной полосой являются на сегодняшний день наиболее распространенными - в обращении находится свыше двух миллиардов карт подобного типа. Магнитная полоса располагается на обратной стороне карты и, в соответствии со стандартом ISO 7811, состоит из трех дорожек. Из них первые две предназначены для хранения идентификационных данных, а на третью дорожку можно записывать информацию (например, текущее значение лимита дебетовой карты).

Однако из-за невысокой надежности многократно повторяемого процесса записи и считывания запись на магнитную полосу обычно не практикуется, и такие карты используются только в режиме считывания информации.

Карты с магнитной, полосой относительно уязвимы для мошенничества. Для повышения защищенности своих карт системы Visa и MasterCard/Europay используют дополнительные графические средства защиты: голограммы и нестандартные шрифты для эмбоссирования. Платежные системы с подобными картами требуют on-line авторизации в торговых точках и, как следствие, наличия разветвленных, высококачественных средств коммуникации (телефонных линий). Поэтому с технической точки зрения подобные системы имеют серьезные ограничения по их применению в странах с плохо развитыми системами связи.

Отличительная особенность активных пластиковых карт - наличие встроенной в нее электронной микросхемы. Принцип пластиковой карты с электронной микросхемой запатентовал в 1974 г. француз Ролан Морено. Стандарт ISO 7816 определяет основные требования к картам на интегральных микросхемах или Чеповым картам. В недалеком будущем карты с микросхемой вытеснят карты с магнитной полосой. Поэтому остановимся более подробно на основных типах карт с микросхемой.

Карты с микросхемой можно классифицировать по нескольким признакам. Первый признак - функциональные возможности карты.

Здесь можно выделить следующие основные типы карт:

-карты-счетчики;
-карты с памятью;
-карты с микропроцессором.
Второй признак-тип обмена со считывающим устройством:
-карты с контактным считыванием;
-карты с индукционным считыванием.

Карты-счетчики применяются, как правило, в тех случаях, когда та или иная платежная операция требует уменьшения остатка на счете держателя карты на некоторую фиксированную сумму. Подобные карты используются в специализированных приложениях с предоплатой (плата за использование телефона-автомата, оплата автостоянки и т.д.) Очевидно, что применение карт со счетчиком ограничено и не имеет большой перспективы

Карты с памятью являются переходными между картами со счетчиком и картами с процессором. Карта с памятью - это в сущности перезаписываемая карта со счетчиком, в которой приняты меры, повышающие ее защищенность от атак злоумышленников. У простейших из существующих карт с памятью объем памяти может составлять от 32 байт до 16 килобайт. Эта память может быть реализована или в виде программируемого постоянного запоминающего устройства ППЗУ которое допускает однократную запись и многократное считывание, или в виде электрически стираемого программируемого постоянного запоминающего устройства ЭСППЗУ допускающего многократную запись и многократное считывание.

Карты с памятью можно подразделить на два типа с незащищенной (полнодоступной) и защищенной памятью.

В картах первого типа нет никаких ограничений на чтение и запись данных Их нельзя использовать в качестве платежных, так как специалист средней квалификации может их достаточно просто "взломать".

Карты второго типа имеют область идентификационных данных и одну или несколько прикладных областей. Идентификационная область карт допускает лишь однократную запись при персонализацию и в дальнейшем доступна лишь для считывания. Доступ к прикладным областям регламентируется и осуществляется только при выполнении определенных операций, в частности при вводе секретного PIN-кода.

Уровень защиты карт с памятью выше, чем у магнитных карт, и они могут быть использованы в прикладных системах, в которых финансовые риски, связанные с мошенничеством, относительно невелики. В качестве платежного средства карты с памятью используются для оплаты таксофонов общего пользования, проезда в транспорте, в локальных платежных системах (клубные карты) Карты с памятью применяются также в системах допуска в помещения и доступа к ресурсам компьютерных сетей (идентификационные карты). Карты с памятью имеют более низкую стоимость по сравнению с картами с микропроцессором

Карты с микропроцессором называют также интеллектуальными картами или смарт-картами (smart cards). Карты с микропроцессором представляют собой по сути микрокомпьютеры и содержат все соответствующие основные аппаратные компоненты центральный процессор (ЦП), оперативное запоминающее устройство (ОЗУ), постоянное запоминающее устройство (ПЗУ) и электрически стираемое программируемое ПЗУ (ЭСППЗУ).

В ПЗУ записан специальный набор программ, называемый операционной системой карты COS (Cards Operation System). Операционная система поддерживает файловую систему, базирующуюся в ЭСППЗУ (емкость которого обычно находится в диапазоне 1.8 Кбайт, но может достигать и 64 Кбайт) и обеспечивающую регламентацию доступа к данным. При этом часть данных может быть доступна только внутренним программам карточки.

Некоторые карты обеспечивают режим "самоблокировки" при попытке несанкционированного доступа. Смарт-карты позволяют существенно упростить процедуру идентификации клиента. Для проверки PIN-кода применяется алгоритм, реализуемый микропроцессором на карте. Это позволяет отказаться от работы POS-терминала и банкомата в режиме реального времени и централизованной проверки PIN. Отмеченные выше особенности делают смарт-карту высокозащищенным платежным инструментом, который может быть использован в финансовых приложениях, предъявляющих повышенные требования к защите информации. Именно поэтому микропроцессорные смарт-карты рассматриваются в настоящее время как наиболее перспективный вид пластиковых карт.

По принципу взаимодействия со считывающим устройством различают карты двух типов:

-карты с контактным считыванием;

-карты с бесконтактным считыванием.

Карта с контактным считыванием имеет на своей поверхности 8.10 контактных пластин. Размещение контактных пластин, их количество и назначение выводов различны у разных производителей и естественно, что считыватели для карт данного типа различаются между собой.

В последние годы начали широко применяться карты с бесконтактным считыванием. В них обмен данными между картой и считывающим устройством производится индукционным способом. Очевидно, что такие карты надежнее и долговечнее.

Персонализацию карты осуществляется при выдаче карты клиенту. При этом на карту заносятся данные, позволяющие идентифицировать карту и ее держателя, а также осуществить проверку платежеспособности карты при приеме ее к оплате или выдаче наличных денег.

Под авторизацией понимают процесс утверждения продажи или выдачи наличных по карте. Для проведения авторизации точка обслуживания делает запрос платежной системе о подтверждении полномочий предъявителя карты и его финансовых возможностей. Технология авторизации зависит от типа карты, схемы платежной системы и технической оснащенности точки обслуживания. Исторически сложилось так, что первоначальным способом персонализации карт было эмбоссирование.

Эмбоссирование - это процесс рельефного тиснения данных на пластиковой основе карты. На картах банков-эмитентов эмбоссируются, как правило, следующие данные: номер карты; даты начала и окончания срока ее действия; фамилия и имя владельца. Некоторые платежные системы, например Visa, требуют тиснения двух специальных символов, однозначно идентифицирующих принадлежность банка-эмитента к платежной системе. Эмбоссеры (устройства для тиснения рельефа на карте) выпускает ограниченный круг изготовителей. В ряде стран Запада законодательно запрещена свободная продажа эмбоссеров. Специальные символы, подтверждающие принадлежность карты к той или иной платежной системе, поставляются владельцу Эмбоссеры только с разрешения руководящего органа платежной системы. Эмбоссированная карта может служить средством платежа при использовании импринтера - устройства для прокатки слипа (чека), подтверждающего совершенную платежную операцию.

К персонализации карт относится также кодирование магнитной полосы либо программирование микросхемы.

Кодирование магнитной полосы производится, как правило, на том же оборудовании, что и эмбоссирование. При этом часть информации о карте, содержащая номер карты и период ее действия, одинаковая как на магнитной полосе, так и на рельефе. Однако бывают ситуации, когда после первичного кодирования требуется дополнительно занести информацию на магнитную дорожку. В этом случае применяются специальные устройства с Функцией "чтение-запись". Это возможно, в частности, когда PIN-код для

пользования картой не формируется специальной программой, а может быть выбран клиентом по своему усмотрению.

Персональный идентификационный номер

Испытанным способом идентификации держателя банковской карты является использование секретного персонального идентификационного номера PIN. Значение PIN должно быть известно только держателю карты. Длина PIN должна быть достаточно большой, чтобы вероятность угадывания злоумышленником правильного значения с помощью атаки полного перебора значений была приемлемо малой. С другой стороны, длина PIN должна быть достаточно короткой, чтобы дать возможность держателям карт запомнить его значение. Рекомендуемая длина PIN составляет 4.8 десятичных цифр, но может достигать 12.

Предположим, что PIN имеет длину четыре цифры, тогда противник, пытающийся подобрать значение PIN к банковской карте, стоит перед проблемой выбора одной из десяти тысяч возможностей. Если число попыток ввода некорректного значения PIN ограничивается пятью на карту в день, этот противник имеет шансы на успех менее чем 1: 2000. Но на следующий день противник может попытаться снова, и его шансы увеличиваются до 1: 1000. Каждый следующий день увеличивает вероятность успеха противника. Поэтому многие банки вводят абсолютный предел на число неверных попыток ввода PIN на карту, чтобы исключить атаку такого рода. Если установленный предел превышен, считается, что данная карта неправильная, и ее отбирают.

Значение PIN однозначно связано с соответствующими атрибутами банковской карты, поэтому PIN можно трактовать как подпись держателя карточки. Чтобы инициировать транзакцию, держатель карты, который использует POS-терминал, вставляет свою карту в специальную Щель считывателя и вводит свой PIN, используя специальную клавиатуру терминала. Если введенное значение PIN и номер счета клиента, записанный на магнитной полосе карты, согласуются между собой, тогда инициируется транзакция.

Защита персонального идентификационного номера PIN для банковской карты является критичной для безопасности всей платежной системы. Банковские карты могут быть потеряны, украдены или подделаны. В таких случаях единственной контрмерой против несанкционированного доступа остается секретное значение PIN. Вот почему открытая форма PIN должна быть известна только законному владельцу карты. Она никогда не хранится и не передается в рамках системы электронных платежей. Очевидно, значение PIN нужно держать в секрете в течение всего срока действия карты.

Метод генерации значения PIN оказывает существенное влияние на безопасность электронной платежной системы. Вообще, персональные идентификационные номера могут формироваться либо банком, либо держателями карт. В частности, клиент различает два типа PIN:

-PIN, назначенный ему банком, выдавшим карту;

-PIN, выбираемый держателем карты самостоятельно.

Если PIN назначается банком, банк обычно использует один из двух вариантов процедур генерации PIN.

При первом варианте PIN генерируется криптографически из номера счета держателя карточки. Процесс генерации назначаемого PIN из номера счета показан на рис.3. Сначала номер счета клиента дополняется нулями или другой константой до 16 шестнадцатеричных цифр (8 байт). Затем получившиеся 8 байт шифруются по алгоритму DES с использованием секретного ключа. Из полученного шифр-текста длиной 8 байт поочередно выделяют 4-битовые блоки, начиная с младшего байта. Если число, образуемое этими битами, меньше 10, то полученная цифра включается в PIN, иначе это значение не используется. Таким путем обрабатывают все 64 бита (8 байт) Если в результате обработки не удалось получить сразу требуемое количество десятичных цифр, то обращаются к неиспользованным 4-битовым блокам, из которых вычитают 10.

Очевидное достоинство этой процедуры заключается в том, что значение PIN не нужно хранить внутри электронной платежной системы. Недостатком этого подхода является то, что при необходимости изменения PIN требуется выбор либо нового счета клиента, либо нового криптографического ключа Банки предпочитают, чтобы номер счета клиента оставался фиксированным. С другой стороны, поскольку все PIN вычисляют, используя одинаковый криптографический ключ, изменение одного PIN при сохранении счета клиента неизбежно влечет за собой изменение всех персональных идентификационных номеров

Использование PIN, назначенного банком, неудобно для клиента даже при небольшой его длине Такой PIN трудно удержать в памяти, и поэтому держатель карты может записать его куда-нибудь Главное - это не записать PIN непосредственно на карту или какое-нибудь другое видное место Иначе задача злоумышленника будет сильно облегчена.

Главное требование безопасности состоит в том, что значение PIN должно запоминаться владельцем карты и никогда не должно храниться в любой читабельной форме. Но люди несовершенны и очень часто забывают свои значения PIN. Поэтому банки должны заранее заготовить специальные процедуры для таких случаев. Банк может реализовать один из следующих подходов. Первый основан на восстановлении забытого клиентом значения PIN и отправке его обратно владельцу карты. При втором подходе просто генерируется новое значение PIN.

При идентификации клиента по значению PIN и предъявленной карте используются два основных способа проверки PIN. неалгоритмический и алгоритмический. Неалгоритмический способ проверки PIN не требует применения специальных алгоритмов. Проверка PIN осуществляется путем непосредственного сравнения введенного клиентом PIN со значениями, хранимыми в базе данных. Обычно база данных со значениями PIN клиентов шифруется методом прозрачного шифрования, чтобы повысить ее защищенность, не усложняя процесса сравнения. Алгоритмический способ проверки PIN заключается в том, что введенный клиентом PIN преобразуют по определенному алгоритму с использованием секретного ключа и затем сравнивают со значением PIN, хранящимся в определенной форме на карте. Достоинства этого метода проверки:

-отсутствие копии PIN на главном компьютере исключает его раскрытие персоналом банка;

-отсутствие передачи PIN между банкоматом или POS-терминалом и главным компьютером банка исключает его перехват злоумышленником или навязывание результатов сравнения;

-упрощение работы по созданию программного обеспечения системы, так как уже нет необходимости действий в реальном масштабе времени.

Список литературы, рекомендуемый к использованию по данной теме.

Основная: 1-3

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

для обучающихся по организации и проведению самостоятельной работы
по дисциплине «Методы и средства защиты информации в банковских системах»
для студентов направления подготовки
10.03.01«Информационная безопасность»
Направленность (профиль):
«Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности»

Ставрополь,
2026

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Целью изучения дисциплины «Методы и средства защиты информации в банковских системах» является формирование у студентов способностей решать профессиональные задачи по обеспечению информационной безопасности в банковских системах путем применения современных методов и средств защиты информации, а также приобретение набора общепрофессиональных компетенций будущего бакалавра по направлению подготовки 10.03.01 «Информационная безопасность».

Основными задачами изучения дисциплины являются:

1. Раскрытие сущности и значения информационной безопасности в банковских системах, их места в системе национальной безопасности.

2. Определение теоретических, концептуальных, методологических, организационных и технических основ обеспечения безопасности информации в автоматизированных банковских системах.

1. Общая характеристика самостоятельной работы студента при изучении дисциплины

Основными видами учебной работы по достижению результатов освоения дисциплины являются лекции, практические работы и самостоятельная работа студентов (СРС).

На лекциях раскрываются основные положения и понятия курса, формируются знания в области защиты информации в банковских системах. На практических работах формируются умения и навыки, необходимые для решения задач профессиональной деятельности.

Приступая к изучению учебной дисциплины, необходимо ознакомиться с учебной программой, получить в библиотеке рекомендованные учебные пособия, а также получить у ведущего преподавателя в электронном виде конспекты лекций, методические рекомендации к практическим работам и тестовые, завести новую тетрадь для конспектирования лекций и выполнения практических работ.

Для изучения дисциплины предлагается список основной и дополнительной литературы. Основная литература предназначена для обязательного изучения, дополнительная – поможет более глубоко освоить отдельные вопросы, подготовить исследовательские задания и выполнить задания для самостоятельной работы.

В ходе лекционных занятий студент обязан осуществлять конспектирование учебного материала, особое внимание, обращая на категории, формулировки, раскрывающие содержание тех или иных понятий, физических явлений, процессов, эффектов. В рабочих конспектах желательно оставлять поля, на которых следует делать пометки из рекомендованной литературы, дополнять материал прослушанной лекции, формулировать научные выводы и практические рекомендации. Студент имеет право задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Самостоятельная работа студентов над материалом учебной дисциплины является неотъемлемой частью учебного процесса и должна предполагать углубление знания учебного материала, излагаемого на аудиторных занятиях, и приобретение дополнительных знаний по отдельным вопросам самостоятельно.

Основными видами самостоятельной работы студентов по учебной дисциплине являются:

- самостоятельное изучение учебного материала по заданным темам;
- подготовка к лабораторным работам, оформление отчета по выполненному практическому занятию и подготовка к собеседованию по результатам работы.

Основными методами самостоятельной работы студентов являются:

1) для овладения знаниями:

- чтение текста (конспекта лекций, учебника, дополнительной литературы) и

конспектирование текста;

– работа с нормативными документами;
– поиск информации в Интернет;

2) для закрепления и систематизации знаний:

– работа с конспектом лекции (обработка текста);
– повторная работа над учебным материалом (учебника, дополнительной литературы, слайдами);
– составление плана и тезисов ответа или графическое изображение структуры ответа;
– составление таблиц для систематизации учебного материала;
– изучение нормативных документов;
– ответы на контрольные вопросы;

3) для формирования умений:

– подготовка к практическим занятиям;
– решение задач и практических заданий;
– подготовка отчетов по практическим занятиям;
– рефлексивный анализ профессиональных умений.

В случае пропуска учебного занятия студент может воспользоваться содержанием различных блоков учебно-методического комплекса (лекции, практические занятия, контрольные вопросы и тесты) для самоподготовки и освоения темы. Для самоконтроля необходимо использовать вопросы и задания, предлагаемые к практическим занятиям, а также варианты тестовых заданий.

2. Технологическая карта самостоятельной работы студента

Коды реализуемых компетенций, индикатора(ов)	Вид деятельности студентов	Средства и технологии оценки	Обьем часов, в том числе		
			СРС	Контактная работа с преподавателем	Всего
7 семестр					
ПК-1 ИД-1	Подготовка к лекциям	Конспект	11.00	2.00	13.00
ПК-1 ИД-1	Подготовка к лабораторным работам	Письменный отчет с решением разноуровневых задач	12.00	2.00	14.00
ПК-1 ИД-1	Самостоятельное изучение литературы	Конспект	11.00	2.00	13.00
ПК-1 ИД-1	Подготовка доклада	Письменный отчет	12.00	2.00	14.00
Итого за 7 семестр			46.00	8.00	54.00
Итого			46.00	8.00	54.00

3. Порядок выполнения самостоятельной работы

3.1 Методические рекомендации по изучению теоретического материала

Комплексное изучение предлагаемой студентам учебной дисциплины «Методы и средства защиты информации в банковских системах» предполагает овладение материалами лекций, учебников, программы, творческую работу студентов в ходе проведения практических занятий, а также систематическое выполнение заданий для самостоятельной работы.

В ходе лекций раскрываются основные вопросы в рамках рассматриваемых тем, делаются акценты на наиболее сложные и интересные положения изучаемого материала, которые должны быть приняты студентами во внимание. Материалы лекций являются основой для подготовки студентов к практическим занятиям.

Работа с конспектом лекций

Просмотрите конспект сразу после занятий. Отметьте материал конспекта лекций, который вызывает затруднения для понимания. Попытайтесь найти ответы на затруднительные вопросы, используя предлагаемую литературу. Если самостоятельно не удалось разобраться в материале, сформулируйте вопросы и обратитесь на текущей консультации или на ближайшей лекции за помощью к преподавателю.

Каждую неделю отводите время для повторения пройденного материала, проверяя свои знания, умения и навыки по контрольным вопросам и тестам.

Выполнение лабораторных работ по дисциплине «Методы и средства защиты информации в банковских системах»

На первом занятии получите у преподавателя задания по курсу, планы подготовки к лабораторным работам. Обзаведитесь всем необходимым методическим обеспечением.

Перед лабораторными работами изучите теорию вопроса, предполагаемого к исследованию, ознакомьтесь с опытом других исследователей в этом направлении.

Целью лабораторных работ является:

- закрепление методов приложения теории к решению лабораторных работ анализа и синтеза психологического знания;
- проверка уровня понимания студентами вопросов, рассмотренных на лекциях и по учебной литературе, степени и качества усвоения материала;
- обучение навыкам освоения методики эксперимента и работы с нормативно-справочной литературой;
- восполнение пробелов в пройденной теоретической части курса и оказание помощи в его усвоении.

3.2 Методические рекомендации по написанию и оформлению доклада

1. Общие положения

1.1. Доклад, как вид самостоятельной работы в учебном процессе, способствует формированию навыков исследовательской работы, расширяет познавательные интересы, учит критически мыслить.

1.2. При написании доклада по заданной теме студент составляет план, подбирает основные источники.

1.3. В процессе работы с источниками систематизирует полученные сведения, делает выводы и обобщения.

1.4. К докладу по крупной теме могут привлекать несколько студентов, между которыми распределяются вопросы выступления.

2. Выбор темы доклада

2.1. Тематика доклада обычно определяется преподавателем, но в определении темы инициативу может проявить и студент.

2.2. Прежде чем выбрать тему доклада, автору необходимо выявить свой интерес, определить, над какой проблемой он хотел бы поработать, более глубоко ее изучить.

3. Этапы работы над докладом
3.1. Формулирование темы, причем она должна быть не только актуальной по своему значению, но и оригинальной, интересной по содержанию.
3.2. Подбор и изучение основных источников по теме (как правильно, при разработке доклада используется не менее 8-10 различных источников).
3.3. Составление списка использованных источников.
3.4. Обработка и систематизация информации
3.5. Разработка плана доклада.
3.6. Написание доклада.
3.7. Публичное выступление с результатами исследования.
4. Структура доклада:
- титульный лист
- оглавление (в нем последовательно излагаются названия пунктов доклада, указываются страницы, с которых начинается каждый пункт);
- введение (формулирует суть исследуемой проблемы, обосновывается выбор темы, определяются ее значимость и актуальность, указываются цель и задачи доклада, дается характеристика используемой литературы);
- основная часть (каждый раздел ее, доказательно раскрывая отдельную проблему или одну из ее сторон, логически является продолжением предыдущего; в основной части могут быть представлены таблицы, графики, схемы);
- заключение (подводятся итоги или дается обобщенный вывод по теме доклада, предлагаются рекомендации);
- список использованных источников
5. Структура и содержание доклада
5.1. Введение - это вступительная часть научно-исследовательской работы. Автор должен приложить все усилия, чтобы в этом небольшом по объему разделе показать актуальность темы, раскрыть практическую значимость ее, определить цели и задачи эксперимента или его фрагмента.
5.2. Основная часть. В ней раскрывается содержание доклада.
Как правило, основная часть состоит из теоретического и практического разделов. В теоретическом разделе раскрываются история и теория исследуемой проблемы, дается критический анализ литературы и показываются позиции автора. В практическом разделе излагаются методы, ход, и результаты самостоятельно проведенного эксперимента или фрагмента.
В основной части могут быть также представлены схемы, диаграммы, таблицы, рисунки и т.д.
5.3. В заключении содержатся итоги работы, выводы, к которым пришел автор, и рекомендации. Заключение должно быть кратким, обязательным и соответствовать поставленным задачам.
5.4. Список использованных источников представляет собой перечень использованных книг, статей, фамилии авторов приводятся в алфавитном порядке, при этом все источники даются под общей нумерацией литературы. В исходных данных источника указываются фамилия и инициалы автора, название работы, место и год издания.
5.5. Приложение к докладу оформляются на отдельных листах, причем каждое должно иметь свой тематический заголовок и номер, который пишется в правом верхнем углу, например: «Приложение 1»
6. Требования к оформлению доклада
6.1. Объем доклада может колебаться в пределах 5-15 печатных страниц; все приложения к работе не входят в ее объем.
6.2. Доклад должен быть выполнен грамотно, с соблюдением культуры изложения.
6.3. Обязательно должны иметься ссылки на используемую литературу.

6.4. Должна быть соблюдена последовательность написания библиографического аппарата.
7. Критерии оценки доклада
- актуальность темы исследования;
- соответствие содержания теме;
- глубина проработки материала; правильность и полнота использования источников;
- соответствие оформления доклада стандартам.
По усмотрению преподавателя доклады могут быть представлены на семинарах, научно-практических конференциях, а также использоваться как зачетные работы по пройденным темам.

3.3 Методические рекомендации по конспектированию первоисточников

Изучение и анализ литературных источников является обязательным видом самостоятельной работы студентов. Изучение литературы по избранной теме имеет своей задачей проследить характер постановки и решения определенной проблемы различными авторами, аргументацию их выводов и обобщений, провести анализ и систематизировать полученный материал на основе собственного осмысления с целью выяснения современного состояния вопроса.

Проработка отобранного материала обязательно должна идти с одновременным ведением записей прочитанного и своих замечаний. Запись может иметь как форму конспекта, так и выписок, а также картотеку положений, тезисов, идей, методик, что в дальнейшем облегчит классификацию и систематизацию полученного материала. Такого рода записи являются лучшим способом накопления и первичной обработки материал, одной из обязательных форм организации умственного труда.

Планом удобно пользоваться при подготовке к устному выступлению по выбранной теме. Каждый пункт плана должен раскрывать одну из сторон избранной темы, а весь план должен охватывать ее целиком.

Тезисы предполагают сжатое изложение основных положений текста в форме утверждения или отрицания. Они являются более совершенной формой записей и представляют основу для дискуссии. К тому же их легко запомнить.

Конспектирование – процесс мысленной переработки и письменной фиксации информации, в виде краткого изложения основного содержания, смысла какого-либо текста.

Результат конспектирования – запись, позволяющая конспектирующему немедленно или через некоторый срок с нужной полнотой восстановить полученную информацию. Конспект в переводе с латыни означает «обзор». По существу его и составлять надо как обзор, содержащий основные мысли текста без подробностей и второстепенных деталей. Конспект носит индивидуализированный характер: он рассчитан на самого автора и поэтому может оказаться малопонятным для других.

Для того чтобы осуществлять этот вид работы, в каждом конкретном случае необходимо грамотно решить следующие задачи:

1. Сориентироваться в общей композиции текста (уметь определить вступление, основную часть, заключение).
2. Увидеть логико-смысловую канву сообщения, понять систему изложения автором информации в целом, а также ход развития каждой отдельной мысли.
3. Выявить «ключевые» мысли, т. е. основные смысловые вехи, на которые «нанизано» все содержание текста.
4. Определить детализирующую информацию.
5. Лаконично сформулировать основную информацию, не перенося на письмо все целиком и дословно.

Во всяком научном тексте содержится информация 2-х видов: основная и вспомогательная. Основной является информация, имеющая наиболее существенное значение для раскрытия

содержания темы или вопроса. К ней относятся: определения научных понятий, формулировки законов, теоретических принципов и т. д. Назначение вспомогательной информации – помочь читателю лучше усвоить предлагаемый материал. К этому типу информации относятся разного рода комментарии. Основную – записываем как можно полнее, вспомогательную, как правило, опускаем. Содержание конспектирования составляет переработка основной информации в целях ее обобщения и сокращения. Обобщить – значит представить ее в более общей, схематической форме, в виде тезисов, выводов, отдельных заголовков, изложения основных результатов и т. п. Читая, мы интуитивно используем некоторые слова и фразы в качестве опорных. Такие опорные слова и фразы называются ключевыми. Ключевые слова и фразы несут основную смысловую и эмоциональную нагрузку содержания текста.

Выбор ключевых слов – это первый этап смыслового свертывания, смыслового сжатия материала.

Важными требованиями к конспекту являются наглядность и обозримость записей и такое их расположение, которое давало бы возможность уяснить логические связи и иерархию понятий.

По форме *конспекты подразделяются* на формализованные и графические.

1. Формализованные (все записи вносятся в заранее подготовленные таблицы).

Это удобно, во-первых, при конспектировании материалов, когда перечень характеристик описываемых предметов или явлений более или менее постоянен, во-вторых, при подготовке единого конспекта по нескольким источникам. Особенно если есть необходимость сравнения отдельных данных. Разновидностью формализованного конспекта является запись, составленная в форме ответов на заранее подготовленные вопросы, обеспечивающие исчерпывающие характеристики однотипных предметов или явлений.

2. Графические (элементы конспектируемой работы располагаются в таком виде, при котором видна иерархия понятий и взаимосвязь между ними).

По каждой работе может быть не один, а несколько графических конспектов, отображающих книгу в целом и отдельные ее части. Ведение графического конспекта - наиболее совершенный способ изображения внутренней структуры книги, а сам этот процесс помогает усвоению ее содержания.

Можно выделить следующие основные **типы конспектов: плановый, текстуальный, сводный, тематический.**

Плановый – легко получить с помощью предварительно сделанного плана произведения, каждому вопросу плана отвечает определенная часть конспекта:

а) вопросно-ответный (на пункты плана, выраженные в вопросительной форме, конспект дает точные ответы);

б) схематичный плановый конспект (отражает логическую структуру и взаимосвязь отдельных положений).

Текстуальный – это конспект, созданный в основном из цитат.

Сводный конспект – сочетает выписки, цитаты, иногда тезисы; часть его текста может быть снабжена планом.

Тематический – дает более или менее исчерпывающий ответ (в зависимости из числа привлеченных источников и другого материала, например, своих же записей) на поставленный вопрос – тему: обзорный; хронологический.

Роль конспекта – чисто учебная: он помогает зафиксировать основные понятия и положения первичного текста и в нужный момент их воспроизвести, например, при написании реферата или подготовке к экзамену.

Способы конспектирования.

- Тезисы – это кратко сформулированные основные мысли, положения изучаемого материала. Тезисы лаконично выражают суть читаемого, дают возможность раскрыть содержание. Приступая к освоению записи в виде тезисов, полезно в самом тексте отмечать

места, наиболее четко формулирующие основную мысль, которую автор доказывает (если, конечно, это не библиотечная книга). Часто такой отбор облегчается шрифтовым выделением, сделанным в самом тексте.

- Линейно-последовательная запись текста. При конспектировании линейно – последовательным способом целесообразно использование плакатно-оформительских средств, которые включают в себя следующие:

- сдвиг текста конспекта по горизонтали, по вертикали;
- выделение жирным (или другим) шрифтом особо значимых слов;
- использование различных цветов;
- подчеркивание;
- заключение в рамку главной информации.

- С***пособ «вопросов – ответов».*** Он заключается в том, что, поделив страницу тетради пополам вертикальной чертой, конспектирующий в левой части страницы самостоятельно формулирует вопросы или проблемы, затронутые в данном тексте, а в правой части дает ответы на них.

Одна из модификаций способа «вопросов – ответов» - таблица, где место вопроса занимает формулировка проблемы, поднятой автором (лектором), а место ответа – решение данной проблемы. Иногда в таблице могут появиться и дополнительные графы: например, «мое мнение» и т. п.

- С***хема с фрагментами*** **–** способ конспектирования, позволяющий ярче выявить структуру текста, - при этом фрагменты текста (опорные слова, словосочетания, пояснения всякого рода) в сочетании с графикой помогают созданию рационально - лаконичного конспекта.

- ***Простая схема*** **–** способ конспектирования, близкий к схеме с фрагментами, объяснений к которой конспектирующий не пишет, но должен уметь давать их устно. Этот способ требует высокой квалификации конспектирующего. В противном случае такой конспект нельзя будет использовать.

- ***Параллельный способ*** конспектирования. Конспект оформляется на двух листах параллельно или один лист делится вертикальной чертой пополам и записи делаются в правой и в левой части листа.

Однако лучше использовать разные способы конспектирования для записи одного и того же материала.

Комбинированный конспект – вершина овладения рациональным конспектированием. При этом умело используются все перечисленные способы, сочетая их в одном конспекте (один из видов конспекта свободно перетекает в другой в зависимости от конспектируемого текста, от желания и умения конспектирующего). Именно при комбинированном конспекте более всего проявляется уровень подготовки и индивидуальность студента.

Принципы составления конспекта прочитанного.

1. Записать все выходные данные источника: автор, название, год и место издания. Если текст взят из периодического издания (газеты или журнала), то записать его название, год, месяц, номер, число, место издания.
2. Выделить поля слева или справа, можно с обеих сторон. Слева на полях отмечаются страницы оригинала, структурные разделы статьи или книги (названия параграфов, подзаголовки и т. п.), формулируются основные проблемы. Справа – способы фиксации прочитанной информации.

Один из видов чтения – углубленное – предполагает глубокое усвоение прочитанного и часто сохранение информации в целях последующего обращения к ней. Эффективность такого чтения повышается, если прочитанное зафиксировано не только в памяти, но и на бумаге. Психологи утверждают, что записанное лучше и полнее усваивается, прочнее откладывается в памяти. Установлено, что если прочитать 1000 слов и затем записать 50, подытоживающих прочитанное, то коэффициент усвоения будет выше, чем, если прочитать 10000 слов, не записав ни одного. Кроме того, при записи прочитанного формируется навык

свертывания информации. И, наконец, чередование чтения и записывания уменьшает усталость, повышает работоспособность и производительность умственного труда.

1. Резюмирование.

Резюме – краткий итог прочитанного, содержащий его оценку. Резюме характеризует основные выводы книги, главные итоги.

Выбор языковых средств для построения резюме-выводов подчинен основной задаче свертывания информации: минимум языковых средств – максимум информации. Это обычно одно – три четких, кратких, выразительных предложения, раскрывающих, по мнению автора, самую суть описываемого объекта.

2. Аннотация.

Аннотация – краткая обобщенная характеристика печатной работы (книги, статьи), включающая иногда и его оценку. Это наикратчайшее изложение содержания первичного документа, дающее общее представление о теме.

Основное ее назначение – дать некоторое представление о книге (статье, научной работе) с тем, чтобы рекомендовать ее определенному кругу читателей или воспользоваться своими записями при выполнении работы исследовательского, реферативного характера. Поэтому аннотации не требуется изложения содержания произведения, в ней лишь перечисляются вопросы, которые освещены в первоисточнике (содержание этих вопросов не раскрывается). Аннотация отвечает на вопрос: «О чем говорится в первичном тексте?», дает представление только о главной теме и перечне вопросов, затрагиваемых в тексте первоисточника.

Текст аннотации не стандартизирован. В научной литературе можно встретить различные требования к составлению аннотаций. Например, текст справочной аннотации может включать следующие сведения:

· тип и название аннотируемого документа (монография, диссертация, сборник, статья и т. п.)

· задачи, поставленные автором аннотируемого документа

· метод, которым пользовался автор (эксперимент, сравнительный анализ, компиляция других источников)

· принадлежность автора к определенной научной школе или направлению

· структуру аннотируемого документа

· предмет и тему произведения, основные положения и выводы автора

· характеристику вспомогательных иллюстративных материалов, дополнений, приложений, справочного аппарата, включая указатели и библиографию.

4.1 Вопросы для собеседования по самостоятельному изучению тем дисциплины

Тема 1. Базовые понятия дисциплины. Банковская система РФ.

1. Платежные средства.
2. Клиринг и взаиморасчет.

Тема 2. Электронная коммерция и платежные системы.

1. Электронные кошельки.
2. Мобильная коммерция.

Тема 3. Электронная коммерция и платежные системы.

1. Компоненты технологии электронного обмена данными (EDI).
2. Информационная безопасность электронного бизнеса.

Тема 4. Проблемы безопасности в банковской сфере.

1. Объекты защиты.
2. Классификация угроз.

3. Состав и структура системы безопасности банка.
4. Анализ риска и составление кризисных планов.

Тема 5. Политика безопасности в банковской сфере.
1. Оценка безопасности банковских систем.
2. Стандарты в области банковской безопасности.

Тема 6. Управление защитой банковских операций и АБС.
1. Дополнительные меры контроля.
2. Методы и механизмы защиты автоматизированных сетей.

Тема 7. Безопасность электронных платежей и платежных систем.
1. Обзор технологий электронных пластиковых карт.
2. Автоматические кассовые аппараты.
3. Особенности расчета в точке продажи.
4. Электронные чеки.

Тема 8. Безопасность платежей в INTERNET.
1. Сравнительная характеристика протоколов SSL и SET.

Тема 9. Реализация защищенных платежных систем.
1. Учетная система WebMoney Transfer.

4.2 Вопросы для собеседования по лабораторным занятиям

Лабораторное занятие 1. Вербальное и графическое моделирование виртуального банка.

Базовый уровень:
1. Описание виртуального банка.
2. Организационная структура виртуального банка.

Повышенный уровень:
1. План здания виртуального банка.

Лабораторное занятие 2. Структурное моделирование виртуальной автоматизированной банковской системы.

Базовый уровень:
1. Описание автоматизированной банковской системы виртуального банка.

Повышенный уровень:
1. Структурная схема автоматизированной банковской системы виртуального банка.

Лабораторное занятие 3. Информационное моделирование автоматизированных банковских операций.

Базовый уровень:
1. Описание и составление алгоритма реализации банковской операции – открытие платежной карты.
2. Описание и составление алгоритма реализации первичной банковской операции – пополнение\удержание.

Повышенный уровень:
1. Описание и составление алгоритма реализации внутренней банковской операции – снятие наличных денег через банкоматы.
2. Описание и составление алгоритма реализации операции – электронных платежей в торгово-сервисной точке.

Лабораторное занятие 4. Разработка политики безопасности виртуального банка.

Базовый уровень:

1. Замысел политики безопасности виртуального банка.

Повышенный уровень:

1. Документальное оформление политики безопасности виртуального банка.

Лабораторное занятие 5. Разработка системы управления защитой автоматизированной банковской системы.

Базовый уровень:

1. Описание модели типовых угроз и нарушителей информационной безопасности виртуального банка.

Повышенный уровень:

1. Описание системы информационной безопасности, на основе составленной на предыдущем занятии политики безопасности банка.
2. Описание процедуры управления доступом к информационным ресурсам автоматизированных систем и администрирования автоматизированной системой виртуального банка.

Лабораторное занятие 6. Разработка механизмов защиты электронных данных в платежных системах виртуального банка.

Базовый уровень:

1. Описание электронной платежной системы виртуального банка.
2. Описание механизмов защиты электронных данных в электронных пластиковых картах.

Повышенный уровень:

1. Описание механизма генерации персонального идентификационного номера для электронных пластиковых карт.

Лабораторное занятие 7. Разработка механизмов защиты платежной системы виртуального банка.

Базовый уровень:

1. Описание системы POS.
2. Описание механизмов обеспечения безопасности систем POS.

Повышенный уровень:

1. Описание механизмов обеспечения безопасности электронных платежей через сеть Internet.

Лабораторное занятие 8. Разработка алгоритма работы протокола безопасных электронных транзакций SET.

Базовый уровень:

1. Описание протокола безопасных электронных транзакций SET.
2. Диаграмма реализации протокола безопасных электронных транзакций SET.

Повышенный уровень:

1. Алгоритм протокола безопасных электронных транзакций SET.

Лабораторное занятие 9. Разработка рекомендаций по созданию защищенной платежной системы виртуального банка.

Базовый уровень:

1. Описание защищенной платежной системы виртуального банка.

Повышенный уровень:

1. Описание программно-аппаратных решений по созданию защищенной платежной системы виртуального банка.

5. Список рекомендуемой литературы

5.1. Основная литература

1. Афанасьева О.Н., Корниенко С.Л., Лаврушин О.И. Банковское дело: современная система кредитования. Учебное пособие. Гриф УМО МО РФ. 3-е изд., доп. – М.: КНОРУС, 2014. – 264 с. http://biblioclub.ru/index.php?page=book&id=445058
2. Ясенев, В.Н. Информационные системы и технологии в экономике / В.Н. Ясенев. – 3-е изд., перераб. и доп. – Москва :Юнити-Дана, 2015. – 560 с. : табл., граф., ил., схемы – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=115182

5.2. Дополнительная литература

1. Емельянова Н.З., Партыка Т.Л., Попов И.И. Основы построения автоматизированных информационных систем: Учебное пособие. – М.: ФОРУМ: ИНФРА-М, 2015. – 416с.
2. Ярочкин В.И. Безопасность банковских систем. – М.: «ОСЬ – 89», 2014. – 416 с.
3.Титоренко Г.А. Автоматизированные информационные технологии в экономике. – М.: Юнити, 2016. – 400 с.
4. Яковец Е.Н. Основы правовой защиты информации и интеллектуальной собственности: Учебное пособие. – М.: Юрлитинформ, 2016. – 400 с.

5.3. Методическая литература:

1. Электронный курс лекций:
2. Электронные методические рекомендации к практическим занятиям.
3. Стандарт банка России СТО БР ИББС-1.0-2010 Обеспечение информационной безопасности организаций банковской системы Российской Федерации: Общие положения. – М.: 2010.

5.4. Интернет-ресурсы:

1. Книги on-line по безопасности. – http://homepage.corbina.net/~ksi/ books.htm
2. Ликбез по защите информации в платежных системах, сайт – http://bankir.ru/tehnologii/s/likbez-po-zashchite-informatsii-v-platezhnykh-sistemakh-10003377/.

5.5. Программное обеспечение

1. Программа тестового контроля «Iren»;
2. Интегрированный офисный пакет MicrosoftOffice, содержащий Visio.