

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

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

по выполнению практических работ

по дисциплине «Защищённый электронный документооборот»

для студентов направления подготовки /специальности

10.03.01 «Информационная безопасность»

Направленность(профиль) «Организация и технологии защиты информации»

(по отрасли или в сфере профессиональной деятельности)

ОГЛАВЛЕНИЕ

<u>Тема 1: Основные объекты автоматизации документационного обеспечения управления. Основные угрозы информации в системах электронного документооборота</u>	
Практическое занятие 1,2 Предпроектный анализ информационной системы организации	3
<u>Тема 3: Доступ персонала к конфиденциальным сведениям</u> Практическое занятие 3 Выбор базового набора организационных и технических мер защиты информации.....	8
<u>Тема 4-5: Порядок организации защищённого электронного документооборота на предприятии. Порядок настройки систем электронного документооборота на структуру организации</u>	
Практическое занятие 4,5 Адаптация базового набора организационных и технических мер ЗИ.	15
<u>Тема 6-7: Современные электронные системы управления и работы с документами. Порядок защиты информации в систем электронного документооборота «Дело»</u>	
Практическое занятие 6,7 Уточнение базового набора организационных и технических мер ЗИ. Построение модели угроз для ИС организации	20
<u>Тема 8-9: Анализ требований нормативно-методических документов по организации построения системы защиты информации (СЗИ) в ИС организации. Предпроектный анализ информационной системы организации</u>	
Практическое занятие 8,9 Выбор технических средств для реализации выбранных технических мер защиты информации в ИС организации.....	26
<u>Тема 10-11: Порядок адаптации базового набора мер по защите информации. Порядок уточнения адаптированного набора мер по защите информации в ИС организации</u>	
Практическое занятие 10,11 Реализация выбранных организационных мер для системы защиты информации в ИС организации	37
<u>Тема 12-13: Определение актуальных угроз для ИС организации. Порядок выбора технических средств для реализации технических мер защиты информации</u> Практическое занятие 12,13 Оценка эффективности системы ЗИ в ИС организации	39
<u>Тема 14-16: Разработка технического задания на создание СЗИ в системе защищённого документооборота. Оценка эффективности СЗИ в ИС организации. Порядок организации отдела конфиденциально делопроизводства</u>	
Практическое занятие 14,15,16 Разработка технического задания на создание системы ЗИ в ИС организации	46

ВВЕДЕНИЕ

Дисциплина «Защищённый электронный документооборот» посвящена изучению научных и методических аспектов организации технологических стадий, выполнения процедур и операций в процессе получения, рассмотрения, исполнения, использования и хранения КД в любых структурах государственных и негосударственных сфер, проектирования рациональной технологической схемы защищённого документооборота.

Целью изучения дисциплины «Защищённый электронный документооборот» является формирование у студентов набора профессиональных компетенций по направлению подготовки 10.03.01 Информационная безопасность в области построения и совершенствования технологии защищённого документооборота в условиях применения разнообразных типов носителей документной информации, средств, способов и систем обработки и хранения КД.

Учебными задачами дисциплины являются:

- формирование системы знаний по организации конфиденциального делопроизводства на предприятии, необходимых для решения профессиональных задач, соответствующих базовому уровню профессиональной компетенции в области защиты информации;
- организация деятельности, направленной на применение знаний по вопросам организации конфиденциального документооборота в сфере профессиональных интересов;
- мотивация деятельности исследовательского характера для развития творческих способностей студентов.

В результате изучения дисциплины студенты должны:

знать:

- сущность и значение информации в развитии современного общества;
- нормативные и методические материалы по вопросам обеспечения информационной безопасности защищённого конфиденциального делопроизводства;
- технологию организации конфиденциального делопроизводства;
- методику анализа защищённости подсистемы конфиденциального делопроизводства;

уметь:

- проводить целенаправленный поиск в различных источниках информации по вопросам защиты конфиденциальной документированной информации, в том числе в глобальных компьютерных системах;
- использовать нормативные правовые документы при организации подсистемы защищённого конфиденциального делопроизводства;
- составлять обзор по вопросам обеспечения информационной безопасности защищённого конфиденциального делопроизводства;

владеть:

- методами подбора, изучения и обобщения научно-технической литературы, нормативных и методических материалов по вопросам обеспечения защищённого конфиденциального делопроизводства;
- технологией организации конфиденциального делопроизводства;
- методикой оценки эффективности функционирования защищённого конфиденциального делопроизводства.

Знания и практические навыки, полученные из курса «Защита и обработка конфиденциальных документов» необходимы для будущей профессиональной деятельности специалиста по защите информации.

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-4 Способен внедрять системы защиты информации в автоматизированных системах	ИД-1 разрабатывает организационно-распорядительные документы по защите информации в автоматизированных системах	Знает требования нормативных документов, регламентирующих порядок разработки текстовых и графических документов по защите информации, умеет разрабатывать различного вида графические и текстовые документы в составе проекта подсистемы защиты информации
	ИД-2 внедряет организационные меры по защите информации в автоматизированных системах	Знает состав, и порядок внедрения организационных мер по защите информации в автоматизированных системах, умеет внедрять организационные меры в систему защиты автоматизированной системы организации

Практическое занятие 1,2 Предпроектный анализ информационной системы организации

Тема 1-2: Основные объекты автоматизации документационного обеспечения управления Основные угрозы информации в системах электронного документооборота

1. Цель занятия.

- приобретение практических навыков анализа информационных систем
- приобретение практических навыков построения системы защиты информации в ИС.

2. Формируемые компетенции или их части

В результате выполнения работы студенты должны:

- уметь использовать нормативные правовые документы при организации подсистемы защищённого конфиденциального делопроизводства;
- владеть технологией организации конфиденциального делопроизводства.

3. Теоретическая часть

1.1 Анализ структуры и деятельности предприятия

На рисунке 1 представлена структура ОАО «Монокристалл»



Рисунок 1 – Структура ОАО «Монокристалл»

Основными видами деятельности АО «Монокристалл» являются:

- производство искусственного корунда,
- производство абразивных изделий,
- производство драгоценных металлов,
- производство диодов, транзисторов и прочих полупроводниковых приборов,
- производство интегральных электронных схем,
- производство фото- и кинооборудования,
- производство изделий технического назначения из драгоценных металлов,
- ремонт электронного и оптического оборудования,
- монтаж промышленных машин и оборудования,
- обработка отходов и лома драгоценных металлов,
- торговля оптовая прочими промежуточными продуктами,
- торговля оптовая неспециализированная,
- перевозка грузов специализированными автотранспортными средствами,
- технические испытания, исследования, анализ и сертификация,
- испытания и анализ физико-механических свойств материалов и веществ.

1.2 Анализ информационных ресурсов предприятия

Перечень защищаемых персональных данных

№ п/п	Наименование ПДн	Категория ПДн.	Срок конфиденциальнос	Перечень сотрудников допущенных к ПДн
----------	------------------	----------------	--------------------------	--

			ти	
1.	Фамилия, имя, отчество, день, месяц, год и место рождения	иные	постоянно	Руководство фирмы. Сотрудник ОК
2.	Состояние здоровья сотрудника оператора (СО)	специальные	постоянно	Сотрудники мед пункта фирмы
3.	Паспортные данные сотрудников	иные	постоянно	Сотрудник ОК
4.	Контактная информация сотрудников: номер телефона		постоянно	Сотрудник ОК
5.	Отпечатки пальцев	биометрические	постоянно	Сотрудник ОК
6.				

1.3 Анализ территориального расположения ИС предприятия

На рисунке 3 представлено территориальное расположение ИС предприятия

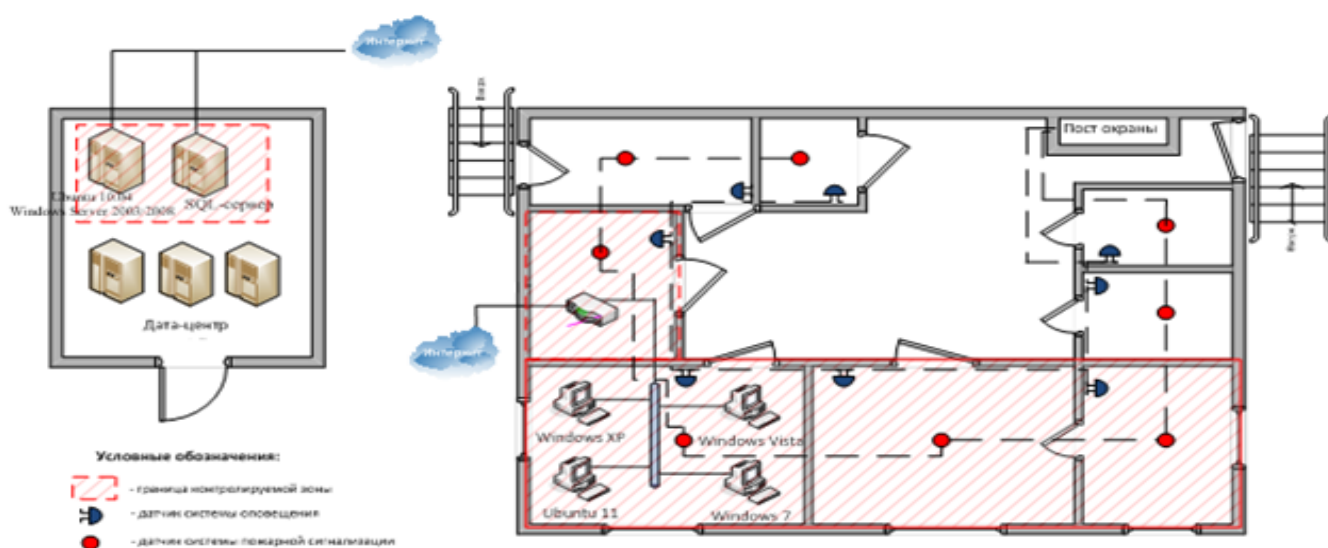


Рисунок 3 - План 2 этажа

4. Оборудование и материалы (перечень используемого оборудования)

Состав раздаточного материала:

- коллекция макетов с конфиденциальными документами;
- коллекция документов для выявления конфиденциальных документов фирмы;
- карточка индивидуального ситуационного варианта к заданиям работы;
- учетные формы;
- рабочая тетрадь;
- перечень конфиденциальных документов (сведений) негосударственной фирмы;
- операционная схема;
- внутренняя опись документов, находящихся у исполнителя (студента);
- практикум.

5. Указания по технике безопасности

- ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории;

- убедиться в целостности электрических розеток и разъемов. В лаборатории необходимо быть в сменной обуви;

- включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

6. Задания

- выполнение операций процедуры приема пакетов;
- составление акта о повреждении или нарушении в оформлении пакета;

- выполнение операций процедуры учета пакетов;
- выполнение операций процедуры распределения и вскрытия пакетов;
- выполнение операций процедуры выделения конфиденциальных документов из документов входного потока.

7. Содержание отчета

По результатам выполнения практического занятия студенты оформляют и защищают в индивидуальном порядке в форме беседы результаты выполнения заданий.

Результатом работы является:

- журнал учёта входящих пакетов;
- журнал учёта входящих документов;
- акты по замечаниям.

8. Контрольные вопросы и тестовые задания

1. Какое назначение имеет стадия приема, первичной обработки, предварительного рассмотрения и распределения поступивших документов?
2. Каким угрозам подвергается документ в процессе его доставки адресату и приема адресатом?
3. Какие задачи защиты информации должны быть решены при выполнении процедур и операций данной стадии?
4. Какое назначение имеет каждая из выполняемых процедур?
5. Как осуществляется прием пакетов от курьеров и из почтового отделения связи?
6. Как осуществляется прием и учет пакетов, поступивших во внерабочее время?
7. Как осуществляется прием пакетов, имеющих повреждения или нарушения в оформлении?
8. Кому и как передаются пакеты, не подлежащие вскрытию?
9. Как проверяется комплектность поступивших документов?
10. Как осуществляется пересылка ошибочно присланных документов?
11. Как происходит выделение документов, содержащих негосударственную тайну, из общего потока открытых документов?

9. Список литературы

Основная литература:

1. Аверченков, В.И. Защита персональных данных в организации [Электронный ресурс] / В.И. Аверченков, М.Ю. Рытов, Т.Р. Гайнулин. - 2-е изд., стер. - М. : Флинта, 2017. - 124 с. - ISBN 978-5-9765-1273-3. - URL: <http://biblioclub.ru/index.php?page=book&id=93260>
2. Минин, И.В. Защита конфиденциальной информации при электронном документообороте: учебное пособие [Электронный ресурс] / И.В. Минин, О.В. Минин. - Новосибирск: НГТУ, 2018. - 20 с. - ISBN 978-5-7782-1829-1. - URL: <http://biblioclub.ru/index.php?page=book&id=228779>

Дополнительная литература:

1. Лузина, Т.В. Основы документооборота в таможенных органах : [16+] / Т.В. Лузина, С.С. Решетникова ; Министерство науки и образования РФ, ФГБОУ ВПО Тюменский государственный университет, Институт дистанционного образования, Институт психологии и др. – Тюмень : Издательство Тюменского государственного университета, 2016. – 524 с. : ил. – Режим доступа: по подписке. – URL: <http://biblioclub.ru/index.php?page=book&id=567333>

Практическое занятие 3 Выбор базового набора организационных и технических мер защиты информации

Тема 3: Доступ персонала к конфиденциальным сведениям

1. Цель занятия.

- приобретение практических навыков анализа информационных систем
- приобретение практических навыков построения системы защиты информации в ИС.

2. Формируемые компетенции или их части

В результате выполнения работы студенты должны:

- уметь использовать нормативные правовые документы при организации подсистемы защищённого конфиденциального делопроизводства;
- владеть технологией организации конфиденциального делопроизводства.

3. Теоретическая часть

2.1 Выбор базового набора мер исходя из класса защищённости ИС

Используя положения приказа №17 ФСТЭК, а также исходные данные (приложение А ЛЗ 1) выбрать базовый набор организационных и технических мер для их реализации в ИС использующей систему электронного документооборота (СЭДО).

Последовательность действий оператора, по выбору организационных и технических мер для их реализации в ИС СЭДО, представлена в таблице 1.

Таблица 1 - Последовательность действий, при выборе организационных и технических мер ЗИ

Стадии работы по построению СЗИ	Содержание работы	Разрабатываемые документы
Определение класса защищённости ИС и уровня значимости (УЗ) персональных данных (ПДн) обрабатываемых в ИС предприятия	Определение уровня значимости информации в ИС, оценка ущерба и определение масштаба ИС. Определение типа угроз для ИС и категории ПДн	Акт классификации ИС
Выбор базового набора мер для определённого класса защищённости ИС	Анализ прил. 2 к Пр ФСТЭК №17	Перечень базового набора мер
Адаптация базового набора мер	Цели и задачи ИС, анализ СФХ и применяемых технологий в ИС	Перечень адаптированного набора мер
Уточнение адаптированного базового набора мер	Модель нарушителя, анализ уязвимостей, сравнение угроз с возможностями нарушителя и базовым набором мер	Уточнённый набор мер
Усиление и дополнение уточнённого адаптированного базового набора мер	Усилить, а при необходимости дополнить уточнённый набор мер. Обосновать применение компенсирующих мер (по необходимости)	Перечень базовых, адаптированных, уточнённых, дополненных и усиленных мер
Выбор технических средств ЗИ (СрЗИ), в соответствии с выбранным классом защиты ИС. Разработка организационных мер защиты	С учетом требований нормативных документов выбираются СрЗИ и разрабатываются организационные мероприятия по ЗИ	Перечень сертифицированных СрЗИ, набор организационно-распорядительных документов
Оценка эффективности СЗИ в составе ИС	Определение значения величины риска ИБ ИС	Количественное значение риска ИБ ИС

2.1.1 Определение класса защищённости информационной системы

Базовый набор мер для ИС организации определяется исходя из класса защищённости ИС. Класс защищённости ИС определяется в зависимости от уровня значимости информации (УЗ), обрабатываемой в этой ИС, и масштаба ИС (федеральный, региональный, объектовый).

Уровень значимости информации определяется степенью возможного ущерба для обладателя информации и (или) оператора от нарушения конфиденциальности, целостности или доступности информации.

Информация имеет высокий уровень значимости (УЗ 1), если определена высокая степень ущерба.

Информация имеет средний уровень значимости (УЗ 2), если определена средняя степень ущерба.

Информация имеет низкий уровень значимости (УЗ 3), если определены низкие степени ущерба.

ИС имеет федеральный масштаб, если она функционирует на территории РФ (в пределах федерального округа).

ИС имеет региональный масштаб, если она функционирует на территории субъекта РФ.

ИС имеет объектовый масштаб, если она функционирует на объектах.

Класс защищённости ИС определяется в соответствии с таблицей 2.

Таблица 2 – Определение класса защищённости ИС

Уровень значимости информации	Масштаб ИС		
	Федеральный	Региональный	Объектовый
УЗ 1	K1	K1	K1
УЗ 2	K1	K2	K2
УЗ 3	K2	K3	K3

В таблице приведён пример определения класса защищённости для варианта с уровнем значимости информации УЗ 2 и регионального масштаба ИС. Из таблицы видно, что итоговый класс защищённости ИС K2.

Базовый набор мер определяется из приложения 2 к Приказу 17 ФСТЭК в соответствии с определённым классом защищённости ИС (фрагмент таблицы 3).

Таблица 3 – Фрагмент таблицы с базовым набором мер для различных КЗ ИС

Условное обозначение и номер меры	Меры защиты информации в информационных системах	Классы защищенности информационной системы		
		3	2	1
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)				
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	+	+	+
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных		+	+
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	+	+	+
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и	+	+	+

	принятие мер в случае утраты и (или) компрометации средств аутентификации			
ИАФ.5	Защита обратной связи при вводе аутентификационной информации	+	+	+

3 Содержание практических заданий и методические указания к их выполнению

Произвести выбор организационных и технических мер для их реализации в СЗИ ИС в соответствии с индивидуальным заданием (таблица 5).

Таблица 5 Фрагмент индивидуального задания

№ вар	Предприятие	Кол-во отделов	Кол-во серверов/ком-ров/маршру-ов	Тип сервера	Кол-во АРМ в отделе	Применяемое ПО	Используемые информационные технологии	Свойства архитектуры ИС	Тип характеристик ИС	Уровень значимости	Масштаб ИС	Потенциал нарушителя	Объект воздействия
1	ЗАО Сигнал	4	2/3/2	Сервер 19-wsus Серверы s19-001	4	Microsoft Windows Server Standard 2008 R2 SP1 Microsoft Windows 7 Professional SP3 Kaspersky Endpoint Security 8 for Windows Kaspersky Endpoint Security 8 for Windows	системы на основе виртуализации системы, реализующие «облачные вычисления» системы с мобильными устройствами	файл-серверные системы центры обработки данных системы с удаленным доступом пользователей;	распределенная ИС ИС, имеющая многоочечный вход в сеть общего пользования ИС, к которой имеют доступ определенные перечнем сотрудник и организации	У 3 1	Федеральный	Внешний нарушитель со средним потенциалом, Внутренний нарушитель с низким потенциалом	Сетевой трафик Метаданные, системное программное обеспечение Микропрограммное и аппаратное обеспечение BIOS/UEFI Прикладное программное обеспечение, сетевое программное обеспечение

4. Оборудование и материалы (перечень используемого оборудования)

Состав раздаточного материала:

- коллекция макетов с конфиденциальными документами;
- коллекция документов для выявления конфиденциальных документов фирмы;
- карточка индивидуального ситуационного варианта к заданиям работы;
- учетные формы;
- рабочая тетрадь;
- перечень конфиденциальных документов (сведений) негосударственной фирмы;
- операционная схема;
- внутренняя опись документов, находящихся у исполнителя (студента);
- практикум.

5. Указания по технике безопасности

- ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в

лаборатории;

- убедиться в целостности электрических розеток и разъемов. В лаборатории необходимо быть в сменной обуви;

- включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

6. Задания

- выполнение операций процедуры приема пакетов;
- составление акта о повреждении или нарушении в оформлении пакета;
- выполнение операций процедуры учета пакетов;
- выполнение операций процедуры распределения и вскрытия пакетов;
- выполнение операций процедуры выделения конфиденциальных документов из документов входного потока.

7. Содержание отчета

По результатам выполнения практического занятия студенты оформляют и защищают в индивидуальном порядке в форме беседы результаты выполнения заданий.

Результатом работы является:

- журнал учёта входящих пакетов;
- журнал учёта входящих документов;
- акты по замечаниям.

8. Контрольные вопросы и тестовые задания

1. Какое назначение имеет стадия приема, первичной обработки, предварительного рассмотрения и распределения поступивших документов?

2. Каким угрозам подвергается документ в процессе его доставки адресату и приема адресатом?

3. Какие задачи защиты информации должны быть решены при выполнении процедур и операций данной стадии?

4. Какое назначение имеет каждая из выполняемых процедур?

5. Как осуществляется прием пакетов от курьеров и из почтового отделения связи?

6. Как осуществляется прием и учет пакетов, поступивших во внерабочее время?

7. Как осуществляется прием пакетов, имеющих повреждения или нарушения в оформлении?

8. Кому и как передаются пакеты, не подлежащие вскрытию?

9. Как проверяется комплектность поступивших документов?

10. Как осуществляется пересылка ошибочно присланных документов?

11. Как происходит выделение документов, содержащих негосударственную тайну, из общего потока открытых документов?

9. Список литературы

Основная литература:

1. Аверченков, В.И. Защита персональных данных в организации [Электронный ресурс] / В.И. Аверченков, М.Ю. Рытов, Т.Р. Гайнулин. - 2-е изд., стер. - М. : Флинта, 2017. - 124 с. - ISBN 978-5-9765-1273-3. - URL: <http://biblioclub.ru/index.php?page=book&id=93260>

2. Минин, И.В. Защита конфиденциальной информации при электронном документообороте: учебное пособие [Электронный ресурс] / И.В. Минин, О.В. Минин. - Новосибирск: НГТУ, 2018. - 20 с. - ISBN 978-5-7782-1829-1. - URL: <http://biblioclub.ru/index.php?page=book&id=228779>

Дополнительная литература:

1. Лузина, Т.В. Основы документооборота в таможенных органах : [16+] / Т.В. Лузина, С.С. Решетникова ; Министерство науки и образования РФ, ФГБОУ ВПО Тюменский

государственный университет, Институт дистанционного образования, Институт психологии и др. – Тюмень : Издательство Тюменского государственного университета, 2016. – 524 с. : ил. – Режим доступа: по подписке. – URL: <http://biblioclub.ru/index.php?page=book&id=567333>

4 Содержание практических заданий и методические указания к их выполнению

Произвести выбор организационных и технических мер для их реализации в СЗИ ИС в соответствии с индивидуальным заданием (таблица 5).

Таблица 5 Фрагмент индивидуального задания

№ вар	Предприятие	Кол-во отделов	Кол-во серверов/ком-ров/маршрутизаторов	Тип сервера	Кол-во АРМ в отделе	Применяемое ПО	Используемые информационные технологии	Свойства архитектуры ИС	Тип характеристик ИС	Уровень значимости	Масштаб ИС	Потенциал нарушителя	Объект воздействия
2	ЗАО Сигнал	4	2/3/2	Сервер 19-wsus Серверы s19-001	4	Microsoft Windows Server Standard 2008 R2 SP1 Microsoft Windows 7 Professional SP3 Kaspersky Endpoint Security 8 for Windows Kaspersky Endpoint Security 8 for Windows	системы на основе виртуализации системы, реализующие «облачные вычисления» системы с мобильными устройствами	файл-серверные системы центры обработки данных системы с удаленным доступом пользователей;	распределенная ИС	У 3 1	Федеральный	Внешний нарушитель со средним потенциалом, Внутренний нарушитель с низким потенциалом	Сетевой трафик
									ИС, имеющая многоочечный вход в сеть общего пользования				Метаданные, системное программное обеспечение
									ИС, к которой имеют доступ определенные перечнем сотрудники и организации				Микропрограммное и аппаратное обеспечение BIOS/UEFI
													Прикладное программное обеспечение, сетевое программное обеспечение

10. Оборудование и материалы (перечень используемого оборудования)

Состав раздаточного материала:

- коллекция макетов с конфиденциальными документами;
- коллекция документов для выявления конфиденциальных документов фирмы;
- карточка индивидуального ситуационного варианта к заданиям работы;
- учетные формы;
- рабочая тетрадь;
- перечень конфиденциальных документов (сведений) негосударственной фирмы;
- операционная схема;
- внутренняя опись документов, находящихся у исполнителя (студента);
- практикум.

11. Указания по технике безопасности

- ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в

лаборатории;

- убедиться в целостности электрических розеток и разъемов. В лаборатории необходимо быть в сменной обуви;

- включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

12. Задания

- выполнение операций процедуры приема пакетов;
- составление акта о повреждении или нарушении в оформлении пакета;
- выполнение операций процедуры учета пакетов;
- выполнение операций процедуры распределения и вскрытия пакетов;
- выполнение операций процедуры выделения конфиденциальных документов из документов входного потока.

13. Содержание отчета

По результатам выполнения практического занятия студенты оформляют и защищают в индивидуальном порядке в форме беседы результаты выполнения заданий.

Результатом работы является:

- журнал учёта входящих пакетов;
- журнал учёта входящих документов;
- акты по замечаниям.

14. Контрольные вопросы и тестовые задания

1. Какое назначение имеет стадия приема, первичной обработки, предварительного рассмотрения и распределения поступивших документов?

2. Каким угрозам подвергается документ в процессе его доставки адресату и приема адресатом?

3. Какие задачи защиты информации должны быть решены при выполнении процедур и операций данной стадии?

4. Какое назначение имеет каждая из выполняемых процедур?

5. Как осуществляется прием пакетов от курьеров и из почтового отделения связи?

6. Как осуществляется прием и учет пакетов, поступивших во внерабочее время?

7. Как осуществляется прием пакетов, имеющих повреждения или нарушения в оформлении?

8. Кому и как передаются пакеты, не подлежащие вскрытию?

9. Как проверяется комплектность поступивших документов?

10. Как осуществляется пересылка ошибочно присланных документов?

11. Как происходит выделение документов, содержащих негосударственную тайну, из общего потока открытых документов?

15. Список литературы

Основная литература:

1. Аверченков, В.И. Защита персональных данных в организации [Электронный ресурс] / В.И. Аверченков, М.Ю. Рытов, Т.Р. Гайнулин. - 2-е изд., стер. - М. : Флинта, 2017. - 124 с. - ISBN 978-5-9765-1273-3. - URL: <http://biblioclub.ru/index.php?page=book&id=93260>

2. Минин, И.В. Защита конфиденциальной информации при электронном документообороте: учебное пособие [Электронный ресурс] / И.В. Минин, О.В. Минин. - Новосибирск: НГТУ, 2018. - 20 с. - ISBN 978-5-7782-1829-1. - URL: <http://biblioclub.ru/index.php?page=book&id=228779>

Дополнительная литература:

1. Лузина, Т.В. Основы документооборота в таможенных органах : [16+] / Т.В. Лузина, С.С. Решетникова ; Министерство науки и образования РФ, ФГБОУ ВПО Тюменский

государственный университет, Институт дистанционного образования, Институт психологии и др. – Тюмень : Издательство Тюменского государственного университета, 2016. – 524 с. : ил. – Режим доступа: по подписке. – URL: <http://biblioclub.ru/index.php?page=book&id=567333>

Практическое занятие 4,5 Адаптация базового набора организационных и технических мер ЗИ.

Тема 4-5: Порядок организации защищённого электронного документооборота на предприятии. Порядок настройки систем электронного документооборота на структуру организации

1. Цель занятия:

- приобретение практических навыков анализа информационных систем
- приобретение практических навыков построения системы защиты информации в ИС.

2. Формируемые компетенции или их части

В результате выполнения работы студенты должны:

- уметь использовать нормативные правовые документы при организации подсистемы защищённого конфиденциального делопроизводства;
- владеть технологией организации конфиденциального делопроизводства.

3. Теоретическая часть

В соответствии с алгоритмом работы по построению СЗИ ИС, необходимо определить адаптированный набор мер (таблица 1).

Таблица 1- Фрагмент алгоритма работы оператора по выбору организационных и технических мер защиты информации в ИС

Стадии работы по построению СЗИ	Содержание работы	Разрабатываемые документы
Адаптация базового набора мер	Цели и задачи ИС, анализ СФХ и применяемых технологий в ИС	Перечень адаптированного набора мер

При адаптации базового набора мер защиты информации учитываются:

- цели (обеспечение конфиденциальности, целостности и (или) доступности информации) и задачи защиты информации в информационной системе;
- перечень мероприятий, проводимых оператором по обеспечению безопасности в рамках организации в целом;
- применяемые информационные технологии и структурно-функциональные характеристики (СФХ) информационной системы.

Адаптация базового набора мер ЗИ предусматривает исключение мер, не связанных с информационными технологиями, не используемыми в ИС, или СФХ, не свойственными ИС.

В таблице 2 представлен полный набор СФХ ИС. Анализируем только те СФХ, которые в Вашем варианте.

Таблица 2 – Анализ структурно–функциональных характеристик ИС

Анализируемые СФХ ИС	Возможные варианты
структура информационной системы	автономное автоматизированное рабочее место
	локальная информационная система
	распределенная информационная система
технологии, применяемые в составе системы	грид–вычисления
	виртуализация

Анализируемые СФХ ИС	Возможные варианты
	беспроводной доступ
	веб–приложения
	облачные технологии
	суперкомпьютеры
	технологии big data
	автоматизация технологических процессов
	мобильные устройства
свойства архитектуры	система на основе тонкого клиента
	система на основе одноранговой сети
	файл–серверная система
	ЦОД
	система с удаленным доступом пользователей
	система с разными типами операционных систем
	система с прикладными программами, независимыми от ОС
	система, использующая выделенные каналы связи
взаимодействие с внешними системами	взаимодействует
	не взаимодействует
подключение к сети	подключена
	не подключена (полностью изолированная)
подключение к сети общего пользования	подключена
	подключена через выделенную инфраструктуру (gov.ru или иную)
	не подключена
размещение компонентов системы по отношению к контролируемой зоне	в пределах одной контролируемой зоны
	в пределах нескольких контролируемых зон
	вне контролируемой зоны
режим обработки информации в системе	однопользовательский
	многопользовательский
разграничение прав доступа к системе	не разграничиваются
	разграничиваются
разделение функций по управлению информационной системой	не разделены
	рабочие места для администрирования выделены в отдельный домен
	для администрирования используются отдельные сетевые адреса
	для администрирования используются выделенные каналы связи
сегментирование ИС	сегментирована
	не сегментирована
источники угроз (нарушитель, обладающий мотивацией для атаки системы)	внешние субъекты (физические лица)
	бывшие работники
	административный, обслуживающий персонал, охрана

Анализируемые СФХ ИС	Возможные варианты
	лица, привлекаемые для установки, наладки, монтажа, пуско-наладочных и иных работ
	пользователи информационной системы
	администраторы информационной системы и администраторы безопасности
	террористические, экстремистские группировки
	преступные группы (криминальные структуры)
	конкурирующие организации
	разработчики, производители, поставщики ПО и технических средств
	специальные службы иностранных государств

Таким образом, из базового набора мер можно исключить меры, которые уже реализованы в данной ИС и меры не актуальные для рассматриваемой ИС исходя из её СФХ.

В качестве примера адаптации можно рассмотреть исключение из базового набора мер защиты информации мер по защите среды виртуализации, в случае если в информационной системе не применяется технология виртуализации, или исключение из базового набора мер защиты информации мер по защите мобильных технических средств, если такие мобильные устройства не применяются или их применение запрещено.

Результаты анализа вносим в таблицу 3.

Таблица 3 - Основания для исключения/добавления/ мер базового набора по обеспечению безопасности ИС

Номер	Описание меры	Основание для исключения
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа	В рассматриваемой ИС не предполагается использование технологий беспроводного доступа
ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации	В рассматриваемой ИС не предполагается использование среды виртуализации
....		
...		...

4. Оборудование и материалы (перечень используемого оборудования)

Состав раздаточного материала:

- коллекция макетов с конфиденциальными документами;
- коллекция документов для выявления конфиденциальных документов фирмы;
- карточка индивидуального ситуационного варианта к заданиям работы;
- учетные формы;
- рабочая тетрадь;

- перечень конфиденциальных документов (сведений) негосударственной фирмы;
- операционная схема;
- внутренняя опись документов, находящихся у исполнителя (студента);
- практикум.

5. Указания по технике безопасности

- ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории;

- убедиться в целостности электрических розеток и разъемов. В лаборатории необходимо быть в сменной обуви;

- включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

6. Задания

- выполнение операций процедуры приема пакетов;
- составление акта о повреждении или нарушении в оформлении пакета;
- выполнение операций процедуры учета пакетов;
- выполнение операций процедуры распределения и вскрытия пакетов;
- выполнение операций процедуры выделения конфиденциальных документов из документов входного потока.

7. Содержание отчета

По результатам выполнения практического занятия студенты оформляют и защищают в индивидуальном порядке в форме беседы результаты выполнения заданий.

Результатом работы является:

- журнал учёта входящих пакетов;
- журнал учёта входящих документов;
- акты по замечаниям.

8. Контрольные вопросы и тестовые задания

1. Какое назначение имеет стадия приема, первичной обработки, предварительного рассмотрения и распределения поступивших документов?

2. Каким угрозам подвергается документ в процессе его доставки адресату и приема адресатом?

3. Какие задачи защиты информации должны быть решены при выполнении процедур и операций данной стадии?

4. Какое назначение имеет каждая из выполняемых процедур?

5. Как осуществляется прием пакетов от курьеров и из почтового отделения связи?

6. Как осуществляется прием и учет пакетов, поступивших во внерабочее время?

7. Как осуществляется прием пакетов, имеющих повреждения или нарушения в оформлении?

8. Кому и как передаются пакеты, не подлежащие вскрытию?

9. Как проверяется комплектность поступивших документов?

10. Как осуществляется пересылка ошибочно присланных документов?

11. Как происходит выделение документов, содержащих негосударственную тайну, из общего потока открытых документов?

9. Список литературы

Основная литература:

1. Аверченков, В.И. Защита персональных данных в организации [Электронный ресурс] / В.И. Аверченков, М.Ю. Рытов, Т.Р. Гайнулин. - 2-е изд., стер. - М. : Флинта, 2017. - 124 с. - ISBN 978-5-9765-1273-3. - URL: <http://biblioclub.ru/index.php?page=book&id=93260>

2. Минин, И.В. Защита конфиденциальной информации при электронном документообороте: учебное пособие [Электронный ресурс] / И.В. Минин, О.В. Минин. - Новосибирск: НГТУ, 2018. - 20 с. - ISBN 978-5-7782-1829-1. - URL: <http://biblioclub.ru/index.php?page=book&id=228779>

Дополнительная литература:

1. Лузина, Т.В. Основы документооборота в таможенных органах : [16+] / Т.В. Лузина, С.С. Решетникова ; Министерство науки и образования РФ, ФГБОУ ВПО Тюменский государственный университет, Институт дистанционного образования, Институт психологии и др. – Тюмень : Издательство Тюменского государственного университета, 2016. – 524 с. : ил. – Режим доступа: по подписке. – URL: <http://biblioclub.ru/index.php?page=book&id=567333>

Практическое занятие 6,7 Уточнение базового набора организационных и технических мер ЗИ. Построение модели угроз для ИС организации

Тема 6-7: Современные электронные системы управления и работы с документами. Порядок защиты информации в систем электронного документооборота «Дело»

1. Цель занятия:

- приобретение практических навыков анализа информационных систем
- приобретение практических навыков построения системы защиты информации в ИС.

1. Формируемые компетенции или их части

В результате выполнения работы студенты должны:

- уметь использовать нормативные правовые документы при организации подсистемы защищённого конфиденциального делопроизводства;
- владеть технологией организации конфиденциального делопроизводства.

2. Теоретическая часть

В соответствии с алгоритмом работы по построению СЗИ ИС, необходимо определить уточненный адаптированный набор мер (таблица 1).

Таблица 1- Фрагмент алгоритма работы оператора по выбору организационных и технических мер защиты информации в ИС

Стадии работы по построению СЗИ	Содержание работы	Разрабатываемые документы
Уточнение адаптированного базового набора мер	Модель угроз, модель нарушителя, определение актуальных угроз, анализ уязвимостей, сравнение угроз с возможностями нарушителя и адаптированным набором мер	Уточнённый набор мер

Сутью процедуры уточнения является исключение из адаптированного набора тех мер, которые не соответствуют актуальным угрозам для данной ИС.

Исходными данными, при уточнении адаптированного базового набора мер ЗИ, являются: перечень угроз безопасности информации и их характеристики (банк угроз ФСТЭК), частная модель угроз безопасности информации, потенциал, оснащенность, мотивация актуального нарушителя, выявленные уязвимости ИС.

Перечень актуальных угроз определяется на основании частной модели угроз, которая, в соответствии с МД ФСТЭК «Методика оценки угроз безопасности информации» от 05.02.202, должна содержать следующие разделы (таблица 2).

Таблица 2 – Содержание частной модели угроз

Разделы МУ	Содержание
Общие положения	назначение и область действия документа, нормативные документы, используемые для разработки модели угроз, наименование обладателя информации, подразделения, должностные лица, ответственные за обеспечение защиты информации (безопасности) систем и сетей
Описание систем и сетей и их характеристика как объектов защиты	наименование систем и сетей, для которых разработана МУ, уровень защищенности персональных данных, назначение, задачи систем и сетей, состав обрабатываемой информации и ее правовой режим
Возможные негативные последствия от реализации угроз	описание видов рисков (ущербов), актуальных для обладателя информации, оператора, которые могут наступить от нарушения или прекращения основных процессов

Разделы МУ	Содержание
Возможные объекты воздействия угроз безопасности информации	наименования и назначение компонентов систем и сетей, которые непосредственно участвуют в обработке и хранении защищаемой информации, или обеспечивают реализацию основных процессов обладателя информации, оператора
Источники угроз безопасности информации (модель нарушителя)	характеристику нарушителей, которые могут являться источниками угроз безопасности информации, и возможные цели реализации ими угроз безопасности информации, категории актуальных нарушителей, которые могут являться источниками угроз безопасности информации
Способы реализации (возникновения) угроз безопасности информации	описание способов реализации (возникновения) угроз безопасности информации, которые могут быть использованы нарушителями разных видов и категорий
Актуальные угрозы безопасности информации	перечень возможных (вероятных) угроз безопасности информации для соответствующих способов их реализации и уровней возможностей нарушителей, описание возможных сценариев реализации угроз безопасности информации, выводы об актуальности угроз безопасности информации.

Фрагмент банка угроз ФСТЭК представлен в таблице 3.

Таблица 3 - Фрагмент банка угроз ФСТЭК

Общая информация					Последствия			
Идентификатор УБИ	Наименование УБИ	Описание	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Нарушение конфиденциальности	Нарушение целостности	Нарушение доступности	Дата последнего изменения данных
1	Угроза автоматического распространения вредоносного кода в грид-системе	Угроза заключается в возможности внедрения и запуска вредоносного кода от имени доверенного процесса на любом из ресурсных центров грид-системы и его автоматического распространения на все узлы грид-системы. Данная угроза обусловлена слабостями технологии грид-вычислений – высоким уровнем автоматизации при малой администрируемости грид-системы. Реализация данной угрозы возможна при условии наличия у нарушителя привилегий легального пользователя грид-системы	Внешний нарушитель со средним потенциалом; Внутренний нарушитель со средним потенциалом	Ресурсные центры грид-системы	1	1	1	08.02.2019
2	Угроза агрегирования данных, передаваемых в грид-системе	Угроза заключается в возможности раскрытия нарушителем защищаемой информации путём выявления задействованных в её обработке узлов, сбора, анализа и обобщения данных, перехватываемых в сети передачи данных грид-системы. Данная угроза обусловлена слабостью технологии грид-вычислений – использованием незащищённых каналов сети Интернет как транспортной сети грид-системы. Реализация данной угрозы возможна при условии наличия у нарушителя: сил и средств, достаточных для компенсации чрезвычайной распределённости грид-заданий между узлами грид-системы; привилегий, достаточных для перехвата трафика сети передачи данных между элементами (узлами) грид-системы	Внешний нарушитель со средним потенциалом	Сетевой трафик	1	0	0	08.02.2019
3	Угроза использования слабостей криптографических алгоритмов и уязвимостей в программном обеспечении их реализации	Угроза заключается в возможности выявления слабых мест в криптографических алгоритмах или уязвимостей в реализующем их программном обеспечении. Данная угроза обусловлена слабостями криптографических алгоритмов, а также ошибками в программном коде криптографических средств, их сопряжении с системой или параметрах их настройки. Реализация угрозы возможна в случае наличия у нарушителя сведений об применяемых в системе средствах шифрования, реализованных в них алгоритмах шифрования и параметрах их настройки	Внешний нарушитель со средним потенциалом; Внутренний нарушитель со средним потенциалом	Метаданные, системное программное обеспечение	1	1	0	29.11.2020
4	Угроза аппаратного сброса	Угроза заключается в возможности сброса паролей, установленных в BIOS/UEFI без прохождения процедуры авторизации в системе путём обесточивания микросхемы BIOS (съёма аккумулятора) или установки перемычки в штатном месте на системной плате (переключение «джампера»). Данная угроза обусловлена уязвимостями некоторых системных (материнских) плат – наличием механизмов аппаратного сброса паролей, установленных в BIOS/UEFI.	Внутренний нарушитель с низким	Микропрограммное и аппаратное обеспечение	0	1	0	08.02.2019

Уточнение адаптированного базового набора мер защиты информации проводится с учетом результатов оценки возможности адаптированного базового набора мер защиты информации адекватно блокировать (нейтрализовать) все актуальные угрозы безопасности информации, включенные в модель угроз безопасности информации, или снизить

вероятность их реализации исходя из условий функционирования информационной системы.
По результатам работы составляется перечень актуальных угроз (таблица 4)

Таблица 4- Перечень актуальных угроз безопасности ИС

Идентификатор УБИ	Описание угрозы
3	Угроза использования слабостей криптографических алгоритмов и уязвимостей в программном обеспечении их реализации
10	Угроза выхода процесса за пределы виртуальной машины
....	
...	

При уточнении адаптированного базового набора мер ЗИ для каждой актуальной угрозы безопасности информации, сопоставляется мера ЗИ из адаптированного базового набора мер (таблица 5). Лишние меры исключаются.

Таблица 5 - Соответствие мер угрозам безопасности информации

Угроза безопасности информации	Меры
УБИ.6	ОПС.3; РСБ.1; РСБ.4; РСБ.5; АВЗ.1; АВЗ.2; АНЗ.1; АНЗ.2; АНЗ.3; АНЗ.4; ОЦЛ.3;
УБИ.8	ЗНИ.8; РСБ.1; РСБ.3; АНЗ.1; ЗТС.3; ЗТС.4
УБИ.15	ИАФ.1; УПД.2; АНЗ.3; АНЗ.5
УБИ.17	ЗИС.3; АНЗ.1; АВЗ.1; АВЗ.2; АНЗ.3
УБИ.19	РСБ.4; РСБ.5; ЗИС.3; ЗИС.20; ЗИС.30
УБИ.23	ИАФ.1; ИАФ.4; ИАФ.5; УПД.2; ОЦЛ.3
УБИ.28	ИАФ.1; ИАФ.4; ИАФ.5; УПД.2; ОЦЛ.3
УБИ.30	ИАФ.3; ИАФ.4; УПД.1; ЗНИ.2; ЗНИ.8; ОЦЛ.3; ЗТС.3
УБИ.31	УПД.2; УПД.4
УБИ.34	УПД.3
УБИ.49	РСБ.1; РСБ.2; РСБ.4; АВЗ.1; АВЗ.2; АНЗ.1; АНЗ.3; ОЦЛ.3
УБИ.62	АВЗ.1; АВЗ.2; АНЗ.1; АНЗ.3
УБИ.67	ЗТС.2; ЗТС.3; ЗТС.4
УБИ.69	УПД.3; УПД.13; УПД.14; РСБ.1; РСБ.4; АНЗ.2; ЗИС.3; ЗИС.20
УБИ.71	ЗНИ.8
УБИ.74	ИАФ.3; ИАФ.4; ИАФ.5; УПД.2; УПД.13
УБИ.86	ИАФ.3; ИАФ.4; ИАФ.5; УПД.2; УПД.13
УБИ.88	ИАФ.3; ИАФ.4; ИАФ.5; УПД.2; УПД.13; ЗТС.3; ЗТС.4
УБИ.89	ОПС.3; РСБ.1; РСБ.3; РСБ.4; АВЗ.1; АВЗ.2; АНЗ.2; АНЗ.3

УБИ.90	ИАФ.3; ИАФ.4; ИАФ.5; УПД.2; УПД.13
УБИ.91	ИАФ.3; ИАФ.4; ИАФ.5; УПД.2; УПД.13
УБИ.98	УПД.3; АНЗ.3; АНЗ.4; ЗТС.3
УБИ.99	УПД.3; АНЗ.3; АНЗ.4; ЗТС.3
УБИ.100	ИАФ.4; ИАФ.5; УПД.2; УПД.6; УПД.10
УБИ.103	УПД.3
УБИ.104	УПД.3
УБИ.116	УПД.3;
УБИ.121	УПД.4; УПД.5; АНЗ.3
УБИ.124	РСБ.3; РСБ.4; РСБ.5; РСБ.7
УБИ.128	ЗНИ.2; ЗНИ.1; УПД.3
УБИ.145	УПД.3; УПД.4; УПД.5; ОПС.3; АВЗ.1; АНЗ.2; АНЗ.3
УБИ.152	ИАФ.4; ИАФ.5; УПД.2; УПД.1; УПД.4; УПД.5
УБИ.153	УПД.3
УБИ.155	УПД.3
УБИ.156	ЗТС.3; АНЗ.4
УБИ.157	ЗТС.3; АНЗ.4
УБИ.158	ОЦЛ.3
УБИ.160	ЗТС.2; ЗТС.3
УБИ.167	АВЗ.1; АВЗ.2
УБИ.168	УПД.3
УБИ.170	АВЗ.1; АВЗ.2; ОЦЛ.3
УБИ.171	АВЗ.1; АВЗ.2
УБИ.172	АВЗ.1; АВЗ.2
УБИ.174	УПД.3; АВЗ.1; АВЗ.2; АНЗ.5
УБИ.175	УПД.3; АВЗ.1; АВЗ.2; АНЗ.5
УБИ.176	АНЗ.3; РСБ.4
УБИ.178	УПД.5; РСБ.3; РСБ.4; РСБ.5; АНЗ.2; АНЗ.3
УБИ.179	УПД.5; РСБ.3; РСБ.4; РСБ.5; АНЗ.2; АНЗ.3
УБИ.182	АНЗ.4
УБИ.185	УПД.5; РСБ.3; РСБ.4; РСБ.5; АНЗ.2; АНЗ.3
УБИ.186	АВЗ.1; АВЗ.2
УБИ.192	АНЗ.2

3. Оборудование и материалы (перечень используемого оборудования)

Состав раздаточного материала:

- коллекция макетов с конфиденциальными документами;
- коллекция документов для выявления конфиденциальных документов фирмы;
- карточка индивидуального ситуационного варианта к заданиям работы;
- учетные формы;
- рабочая тетрадь;
- перечень конфиденциальных документов (сведений) негосударственной фирмы;

- операционная схема;
- внутренняя опись документов, находящихся у исполнителя (студента);
- практикум.

4. Указания по технике безопасности

- ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории;
- убедиться в целостности электрических розеток и разъемов. В лаборатории необходимо быть в сменной обуви;
- включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

5. Задания

- выполнение операций процедуры приема пакетов;
- составление акта о повреждении или нарушении в оформлении пакета;
- выполнение операций процедуры учета пакетов;
- выполнение операций процедуры распределения и вскрытия пакетов;
- выполнение операций процедуры выделения конфиденциальных документов из документов входного потока.

6. Содержание отчета

По результатам выполнения практического занятия студенты оформляют и защищают в индивидуальном порядке в форме беседы результаты выполнения заданий.

Результатом работы является:

- журнал учёта входящих пакетов;
- журнал учёта входящих документов;
- акты по замечаниям.

7. Контрольные вопросы и тестовые задания

1. Какое назначение имеет стадия приема, первичной обработки, предварительного рассмотрения и распределения поступивших документов?
2. Каким угрозам подвергается документ в процессе его доставки адресату и приема адресатом?
3. Какие задачи защиты информации должны быть решены при выполнении процедур и операций данной стадии?
4. Какое назначение имеет каждая из выполняемых процедур?
5. Как осуществляется прием пакетов от курьеров и из почтового отделения связи?
6. Как осуществляется прием и учет пакетов, поступивших во внерабочее время?
7. Как осуществляется прием пакетов, имеющих повреждения или нарушения в оформлении?
8. Кому и как передаются пакеты, не подлежащие вскрытию?
9. Как проверяется комплектность поступивших документов?
10. Как осуществляется пересылка ошибочно присланных документов?
11. Как происходит выделение документов, содержащих негосударственную тайну, из общего потока открытых документов?

8. Список литературы

Основная литература:

1. Аверченков, В.И. Защита персональных данных в организации [Электронный ресурс] / В.И. Аверченков, М.Ю. Рытов, Т.Р. Гайнулин. - 2-е изд., стер. - М. : Флинта, 2017. - 124 с. - ISBN 978-5-9765-1273-3. - URL: <http://biblioclub.ru/index.php?page=book&id=93260>

2. Минин, И.В. Защита конфиденциальной информации при электронном документообороте: учебное пособие [Электронный ресурс] / И.В. Минин, О.В. Минин. - Новосибирск: НГТУ, 2018. - 20 с. - ISBN 978-5-7782-1829-1. - URL:<http://biblioclub.ru/index.php?page=book&id=228779>

Дополнительная литература:

1. Лузина, Т.В. Основы документооборота в таможенных органах : [16+] / Т.В. Лузина, С.С. Решетникова ; Министерство науки и образования РФ, ФГБОУ ВПО Тюменский государственный университет, Институт дистанционного образования, Институт психологии и др. – Тюмень : Издательство Тюменского государственного университета, 2016. – 524 с. : ил. – Режим доступа: по подписке. – URL: <http://biblioclub.ru/index.php?page=book&id=567333>

Практическое занятие 8,9 Выбор технических средств для реализации выбранных технических мер защиты информации в ИС организации

Тема 8-9 Анализ требований нормативно-методических документов по организации построения системы защиты информации (СЗИ) в ИС организации. Предпроектный анализ информационной системы организации

1. Цель занятия:

- приобретение практических навыков анализа информационных систем
- приобретение практических навыков построения системы защиты информации в ИС.

2. Формируемые компетенции или их части

В результате выполнения работы студенты должны:

- уметь использовать нормативные правовые документы при организации подсистемы защищённого конфиденциального делопроизводства;
- владеть технологией организации конфиденциального делопроизводства.

3. Теоретическая часть

В зависимости от класса защищенности ИС минимальные требования к реализации, уточненной адаптированной базовой меры ЗИ подлежат усилению для повышения уровня защищенности информации:

Пример:

ИАФ.1 ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ, ЯВЛЯЮЩИХСЯ РАБОТНИКАМИ ОПЕРАТОРА

Требования к реализации ИАФ.1: В ИС должна обеспечиваться идентификация и аутентификация пользователей, являющихся работниками оператора.

При доступе в ИС должна осуществляться идентификация и аутентификация пользователей, являющихся работниками оператора (внутренних пользователей), и процессов, запускаемых от имени этих пользователей, а также процессов, запускаемых от имени системных учетных записей.

Аутентификация пользователя осуществляется с использованием паролей, аппаратных средств, биометрических характеристик, иных средств или в случае многофакторной (двухфакторной) аутентификации - определенной комбинации указанных средств.

В ИС должна быть обеспечена возможность однозначного сопоставления идентификатора пользователя с запускаемыми от его имени процессами.

Правила и процедуры идентификации и аутентификации пользователей регламентируются в организационно-распорядительных документах по защите информации.

Требования к усилению ИАФ.1:

1) в ИС должна обеспечиваться многофакторная (двухфакторная) аутентификация для удаленного доступа в систему с правами привилегированных учетных записей (администраторов):

- а) с использованием сети связи общего пользования, в том числе сети Интернет;
- б) без использования сети связи общего пользования;

2) в ИС должна обеспечиваться многофакторная (двухфакторная) аутентификация для удаленного доступа в систему с правами непривилегированных учетных записей (пользователей):

- а) с использованием сети связи общего пользования, в том числе сети Интернет;

- б) без использования сети связи общего пользования;
- 3) в ИС должна обеспечиваться многофакторная (двухфакторная) аутентификация для локального доступа в систему с правами привилегированных учетных записей (администраторов);
- 4) в ИС должна обеспечиваться многофакторная (двухфакторная) аутентификация для локального доступа в систему с правами непривилегированных учетных записей (пользователей);
- 5) в ИС должна обеспечиваться многофакторная (двухфакторная) аутентификация при доступе в систему с правами привилегированных учетных записей (администраторов), где один из факторов обеспечивается аппаратным устройством аутентификации, отделенным от ИС, к которой осуществляется доступ;
- 6) в ИС должна обеспечиваться многофакторная (двухфакторная) аутентификация при доступе в систему с правами непривилегированных учетных записей (пользователей), где один из факторов обеспечивается устройством, отделенным от ИС, к которой осуществляется доступ;
- 7) в ИС должен использоваться механизм одноразовых паролей при аутентификации пользователей, осуществляющих удаленный или локальный доступ;
- 8) в ИС для аутентификации пользователей должно обеспечиваться применение в соответствии с законодательством РФ криптографических методов ЗИ.

Содержание базовой меры ИАФ.1:

Мера защиты информации	Класс защищенности ИС			
	4	3	2	1
ИАФ.1	+	+	+	+
Усиление ИАФ.1			1а, 2а, 3	1а, 2а, 3, 4

1.2 Дополнение уточнённых мер

Дополнение уточненного адаптированного базового набора мер ЗИ осуществляется с целью выполнения требований о ЗИ, установленных иными нормативными правовыми актами в области ЗИ, в том числе в области защиты персональных данных.

Дополнение уточненного адаптированного базового набора мер ЗИ может потребоваться в следующих случаях:

а) если федеральным законом, указом Президента РФ, постановлением Правительства РФ, нормативными актами органа государственной власти, органа местного самоуправления или организации, определяющими порядок создания и эксплуатации ИС, устанавливаются дополнительные требования к ЗИ, выполнение которых не предусмотрено Требованиями Пр.17;

б) политиками обеспечения ИБ обладателя информации (заказчика), оператора и уполномоченного лица, разработанными по ГОСТ Р ИСО/МЭК 27001 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования», предъявлены дополнительные требования к защите информации в ИС.

При дополнении уточненного адаптированного базового набора мер ЗИ возможны следующие действия:

1) может быть обосновано, что меры ЗИ, включенные в уточненный адаптированный базовый набор мер ЗИ, достаточны для выполнения дополнительных требований,

установленных ФЗ , указом Президента РФ, постановлением Правительства РФ, нормативными актами органа государственной власти, органа местного самоуправления или организации. В этом случае дополнение уточненного адаптированного базового набора мер ЗИ не требуется;

2) могут быть усилены (ужесточены) требования к некоторым мерам ЗИ, ранее включенным в уточненный адаптированный базовый набор мер ЗИ, до уровня, обеспечивающего выполнение дополнительных требований, установленных федеральным законом, указом Президента РФ, постановлением Правительства РФ, нормативными актами органа государственной власти, органа местного самоуправления или организации;

3) может быть дополнен уточненный адаптированный базовый набор мер ЗИ мерами ЗИ для выполнения дополнительных требований, установленных федеральным законом, указом Президента РФ, постановлением Правительства Российской Федерации, нормативными актами органа государственной власти, органа местного самоуправления или организации в случае, если такие меры не установлены Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных ИС, утвержденных приказом ФСТЭК России от 11 февраля 2013 г. No17.

2 Выбор технических средств и реализация организационных мер

2.1 выбор технических средств

Технические средства для реализации технических мер выбираются с учётом требований по сертификации технических средств (ТСр) ЗИ и класса защищённости ИС (таблица 1).

Таблицу 1 – Порядок выбора технических средств

№ п.п	Мера	Техническое средство
1.	Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)	Aladdin SAM АПКШ Континент ПАК VipNet TrustAccess Imperva SecureSphere Встроенные средства ОС и ППО
2.	Управление доступом субъектов доступа к объектам доступа (УПД)	СЗИ от НСД SecretNet ПАК Соболь Oracle IAMS АПКШ Континент ПАК VipNet TrustAccess Imperva SecureSphere Встроенные средства ОС и ППО
3.	Ограничение программной среды (ОПС)	СЗИ от НСД SecretNet Код безопасности: Инвентаризации
4.	Защита машинных носителей информации (ЗНИ)	СЗИ от НСД SecretNet
5.	Регистрация событий безопасности (РСБ)	HP ArcSight McAfee SIEM Встроенные механизмы СЗИ
6.	Антивирусная защита (АВЗ)	Антивирус Касперского McAfee Antivirus Security Studio Endpoint Protection TrendMicro Deep Security

7.	Обнаружение (предотвращение) вторжений (COB)	Детектор атак «Континент» Palo Alto StoneGate CheckPoint Imperva SecureSphere Антивирусные средства с функциями COB
8.	Контроль (анализ) защищенности информации (АНЗ)	MaxPatrol / xSpider Комплексный аудит ГИС Тест на проникновение
9.	Целостность ИСи информации (ОЦЛ)	СЗИ от НСД SecretNet ПАК Соболев Средства резервного копирования
10.	Доступность технических средств и информации (ОДТ)	Отказоустойчивые конфигурации Средства резервного копирования
11.	Защита среды виртуализации (ЗСВ)	vGate TrendMicro Deep Security Сертифицированная VMware vSphere 5.1
12.	Защита технических средств и оборудования (ЗТС)	Применяемые на объекте системы физической охраны (видеонаблюдение, контроль и управление доступом, сигнализация и пр).
13.	Защиту автоматизированной системы и ее компонентов (ЗИС)	СЗИ от НСД SecretNet vGate АПКШ Континент Arbor

Пример выбора технических средств

Группа мер	Средства защиты информации
Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)	АПКШ «Континент» 3,9
Управление доступом субъектов доступа к объектам доступа (УПД)	АПКШ «Континент» 3,9
Ограничение программной среды (ОПС)	vGate - S SecretNet Studio
Защита машинных носителей информации (ЗНИ)	СЗИ от НСД SecretNet LSP
Регистрация событий безопасности (РСБ)	АПКШ «Континент» 3.9
Антивирусная защита (АВЗ)	SecretNet Studio
Обнаружение (предотвращение) вторжений (COB)	COB Континент (детектор атак)
Контроль (анализ) защищенности информации (АНЗ)	СЗИ от НСД SecretNet LSP
Целостность информационной системы и информации (ОЦЛ)	Соболев
Доступность технических средств и информации (ОДТ)	АПКШ «Континент» 3.9
Защита среды виртуализации (ЗСВ)	Не реализована
Защита технических средств и оборудования (ЗТС)	Применяемые на объекте системы физической охраны (видеонаблюдение, СКУД и пр).
Защиту автоматизированной системы и ее компонентов (ЗИС)	АПКШ «Континент» 3.9
Выявление инцидентов и реагирование на них (ИНЦ)	АПКШ «Континент» 3.9
Управление конфигурацией информационной системы и системы защиты ПДн(УКФ)	Периодический анализ уровня защищённости ИСПДн и управление конфигурацией по ситуации

2.2 Класс защиты технических средств

Согласно новых нормативных документов ФСТЭК России, технические меры защиты информации реализуются посредством применения средств защиты информации, имеющих

необходимые функции безопасности. В этом случае:

в ГИС 1 и 2 классов защищенности применяются:

- СЗИ, программное обеспечение которых прошло проверку не ниже чем по 4 уровню контроля отсутствия недекларированных возможностей, а также:

- средства вычислительной техники не ниже 5 класса;
- системы обнаружения вторжений и средства антивирусной защиты не ниже 4 класса;
- межсетевые экраны не ниже 3 класса в случае взаимодействия ГИС с

информационно-телекоммуникационными сетями международного информационного обмена и не ниже 4 класса в случае отсутствия взаимодействия ГИС с информационно-телекоммуникационными сетями международного информационного обмена.

В ГИС 3 класса защищенности применяются:

- средства вычислительной техники не ниже 5 класса;

- системы обнаружения вторжений и средства антивирусной защиты не ниже 4 класса, в случае взаимодействия ГИС с информационно-телекоммуникационными сетями международного информационного обмена, и не ниже 5 класса, в случае отсутствия взаимодействия ГИС с информационно-телекоммуникационными сетями международного информационного обмена;

- межсетевые экраны не ниже 3 класса в случае взаимодействия ГИС с информационно-телекоммуникационными сетями международного информационного обмена и не ниже 4 класса в случае отсутствия взаимодействия ГИС с информационно-телекоммуникационными сетями международного информационного обмена.

Пример соответствия выбранных мер техническим и организационным средствам

№ п/п	Условное обозначение и номер меры	Содержание мер по обеспечению безопасности ИС	Усиление мер	Способ реализации меры по обеспечению безопасности ИС	Класс защиты
1.	ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	1а, 2а, 3	АПКШ «Континент» 3,9 Приказ об утверждении списка должностных лиц, которым необходим доступ к персональным данным.	4 класс
2.	ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов		АПКШ «Континент» 3,9; Приказ о назначении и инструкция ответственного за обеспечение безопасности персональных данных; Приказ об утверждении списка должностных лиц, которым необходим доступ к персональным данным; Матрица доступа сотрудников к информационным ресурсам ГИС; Инструкция пользователя по работе в ИС; Положение об обеспечении безопасности ПДн; Инструкция по организации парольной защиты в ГИС.	
3.	ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации		Средство ЗИDallas Lock 8.0-К с межсетевым экраном; Инструкция о порядке проведения служебного расследования, нарушений режима информационной безопасности; Матрица доступа сотрудников к информационным ресурсам ГИС; Инструкция пользователя по работе в ИС.	
4.	ИАФ.5	Защита обратной связи при вводе аутентификационной информации		Средство ЗИDallas Lock 8.0-К с межсетевым экраном;	
5.	УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей		Средство ЗИDallas Lock 8.0-К с межсетевым экраном; Приказ о назначении и инструкция ответственного за обеспечение безопасности персональных данных; Приказ об утверждении списка должностных лиц, которым необходим доступ к персональным данным; Матрица доступа сотрудников к информационным ресурсам ГИС; Инструкция пользователя по работе в ИС.	
6.	УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и		Средство ЗИDallas Lock 8.0-К с межсетевым экраном; Политика в отношении обработки ПДн; Положение об обеспечении безопасности ПДн; Матрица доступа сотрудников к информационным ресурсам ГИС.	

		правил разграничения доступа			
7.	УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами ИС, а также между информационными системами		Средство ZIDallas Lock 8.0-К с межсетевым экраном; Приказ о назначении и инструкция ответственного за обеспечение безопасности персональных данных.	
8.	УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной безопасности		Средство ZIDallas Lock 8.0-К с межсетевым экраном; Приказ об утверждении списка должностных лиц, которым необходим доступ к персональным данным; Положение об обеспечении безопасности ПДн; Матрица доступа сотрудников к информационным ресурсам ГИС.	
9.	УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование ИС		Средство ZIDallas Lock 8.0-К с межсетевым экраном; Приказ о назначении и инструкция ответственного за обеспечение безопасности персональных данных; Приказ об утверждении списка должностных лиц, которым необходим доступ к персональным данным; Приказ об обеспечении безопасности ПДн; Матрица доступа сотрудников к информационным ресурсам ГИС; Инструкция пользователя по работе в ИС.	
10.	УПД.6	Ограничение неуспешных попыток входа в ИС (доступа к ИС)		Средство ZIDallas Lock 8.0-К с межсетевым экраном; Приказ о назначении и инструкция ответственного за обеспечение безопасности персональных данных; Инструкция пользователя по работе в ИС.	
11.	УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети		Программно-аппаратный комплекс ViPNet Coordinator HW 1000.	
12.	ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов		Приказ о списке обязательного и дополнительного разрешенного ПО; Белый лист; Черный лист.	
13.	ЗНИ.1	Учет машинных носителей		Журнал учета машинных носителей информации.	

		информации			
14.	ЗНИ.2	Управление доступом к машинным носителям информации		Положение о пропускном режиме; Положение о лицах, допущенных к работе на АРМ и обработке ПДн.	
15.	ЗНИ.8	Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания)		Средство ZIDallas Lock 8.0-К с межсетевым экраном; Политика в отношении обработки ПДн; Положение об обеспечении безопасности ПДн; Приказ о назначении и инструкция ответственного за обеспечение безопасности персональных данных; Порядок организации безопасности носителей информации; Журнал учета машинных носителей информации, на которых хранятся и (или) обрабатываются ПДн.	
16.	РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения		Средство ZIDallas Lock 8.0-К с межсетевым экраном; Программа «Kaspersky Endpoint Security 10»; Приказ о назначении и инструкция ответственного за обеспечение безопасности персональных данных; Положение об обеспечении безопасности ПДн; Инструкция о порядке проведения служебного расследования, нарушения режима информационной безопасности; Средство регистрации и учета операционной системы.	
17.	РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации		Средство ZIDallas Lock 8.0-К с межсетевым экраном; Программа «Kaspersky Endpoint Security 10»; Приказ о назначении и инструкция ответственного за обеспечение безопасности персональных данных; Положение об обеспечении безопасности ПДн; Инструкция о порядке проведения служебного расследования, нарушения режима информационной безопасности; Средство регистрации и учета операционной системы.	
18.	РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения		Средство ZIDallas Lock 8.0-К с межсетевым экраном; Программа «Kaspersky Endpoint Security 10»; Приказ о назначении и инструкция ответственного за обеспечение безопасности персональных данных; Положение об обеспечении безопасности ПДн; Инструкция о порядке проведения служебного расследования, нарушения режима информационной безопасности; Средство регистрации и учета операционной системы.	
19.	РСБ.4	Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах		Средство ZIDallas Lock 8.0-К с межсетевым экраном; Программа «Kaspersky Endpoint Security 10»; Приказ о назначении и инструкция ответственного за обеспечение безопасности персональных данных; Положение об обеспечении безопасности ПДн;	

		сбора информации и достижение предела или переполнения объема (емкости) памяти		Инструкция о порядке проведения служебного расследования, нарушения режима информационной безопасности; Средство регистрации и учета операционной системы.	
20.	РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них		Средство ZIDallas Lock 8.0-K с межсетевым экраном; Программа «Kaspersky Endpoint Security 10»; Приказ о назначении и инструкция ответственного за обеспечение безопасности персональных данных; Положение об обеспечении безопасности ПДн; Инструкция о порядке проведения служебного расследования, нарушения режима информационной безопасности; Средство регистрации и учета операционной системы.	
21.	РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в ИС		Средство ZIDallas Lock 8.0-K с межсетевым экраном; Программа «Kaspersky Endpoint Security 10»; Приказ о назначении и инструкция ответственного за обеспечение безопасности персональных данных; Положение об обеспечении безопасности ПДн; Инструкция о порядке проведения служебного расследования, нарушения режима информационной безопасности; Средство регистрации и учета операционной системы.	
22.	РСБ.7	Защита информации о событиях безопасности		Средство ZIDallas Lock 8.0-K с межсетевым экраном; Программа «Kaspersky Endpoint Security 10»; Приказ о назначении и инструкция ответственного за обеспечение безопасности персональных данных; Положение об обеспечении безопасности ПДн; Инструкция о порядке проведения служебного расследования, нарушения режима информационной безопасности; Средство регистрации и учета операционной системы.	
23.	АВЗ.1	Реализация антивирусной защиты		Программа «Kaspersky Endpoint Security 10».	
24.	АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)		Программа «Kaspersky Endpoint Security 10»; Инструкция по организации антивирусной защиты в ГИС; Инструкция по организации обновления общесистемного и прикладного программного обеспечения ГИС.	
25.	АНЗ.1	Выявление, анализ уязвимостей ИС и оперативное устранение вновь выявленных уязвимостей		Программа «Kaspersky Endpoint Security 10»; Сетевой сканер безопасности Сканер-ВС; Положение об обеспечении безопасности ПДн; Инструкция о порядке проведения служебного расследования, нарушения режима информационной безопасности; Инструкция пользователя по работе в ИС.	

4. Оборудование и материалы (перечень используемого оборудования)

Состав раздаточного материала:

- коллекция макетов с конфиденциальными документами;
- коллекция документов для выявления конфиденциальных документов фирмы;
- карточка индивидуального ситуационного варианта к заданиям работы;
- учетные формы;
- рабочая тетрадь;
- перечень конфиденциальных документов (сведений) негосударственной фирмы;
- операционная схема;
- внутренняя опись документов, находящихся у исполнителя (студента);
- практикум.

5. Указания по технике безопасности

- ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории;
- убедиться в целостности электрических розеток и разъемов. В лаборатории необходимо быть в сменной обуви;
- включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

6. Задания

- выполнение операций процедуры приема пакетов;
- составление акта о повреждении или нарушении в оформлении пакета;
- выполнение операций процедуры учета пакетов;
- выполнение операций процедуры распределения и вскрытия пакетов;
- выполнение операций процедуры выделения конфиденциальных документов из документов входного потока.

7. Содержание отчета

По результатам выполнения практического занятия студенты оформляют и защищают в индивидуальном порядке в форме беседы результаты выполнения заданий.

Результатом работы является:

- журнал учёта входящих пакетов;
- журнал учёта входящих документов;
- акты по замечаниям.

8. Контрольные вопросы и тестовые задания

1. Какое назначение имеет стадия приема, первичной обработки, предварительного рассмотрения и распределения поступивших документов?
2. Каким угрозам подвергается документ в процессе его доставки адресату и приема адресатом?
3. Какие задачи защиты информации должны быть решены при выполнении процедур и операций данной стадии?
4. Какое назначение имеет каждая из выполняемых процедур?
5. Как осуществляется прием пакетов от курьеров и из почтового отделения связи?
6. Как осуществляется прием и учет пакетов, поступивших во вне рабочее время?
7. Как осуществляется прием пакетов, имеющих повреждения или нарушения в оформлении?
8. Кому и как передаются пакеты, не подлежащие вскрытию?

9. Как проверяется комплектность поступивших документов?
10. Как осуществляется пересылка ошибочно присланных документов?
11. Как происходит выделение документов, содержащих негосударственную тайну, из общего потока открытых документов?

9. Список литературы

Основная литература:

1. Аверченков, В.И. Защита персональных данных в организации [Электронный ресурс] / В.И. Аверченков, М.Ю. Рытов, Т.Р. Гайнулин. - 2-е изд., стер. - М. : Флинта, 2017. - 124 с. - ISBN 978-5-9765-1273-3. - URL: <http://biblioclub.ru/index.php?page=book&id=93260>
2. Минин, И.В. Защита конфиденциальной информации при электронном документообороте: учебное пособие [Электронный ресурс] / И.В. Минин, О.В. Минин. - Новосибирск: НГТУ, 2018. - 20 с. - ISBN 978-5-7782-1829-1. - URL: <http://biblioclub.ru/index.php?page=book&id=228779>

Дополнительная литература:

1. Лузина, Т.В. Основы документооборота в таможенных органах : [16+] / Т.В. Лузина, С.С. Решетникова ; Министерство науки и образования РФ, ФГБОУ ВПО Тюменский государственный университет, Институт дистанционного образования, Институт психологии и др. – Тюмень : Издательство Тюменского государственного университета, 2016. – 524 с. : ил. – Режим доступа: по подписке. – URL: <http://biblioclub.ru/index.php?page=book&id=567333>

Практическое занятие 10,11 Реализация выбранных организационных мер для системы защиты информации в ИС организации

Тема 10- 11: Порядок адаптации базового набора мер по защите информации. Порядок уточнения адаптированного набора мер по защите информации в ИС организации

1. Цель занятия:

- приобретение практических навыков анализа информационных систем
- приобретение практических навыков построения системы защиты информации в ИС.

1. Формируемые компетенции или их части

В результате выполнения работы студенты должны:

- уметь использовать нормативные правовые документы при организации подсистемы защищённого конфиденциального делопроизводства;
- владеть технологией организации конфиденциального делопроизводства.

2. Теоретическая часть

3. Оборудование и материалы (перечень используемого оборудования)

Состав раздаточного материала:

- коллекция макетов с конфиденциальными документами;
- коллекция документов для выявления конфиденциальных документов фирмы;
- карточка индивидуального ситуационного варианта к заданиям работы;
- учетные формы;
- рабочая тетрадь;
- перечень конфиденциальных документов (сведений) негосударственной фирмы;
- операционная схема;
- внутренняя опись документов, находящихся у исполнителя (студента);
- практикум.

4. Указания по технике безопасности

- ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории;
- убедиться в целостности электрических розеток и разъемов. В лаборатории необходимо быть в сменной обуви;
- включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

5. Задания

- выполнение операций процедуры приема пакетов;
- составление акта о повреждении или нарушении в оформлении пакета;
- выполнение операций процедуры учета пакетов;
- выполнение операций процедуры распределения и вскрытия пакетов;
- выполнение операций процедуры выделения конфиденциальных документов из документов входного потока.

6. Содержание отчета

По результатам выполнения практического занятия студенты оформляют и защищают в индивидуальном порядке в форме беседы результаты выполнения заданий.

Результатом работы является:

- журнал учёта входящих пакетов;
- журнал учёта входящих документов;

- акты по замечаниям.

7. Контрольные вопросы и тестовые задания

1. Какое назначение имеет стадия приема, первичной обработки, предварительного рассмотрения и распределения поступивших документов?
2. Каким угрозам подвергается документ в процессе его доставки адресату и приема адресатом?
3. Какие задачи защиты информации должны быть решены при выполнении процедур и операций данной стадии?
4. Какое назначение имеет каждая из выполняемых процедур?
5. Как осуществляется прием пакетов от курьеров и из почтового отделения связи?
6. Как осуществляется прием и учет пакетов, поступивших во внерабочее время?
7. Как осуществляется прием пакетов, имеющих повреждения или нарушения в оформлении?
8. Кому и как передаются пакеты, не подлежащие вскрытию?
9. Как проверяется комплектность поступивших документов?
10. Как осуществляется пересылка ошибочно присланных документов?
11. Как происходит выделение документов, содержащих негосударственную тайну, из общего потока открытых документов?

8. Список литературы

Основная литература:

1. Аверченков, В.И. Защита персональных данных в организации [Электронный ресурс] / В.И. Аверченков, М.Ю. Рытов, Т.Р. Гайнулин. - 2-е изд., стер. - М. : Флинта, 2017. - 124 с. - ISBN 978-5-9765-1273-3. - URL: <http://biblioclub.ru/index.php?page=book&id=93260>
2. Минин, И.В. Защита конфиденциальной информации при электронном документообороте: учебное пособие [Электронный ресурс] / И.В. Минин, О.В. Минин. - Новосибирск: НГТУ, 2018. - 20 с. - ISBN 978-5-7782-1829-1. - URL: <http://biblioclub.ru/index.php?page=book&id=228779>

Дополнительная литература:

1. Лузина, Т.В. Основы документооборота в таможенных органах : [16+] / Т.В. Лузина, С.С. Решетникова ; Министерство науки и образования РФ, ФГБОУ ВПО Тюменский государственный университет, Институт дистанционного образования, Институт психологии и др. – Тюмень : Издательство Тюменского государственного университета, 2016. – 524 с. : ил. – Режим доступа: по подписке. – URL: <http://biblioclub.ru/index.php?page=book&id=567333>

Практическое занятие 12,13 Оценка эффективности системы ЗИ в ИС организации
Тема 12-13: Определение актуальных угроз для ИС организации Порядок выбора
технических средств для реализации технических мер защиты информации

1. Цель занятия:

- приобретение практических навыков анализа информационных систем
- приобретение практических навыков построения системы защиты информации в ИС.

2. Формируемые компетенции или их части

В результате выполнения работы студенты должны:

- уметь использовать нормативные правовые документы при организации подсистемы защищённого конфиденциального делопроизводства;
- владеть технологией организации конфиденциального делопроизводства.

3. Теоретическая часть

3.1 Оценка эффективности СЗИ в ИС по критерию оценки риски информационной безопасности ИС

Оценка риска ИБ ИС предприятия состоит из следующих этапов (таблица 1).

Таблица 1 - Этапы работы по оценке риска ИБ ИС

Этапы	Название этапов
Этап 1	Определение риска несоответствия требованиям законодательства в области ИБ для ПДн
Этап 2	Определение вероятностей реализации хотя бы одной из актуальных угроз
Этап 3	Определение ценности информационных активов
Этап 4	Определение степени использования организационных и технических средств защиты ПДн
Этап 5	Определение количественного значения риска ИБ

Этап 1 Определение риска несоответствия требованиям законодательства в области ИБ для ПДн

В ходе проведения анализа всем требованиям, которые выполняются, присваивается значение «1», частично выполняются – «0,5» не выполняются – «0».

Все значения, которым присвоено значение 0,5 и 1, суммируются, остальные значения не учитываются (таблица 2).

Таблица 2 - Анализ риска несоответствия требования законодательства в области ИБ ПДн

Нормативные документы по ИБ предприятия ()	Соответствие	
	До (0 и 1 произвольно)	После (только 1)
<i>Акт по результатам обследования ИС</i>	0	1
<i>Перечень сведений конфиденциального характера предприятия</i>		
<i>Перечень ПДн обрабатываемых в ИС ПДн</i>		
<i>Инструкция администратора информационной безопасности</i>		
ИТОГО		

Уровень риска несоответствия требований законодательства по ИБ R_n , который определяется суммированием полученных значений соответствия (таблица 5). Результат оценки определяется по соответствующему значению таблицы 3.

Таблица 3 - Результаты анализа риска несоответствия требованиям законодательства в области защиты конфиденциальной документированной информации

% выполнения требований нормативных документов	Риск несоответствия требованиям законодательства (R_n)
91-100	0,01
61-90	0,25
21-60	0,5
≤ 20	0,9

Таким образом, значение риска несоответствия требования законодательства в области ИБ для ПДн равно $R_{n1} = 71\%$, $R_{n2} = 0,25$.

Этап 2 Определение вероятностей реализации актуальных угроз.

На основании построенной частной модели угроз для ИС предприятия определён перечень актуальных угроз и вероятности их реализации (таблица 4).

Таблица 4 - Перечень актуальных угроз и вероятности их реализации

№ п/п	Перечень актуальных угроз безопасности для ИС	Вероятность реализации угрозы до внедрения СЗ	Вероятность реализации угрозы после внедрения
		0,5	0,4
		0,5	0,4
		0,5	0,4
		0,5	0,4
		0,5	0,4
		0,5	0,4
		0,5	0,4
		0,5	0,4
		0,5	0,4
0		0,5	0,4
1		0,5	0,4
2		0,5	0,4
3		0,5	0,4
4		0,5	0,4
5		0,5	0,4
6		.	.
7		.	.
8		.	.

Вероятность реализации хотя бы одной угрозы из совокупности вероятностей угроз $P_{y1}, P_{y2}, \dots, P_{yn}$, равна разности между единицей и произведением вероятностей противоположных событий. Вероятность противоположных событий определяется как разность между единицей и вероятностью угроз.

$$D_{\acute{o}\tilde{\alpha}\delta} = 1 - \tilde{I} (1 - D_{\acute{o}1})(1 - D_{\acute{o}2})(1 - D_{\acute{o}3})...(1 - D_{\acute{o}i})$$

где n-количество угроз.

$$P_{\text{угр}} = 1 - \Pi(1 - 0,35)(1 - 0,35)(1 - 0,35)(1 - 0,35)(1 - 0,35)(1 - 0,35)(1 - 0,25)(1 - 0,35)(1 - 0,35)(1 - 0,35)(1 - 0,25)(1 - 0,35)(1 - 0,35)(1 - 0,25)(1 - 0,35) = 0,696.$$

В результате проведенных расчетов вероятность реализации угроз по основным типам объектов среды:

$$P_{\text{угр } 1} = 0,696; P_{\text{угр } 2} = 0,52.$$

Этап 3. Определение ценности информационных активов.

Ценность информационного актива определяется, как отношение стоимости обрабатываемой в ИС информации к стоимости всего предприятия, в нашем случае:

$$C = \frac{C_{\text{ПДн}}}{C_{\text{п}}},$$

где $C_{\text{ПДн}}$ – стоимость обрабатываемых ПДн в ИС предприятия;

$C_{\text{п}}$ – стоимость всего предприятия.

В связи с тем, что зачастую невозможно определить точные стоимости активов и предприятия в целом, рекомендуется ценность актива задавать в диапазоне от 0 до 1, которая будет показывать отношение цены актива к стоимости всего бизнеса. Т.о., можно принять $C = 0,5$. (Принимаем C равное № - ру варианта)

Этап 4. Определение степени использования организационных мер и технических средств защиты информации в ИС

4.1 Определение степени использования организационных мер защиты информации в ИС

В ходе проведения анализа всем требованиям, которые выполняются, присваивается значение «1», частично выполняются – «0,5» не выполняются – «0» (таблица 5).

Таблица 5 - Перечень организационных мер ЗИ реализованных в ИС

Организационные меры защиты информации	Соответствия	
	до	после
<i>(Организационные меры защиты)</i>	0	1
	0	0
	1	1
Итого	13	21

В таблице 6 представлены соответствие выполняемых организационных мер защиты информации и коэффициент использования организационных мер защиты информации.

Таблица 6 - Коэффициент использования организационных мер защиты в ИС

% выполнения организационных мер защиты в ИС	Риск несоответствия (R_o)
91-100	0,01
61-90	0,25

21-60	0,5
≤ 20	0,9

Таким образом, коэффициент использования организационных мер защиты информации $K_{o1} = 0,25$, $K_{o2} = 0,01$.

4.2 Определение степени использования технических мер защиты информации в ИС

В ходе проведения анализа всем техническим мерам, которые выполняются, присваивается значение «1», частично выполняются – «0,5» не выполняются – «0» (таблица 7).

Таблица 7 - Перечень технических мер защиты информации реализованных в ИС

Технические меры защиты информации	Соответствия	
	до	после
<i>(Технические меры защиты)</i>	0	1
	1	1
ИТОГО	14	23

Таблица 8- Коэффициент использования технических мер защиты в ИС

% выполнения организационных мер защиты в ИС	Риск несоответствия требованиям законодательства (R_t)
91-100	0,01
61-90	0,25
21-60	0,5
≤ 20	0,9

Расчёты показали, что $K_{t1} = 0,25$, $K_{t2} = 0,15$.

Этап 4. Количественное определение риска

В разрабатываемой методике процедура оценки рисков реализации хотя бы одной угрозы основывается на взаимности нескольких факторов – вероятности происшествия, а именно вероятности реализации хотя бы одной актуальной угрозы, коэффициента ценности актива, среднеарифметического значения коэффициентов возможности использования организационных уязвимостей и возможности использования технических уязвимостей и риска несоответствия требованиям законодательства. Под коэффициентом ценности актива понимают ценность или критичность актива по отношению ко всему бизнесу.

Общая формула определения риска информационной безопасности для ИС имеет вид [8]:

$$R = P_{\text{угр}} \cdot R_n \cdot C \cdot \frac{K_o + K_T}{2} \cdot 100 \%,$$

где R - численная величина риска реализации угроз ИБ;

$P_{\text{угр}}$ - вероятность реализации хотя бы одной угрозы из всего перечня угроз;

R_n - риск несоответствия требованиям законодательства в области информационной безопасности;

C - ценность актива (0...1);

Ko - вероятность использования организационных уязвимостей;

Kt - вероятность использования технических уязвимостей.

$$R_1 = 0.996 \cdot 0.5 \cdot 0.5 \cdot \frac{0.25 + 0.5}{2} \cdot 100 \% = 8.4 \%$$

$$R_2 = 0.95 \cdot 0.25 \cdot 0.5 \cdot \frac{0.15 + 0.15}{2} \cdot 100 \% = 3.27 \%$$

Сравнительный анализ основных показателей риска ИБ представлен на рисунке 1

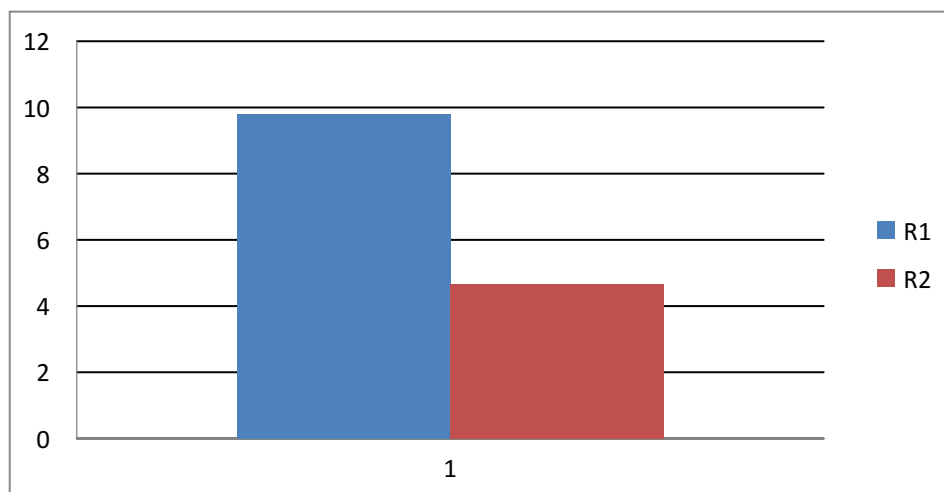


Рисунок 1 – Значение риска ИБ ИС

2 Технико-экономическое обоснование предложенных рекомендаций по защите информации

Таблица 9 - Спецификация затрат на средства защиты ИС предприятия

Наименование средства/меры (выбираем из графы «Технические средства защиты»)	Количество	Стоимость, тыс. руб.
Сертифицированная ОС Windovs Server 2012 Standard	6	53,1
Сертифицированная ОС Windovs 7 Professional	10	18
С-Терра Криптошлюз 1000V	1	101
	14	61,6
	25	28,5
	6	54,7
	2	110
	3	47,2
	106	27,7
	106	166,6
СКУД	1	151
ИТОГО		919,4

4. Оборудование и материалы (перечень используемого оборудования)

Состав раздаточного материала:

- коллекция макетов с конфиденциальными документами;
- коллекция документов для выявления конфиденциальных документов фирмы;
- карточка индивидуального ситуационного варианта к заданиям работы;
- учетные формы;
- рабочая тетрадь;
- перечень конфиденциальных документов (сведений) негосударственной фирмы;
- операционная схема;
- внутренняя опись документов, находящихся у исполнителя (студента);
- практикум.

5. Указания по технике безопасности

- ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории;
- убедиться в целостности электрических розеток и разъемов. В лаборатории необходимо быть в сменной обуви;
- включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

6. Задания

- выполнение операций процедуры приема пакетов;
- составление акта о повреждении или нарушении в оформлении пакета;
- выполнение операций процедуры учета пакетов;
- выполнение операций процедуры распределения и вскрытия пакетов;
- выполнение операций процедуры выделения конфиденциальных документов из документов входного потока.

7. Содержание отчета

По результатам выполнения практического занятия студенты оформляют и защищают в индивидуальном порядке в форме беседы результаты выполнения заданий.

Результатом работы является:

- журнал учёта входящих пакетов;
- журнал учёта входящих документов;
- акты по замечаниям.

8. Контрольные вопросы и тестовые задания

1. Какое назначение имеет стадия приема, первичной обработки, предварительного рассмотрения и распределения поступивших документов?
2. Каким угрозам подвергается документ в процессе его доставки адресату и приема адресатом?
3. Какие задачи защиты информации должны быть решены при выполнении процедур и операций данной стадии?
4. Какое назначение имеет каждая из выполняемых процедур?
5. Как осуществляется прием пакетов от курьеров и из почтового отделения связи?
6. Как осуществляется прием и учет пакетов, поступивших во внерабочее время?
7. Как осуществляется прием пакетов, имеющих повреждения или нарушения в оформлении?
8. Кому и как передаются пакеты, не подлежащие вскрытию?

9. Как проверяется комплектность поступивших документов?
10. Как осуществляется пересылка ошибочно присланных документов?
11. Как происходит выделение документов, содержащих негосударственную тайну, из общего потока открытых документов?

9. Список литературы

Основная литература:

1. Аверченков, В.И. Защита персональных данных в организации [Электронный ресурс] / В.И. Аверченков, М.Ю. Рытов, Т.Р. Гайнулин. - 2-е изд., стер. - М. : Флинта, 2017. - 124 с. - ISBN 978-5-9765-1273-3. - URL: <http://biblioclub.ru/index.php?page=book&id=93260>
2. Минин, И.В. Защита конфиденциальной информации при электронном документообороте: учебное пособие [Электронный ресурс] / И.В. Минин, О.В. Минин. - Новосибирск: НГТУ, 2018. - 20 с. - ISBN 978-5-7782-1829-1. - URL: <http://biblioclub.ru/index.php?page=book&id=228779>

Дополнительная литература:

1. Лузина, Т.В. Основы документооборота в таможенных органах : [16+] / Т.В. Лузина, С.С. Решетникова ; Министерство науки и образования РФ, ФГБОУ ВПО Тюменский государственный университет, Институт дистанционного образования, Институт психологии и др. – Тюмень : Издательство Тюменского государственного университета, 2016. – 524 с. : ил. – Режим доступа: по подписке. – URL: <http://biblioclub.ru/index.php?page=book&id=567333>

Практическое занятие 14,15,16 Разработка технического задания на создание системы ЗИ в ИС организации

Тема 14-16: Разработка технического задания на создание СЗИ в системе защищённого документооборота. Оценка эффективности СЗИ в ИС организации. Порядок организации отдела конфиденциально делопроизводства

1. Цель занятия:

- приобретение практических навыков анализа информационных систем
- приобретение практических навыков построения системы защиты информации в ИС.

2. Формируемые компетенции или их части

В результате выполнения работы студенты должны:

- уметь использовать нормативные правовые документы при организации подсистемы защищённого конфиденциального делопроизводства;
- владеть технологией организации конфиденциального делопроизводства.

3. Теоретическая часть

1. Общие сведения

1.1 Полное наименование системы и ее условное обозначение

Полное наименование системы «Система защиты информации».

1.2 Шифр темы

ОТЗИ 18АО.НИР

1.3 Наименование предприятий (объединений) разработчика и заказчика (пользователя) системы и их реквизиты

Предприятие разработчика: ФГБОУ ВО «Северо-кавказский федеральный университет». Адрес: г. Ставрополь, ул. Пушкина 1.

Предприятие заказчика: АО «Электроавтоматика». Адрес: г. Ставрополь, ул. Заводская 3.

1.4 Перечень документов, на основании которых создается система, кем и когда утверждены эти документы

Полный перечень документов приведен в разделе «Источники разработки».

1.5 Плановые сроки начала и окончания работы по созданию системы

Начало работ: 13.03.2021. Окончание работ: 20.06.2022.

1.6 Сведения об источниках и порядке финансирования работ

Работы по разработке СЗИ финансируются из государственного бюджета. Являются инициативными на основании выполнения требований по договору обучения №18У234.

1.7 Порядок оформления и предъявления заказчику результатов работ по созданию системы (ее частей), по изготовлению и наладке отдельных средств (технических, программных, информационных) и программно-технических (программно-методических) комплексов системы.

Результаты работы по СЗИ передаются Заказчику в письменном виде в составе выпускной квалификационной работы в сроки, установленные заданием.

2. Назначение и цели создания системы защиты персональных данных

2.1 Назначение системы

СЗИ в ИС предназначены для обеспечения конфиденциальности, целостности и доступности информации, обрабатываемых в ИС, исключая несанкционированный, в

том числе случайный доступ к конфиденциальной информации, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение информации.

2.2 Цели создания системы

Целями работ по созданию СЗИ являются:

- реализация мер по защите информации, хранимых и обрабатываемых в ИС, в части требований конфиденциальности, целостности и доступности;
- соответствие требованиям обеспечения информационной безопасности при обработке Информации в ИС, регламентируемых руководящими документами ФСТЭК и ФСБ РФ;
- сохранение режима работы пользователей ИС максимально близкого к привычному режиму.
- снижение вероятности реализации актуальных угроз несанкционированного доступа к Информации;
- определение подлинности субъекта доступа;

Критериями оценки достижения поставленных целей по созданию СЗИ являются:

- соответствие требованиям по обеспечению безопасности информации соответствующего класса защиты;
- выполнение функциональных требований настоящего технического задания.

2.3 Класс защищенности информационной системы

АС, обрабатывающие защищаемую информацию, должны быть отнесены по уровню защищенности к классам 3Б, 2Б и не ниже 1Д.

УТВЕРЖДАЮ
Генеральный директор
Ю.Д. Мишин
08.06.2021

АКТ
предварительной классификации информационной системы

Комиссия в составе:

Председатель комиссии	начальник службы безопасности	Юрьев Вячеслав Григорьевич
Член комиссии	заместитель начальника технического отдела	Свиридов Вячеслав Григорьевич
Член комиссии	ст. специалист	Петров Дмитрий Владимирович

рассмотрев исходные данные информационной системы в соответствии с требованиями ФЗ №152 «О защите персональных данных» и требования руководящего документа Гостехкомиссии России "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации" от 30.03.1992 определили:

1. По категории персональные данные, обрабатываемые в ИС относятся **иным**;

2. Объем обрабатываемых информации менее чем 100 000 субъектов Информации .

3 Структура информационной системы: комплекс автоматизированных рабочих мест, объединенных в единую информационную систему средствами связи с использованием технологии удаленного доступа (поскольку используется автоматизированная система в распределенном режиме).

5. Наличие подключений к сетям связи общего пользования и (или) сетям международного информационного обмена: имеются (имеется многоточечное подключение к сети Интернет).

6. Режим обработки информации в информационной системе: многопользовательский.

7. Разграничение прав доступа пользователей: с разграничением (поскольку доступ к системе имеют разные лица, каждый из которых наделен своими полномочиями, перечисленными в описании ИС информации настоящего документа).

8. Местонахождение информационной системы персональных данных: в пределах Российской Федерации.

По результатам анализа исходных данных ИС присвоен класс защищённости **2**, Уровень защищённости ПДн **УЗ=3**.

Председатель комиссии

В.Г. Юрьев

Члены комиссии

В.Г. Свиридов

Д.В. Петров

Для повышения уровня защищенности информации рекомендуется использовать сертифицированные по требованиям безопасности информации СВТ для 3 УЗ.

3. Характеристика объектов автоматизации

3.1 Краткие сведения об объекте автоматизации

1. Наименование организации: АО «Электроавтоматика.
2. Физическое расположение ИС, Расположена по адресу: 355040, Ставропольский край г. Ставрополь, ул. Заводская, д. 3.

ИС расположена в 3-х отдельных помещениях на 3 этаже 4 этажного здания с двумя выходами (основным и пожарным). На выходах комплекса помещений установлены металлические двери, СКУД не установлен. Охрана здания осуществляется собственником здания. Пост охраны расположен при входе в здание. В комплексе помещений развернута пожарная сигнализация и система оповещения.

4. Логическая структура ИС

ИС АО «Электроавтоматика» представляет собой АС на базе ЛВС с серверами и рабочими станциями (АРМ).

Все сервера реализованы на серверах предприятия и установлены в серверной, которая расположена в отдельном помещении. На серверах установлены ОС: Ubuntu 10.04, Windows Server 2003/2008.

АРМ расположены в общем свободном пространстве помещений, в которые имеют доступ все сотрудники предприятия. АРМ принадлежат предприятию. На АРМ используются ОС: Windows Vista, Windows 7, Ubuntu 11.

Сервера и рабочие станции подключены к локальной сети организации, образованной ИТ-инфраструктурой, которая подключена к сети интернет через оборудование провайдера. Сетевая инфраструктура построена на оборудовании DLink. Связь между серверным помещением и помещениями с АРМ через интернет.

3.2 Сведения об условиях эксплуатации объекта автоматизации и характеристика окружающей среды

Поддержку ИС осуществляет по договору консалтинга программист 1С. В соответствии с действующим законодательством РФ, обработка Информации на предприятии осуществляется в соответствии с учредительными документами в специализированной учетной системе, реализованная на выделенном сервере с тонким клиентом.

4. Требования к системе защиты информации

4.1 Требования к системе в целом

К СЗИ ИС предъявляются следующие общие требования:

- СЗИ должна представлять собой согласованный комплекс организационных мероприятий, программных, технических и программно-технических мер, направленных на обеспечение ИБ функционирования системы;
- СЗИ должна существенно затруднять реализацию потенциальных угроз ИБ функционированию ИС ИС. При невозможности использования мер по предотвращению реализации угроз ИБ, СЗИ должна реализовывать механизмы, позволяющие своевременно обнаружить несанкционированную деятельность и локализовать ее источник (субъект, канал воздействия);
- СЗИ ИС должна отвечать требованиям нормативно-правовой базы РФ в области защиты Информации.

- СЗИ ИС должна включать в себя средства (методики) тестирования состояния СЗИ и контроля целостности средств защиты информации.

Средства защиты, используемые при построении СЗИ, должны обеспечивать необходимый уровень ЗИ, не снижая, при этом, надежности технологий обработки информации и не оказывая существенного влияния на производительность средств вычислительной техники, входящих в ИС.

Проектные решения должны предусматривать план мероприятий по внедрению средств защиты информации, согласно которым период установки и настройки средств защиты информации не должен превышать одного рабочего дня.

4.1.1 Требования к численности и квалификации обслуживающего персонала

Для сопровождения СЗИ ИС необходимо иметь в штате:

- администратора безопасности, имеющего высшее профессиональное образование в области технической защиты информации либо высшее техническое или среднее профессиональное (техническое) образование и прошедшего переподготовку или повышение квалификации по вопросам технической защиты информации;
- системного администратора, имеющего высшее техническое образование.

4.1.2 Требования к техническим средствам и системам защиты

Требования к техническим средствам и системам защиты представлены в таблице

9.

Таблица 9- Соответствие СЗИ классу защиты ИС

Класс защиты ИС	Класс защиты СЗИ						Уровень контроля на отсутствие не декларированных возможностей
	СВТ	САВЗ	СОВ	МЭ	СДЗ	СЗИ	
КЗ 3	Не ниже 5 класса	Не ниже 4 класса	Не ниже 4 класса	Не ниже 3 класса	Не ниже 4 класса	Не ниже 6 класса	4 уровень контроля
Требования к сертификации	Использовать сертифицированные по требованиям безопасности информации СВТ и СЗИ						

4.1.3 Требования к надежности

Аппаратно-программные компоненты СЗИ должны удовлетворять условию круглосуточной работы, позволять осуществлять резервирование и восстановление системы после сбоев.

Должна быть обеспечена возможность резервного копирования конфигураций и журналов регистрации событий компонентов СЗИ.

4.1.4 Требования к безопасности

Все внешние элементы технических средств системы, находящиеся под напряжением, должны иметь защиту от случайного прикосновения, а сами технические средства иметь защитное заземление в соответствии с ГОСТ 12.1.030-81 и ПУЭ.

Система электропитания должна обеспечивать защитное отключение при перегрузках и коротких замыканиях в цепях нагрузки, а также аварийное ручное отключение.

Общие требования пожарной безопасности должны соответствовать нормам на бытовое электрооборудование. В случае возгорания не должно выделяться ядовитых газов и дымов. После снятия электропитания должно быть допустимо применение любых средств пожаротушения.

Факторы, оказывающие вредные воздействия на здоровье со стороны всех элементов системы (в том числе инфракрасное, ультрафиолетовое, рентгеновское и электромагнитное излучения, вибрация, шум, электростатические поля, ультразвук строчной частоты и т.д.), не должны превышать действующих норм (СанПиН 2.2.2./2.4.1340-03 от 03.06.2003 г.).

4.1.5 Требования к эргономике и технической эстетике

Серверные компоненты и активное сетевое оборудование СЗИ должны иметь возможность установки в монтажные стойки, предоставленные для размещения оборудования системы.

АРМ администратора СЗИ должен обеспечивать возможность непрерывной работы операторов в течение смены в соответствии с требованиями Постановления Главного государственного санитарного врача РФ от 3 июня 2003 г. № 118 «О введении в действие санитарно-эпидемиологических правил и нормативов СанПиН 2.2.2/2.4.1340-03» с изменениями от 25 апреля 2007 г.

Система должна иметь эргономичный интерфейс пользователя:

- взаимодействие системы и пользователя должно осуществляться на русском языке, за исключением системных сообщений, не подлежащих русификации;
- при работе с интерфейсом пользователь должен быть ориентирован на работу с клавиатурой и манипулятором графической информации «мышь»;
- для активного пользователя требуется отображать только тот функционал, который доступен в рамках его функциональной роли в системе.

4.1.6 Требования к эксплуатации, техническому обслуживанию, ремонту и хранению компонентов СЗИ

При создании СЗИ должны использоваться унифицированные, однотипные компоненты в целях обеспечения снижения расходов на обслуживание и ремонт, удобства эксплуатации.

Климатические условия эксплуатации компонентов СЗИ должны соответствовать требованиям ГОСТ 21552-84 и ГОСТ 27201-87.

Эксплуатация программно-технических средств должна предусматривать следующие виды технического обслуживания:

- оперативное обслуживание;
- профилактические работы.

Оперативное обслуживание должно предусматривать ежедневный контроль функционирования аппаратно-технических средств, целостности ресурсов системы. Оперативное обслуживание не должно нарушать выполнения функций СЗИ в целом.

Профилактическое обслуживание должно предусматривать периодическую проверку и обслуживание составных частей СЗИ, для которых такое обслуживание предусмотрено эксплуатационной документацией.

Объем и порядок выполнения технического обслуживания технических и программных средств СЗИ должны определяться эксплуатационной документацией.

Физический доступ неуполномоченных лиц к сетевому и серверному оборудованию должен быть запрещен.

Требования к эксплуатации, техническому обслуживанию, ремонту и хранению могут уточняться на этапе проектирования СЗИ.

4.1.7 Требования по сохранности информации при авариях

Сохранность информации при авариях в СЗИ должна обеспечиваться методом

резервного копирования.

Решения по обеспечению сохранности информации в СЗИ при авариях должны быть разработаны на стадии технического задания.

4.1.8 Требования к защите от влияния внешних воздействий

Защита ИС от влияния внешних воздействий должна осуществляться в рамках общих организационно-технических мероприятий по обеспечению безопасности и физической защите на объектах Пользователя. Должна обеспечиваться защита от ЭМИ согласно СанПиН 2.2.4/2.1.8.055-96, СанПиН 2.2.2.542-96.

4.1.9 Требования к патентной чистоте

При создании СЗИ должны соблюдаться положения законодательных актов РФ по соблюдению авторских прав и защите специальных знаков.

При поставке программного обеспечения должны быть выполнены требования ФЗ РФ «О правовой охране программ для электронных вычислительных машин и баз данных» от 23.09.1992г., а также международные патентные соглашения.

4.1.10 Требования по стандартизации и унификации

Для обработки Информации следует использовать СВТ, удовлетворяющие требованиям стандартов РФ по электромагнитной совместимости, по безопасности и эргономическим требованиям к средствам отображения информации, по санитарным нормам, предъявляемым к видеодисплейным терминалам ПЭВМ (ГОСТ 29216-91, ГОСТ Р 50948-96, ГОСТ Р 50949-96, ГОСТ Р 50923-96, СанПиН 2.2.2.542-96).

4.1.11 Требования по защите информации к организационным мерам защиты

Исполнителю необходимо разработать следующие проекты организационно-распорядительных документов, регламентирующих работу в ИС и СЗИ: (Из таблицы организационных средств ЛЗ 5)

- перечень сведений конфиденциального характера;
- инструкция администратора информационной безопасности;
- приказ о назначении лиц, ответственных за организацию обработки Информации и перечне мер по защите Информации;
- перечень Информации, подлежащих защите;
- приказ об утверждении мест хранения Информации;
- инструкция пользователей ИС;
- приказ о назначении комиссии по уничтожению Информации;
- порядок резервирования и восстановления работоспособности технических средств и ПО, баз данных и СЗИ;
- план внутренних проверок режима защиты Информации;
- приказ о вводе в эксплуатацию ИС;
- журнал учета носителей информации ИС;
- журнал учета мероприятий по контролю обеспечения защиты Информации;
- журнал учета обращений граждан-субъектов Информациоо выполнении их законных прав;
- правила обработки Информации без использования средств автоматизации;
- положение о разграничении прав доступа к обрабатываемым Информации;
- акт классификации ИС;
- инструкция по проведения антивирусного контроля в ИС;
- инструкция по организации парольной защиты;

- журнал периодического тестирования СЗИ;
- форма акта уничтожения документов, содержащих Информации;
- соглашение о неразглашении персональных данных;
- журнал учета средств защиты информации;
- журнал проведения инструктажа по информационной безопасности;
- инструкция пользователю по обеспечению безопасности при возникновении

внештатных ситуаций;

- приказ о перечне лиц, допущенных к обработке Информации;
- положение об обработке и защите Информации;
- план мероприятий по обеспечению безопасности Информации;
- модель угроз безопасности в ИС.

4.2 Требования к функциям, выполняемым системой (класс 2Б)

4.2.1 Подсистема контроля доступа

Должна осуществляться идентификация и проверка подлинности пользователя при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов.

4.2.2 Подсистема регистрации и учета

Должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС.

В параметрах регистрации указываются:

- дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;
- результат попытки входа: успешная или неуспешная (при НСД);
- должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку).

4.2.3 Подсистема обеспечения целостности

Должна быть обеспечена целостность программных средств СЗИ НСД, обрабатываемой информации, а также неизменность программной среды.

При этом:

- целостность СЗИ НСД проверяется при загрузке системы по наличию имен (идентификаторов) компонент СЗИ;
- целостность программной среды обеспечивается отсутствием в АС средств разработки и отладки программ во время обработки и (или) хранения защищаемой информации;
- должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая контроль доступа в помещения АС посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения АС и хранилище носителей информации, особенно в нерабочее время;
- должно проводиться периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест - программ, имитирующих попытки НСД;

- должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности.

4.2.4 Подсистема антивирусной безопасности

Должны использоваться сертифицированные в системе сертификации ФСТЭК России антивирусные средства защиты информации.

4.2.5 Подсистема межсетевой безопасности

МЭ должен обеспечивать:

- фильтрацию на сетевом уровне для каждого сетевого пакета независимо (решение о фильтрации принимается на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов);
- фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;
- фильтрацию с учетом входного и выходного сетевого интерфейса как средства проверки подлинности сетевых адресов;
- фильтрацию с учетом любых значимых полей сетевых пакетов;
- регистрацию и учет фильтруемых пакетов (в параметру регистрации включается адрес, время и результат фильтрации);
- идентификацию и аутентификацию администратора межсетевого экрана при его локальных запросах на доступ по идентификатору (коду) и паролю условно-постоянного действия;
- регистрацию входа (выхода) администратора МЭ в систему либо загрузки и инициализации системы и ее программного останова (регистрация выхода из системы не проводится в моменты аппаратурного отключения межсетевого экрана);
- регистрацию запуска программ и процессов (заданий, задач);
- контроль целостности своей программной и информационной части;
- восстановление свойств межсетевого экрана после сбоев и отказов оборудования;
- регламентное тестирование реализации правил фильтрации, процесса регистрации, процесса идентификации и аутентификации запросов, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления.

4.2.6 Подсистема обнаружения вторжений

Обнаружение вторжений проводится для информационных систем, подключенных к сетям международного информационного обмена, путем использования в составе информационной системы программных или программно-аппаратных средств (систем) обнаружения вторжений.

4.2.7 Подсистема анализа защищенности

Средства (системы) анализа защищенности должны обеспечивать возможность выявления уязвимостей, связанных с ошибками в конфигурации программного обеспечения информационной системы, которые могут быть использованы нарушителем для реализации атаки на систему.

4.3 Требования к видам обеспечения

Аппаратно-программные средства СЗИ должны быть обеспечены гарантийными обязательствами производителей предложенных средств, а также сертификатами соответствия средств защиты информации.

4.3.1 Требования к математическому обеспечению

Используемые математические методы и алгоритмы для шифрования/дешифрования данных, а также ПО, реализующее их, должны быть сертифицированы в системе сертификации криптографических средств ФСБ России и использовать алгоритмы согласно ГОСТ 28147-89.

4.3.2 Требования к информационному обеспечению

Состав, структура и способы организации данных в системе должны быть определены на этапе технического проектирования. Доступ к данным должен быть предоставлен только авторизованным пользователям с учетом их служебных полномочий, а также с учетом категории запрашиваемой информации. Технические средства, обеспечивающие хранение информации, должны использовать современные технологии, позволяющие обеспечить повышенную надежность хранения данных и оперативную замену оборудования. В состав системы должна входить специализированная подсистема резервного копирования и восстановления данных.

4.3.3 Требования к техническому обеспечению

Техническое обеспечение системы должно максимально и наиболее эффективным образом использовать существующие технические средства.

В состав комплекса должны входить следующие технические средства:

- серверы приложений;
- ЭВМ пользователей;
- ЭВМ администраторов.

4.3.4 Требования к организационному обеспечению

Должно быть назначено лицо, ответственное за обеспечение безопасности Информации при их обработке в ИС.

Должно быть назначено лицо, ответственное за администрирование СЗИ.

К работе с системой должны допускаться сотрудники, имеющие навыки работы на персональном компьютере, ознакомленные с правилами эксплуатации и прошедшие обучение работе с системой

Система должна иметь эргономичный интерфейс пользователя.

Взаимодействие системы и пользователя должно осуществляться на русском языке, за исключением системных сообщений, не подлежащих русификации;

При работе с интерфейсом пользователь должен быть ориентирован на работу с клавиатурой и манипулятором графической информации «мышь»;

Должно быть реализовано отображение на экране только тех возможностей, которые доступны конкретному пользователю в соответствии с его функциональной ролью в системе.

5. Состав и содержание работ по созданию системы

Раздел «Состав и содержание работ по созданию (развитию) системы» должен содержать перечень стадий и этапов работ по созданию системы в соответствии с ГОСТ 34.601. Применительно к разрабатываемой ИС перечень необходимых стадий и этапов работ представлен в таблице 10.

Таблица 10- Стадии и этапы работ по разработке СЗИ в ИС

Стадии	Этапы работ
1. Исследование и обоснование создания ИС	1.1 Разработка и оформление требований к системе (технико-экономическое обоснование, тактико-техническое задание, заявка)
	1.2 Разработка технического задания на ИС в целом и, при необходимости, частных ТЗ на подсистемы ИС
2. Технический проект. Рабочая документация	2.1 Разработка рабочей документации по информационному обеспечению
	2.2 Разработка рабочей документации по организационному обеспечению
	2.3 Разработка или адаптация программ и программной документации
3. Ввод в действие	3.4 Подготовка организации к вводу ИС в действие, обучение персонала пользователя
	3.5 Проведение опытной эксплуатации ИС
	3.6 Проведение приемочных испытаний (государственных, межведомственных или ведомственных)
	3.7 Приемка ИС в промышленную эксплуатацию

6. Порядок контроля и приемки системы

Контроль и приемка работ осуществляются на основании ЧТЗ. Содержание отчетных материалов согласуется на уровне специалистов Заказчика и Исполнителя в соответствии с ЧТЗ. Настоящее ЧТЗ может быть уточнено или изменено в процессе работы. Уточнения и изменения ЧТЗ производятся по согласованию сторон. Оформление изменений осуществляется выпуском дополнений, которые являются неотъемлемой частью настоящего ЧТЗ. Согласование и утверждение изменений производится в том же порядке и теми же должностными лицами, что и согласование и утверждение ЧТЗ. Замечания по отчетным материалам должны быть представлены Исполнителю с техническим обоснованием в письменной форме. Сроки приемки работ определяются календарными планами и сроками проведения соответствующих этапов в соответствии с техническими требованиями на создание СЗИ. Прием и сдача проводимых работ осуществляются совместной комиссией. Тестирование системы защиты должно проводиться без доступа к реальным данным ИС.

7. Требования к составу и содержанию работ по подготовке объекта автоматизации к вводу системы в действие

Реализация требований настоящего раздела не входит в перечень работ, выполняемых Исполнителем в рамках создания СЗИ. Данные требования должны быть реализованы Пользователем. На этапе ввода СЗИ должен быть определен перечень лиц, допущенных к обработке Информации, обрабатываемых в ИС. Должен быть определен перечень информации, классифицируемой как Информации. Компоненты СЗИ, в том числе телекоммуникационное оборудование, должны быть подключены к источникам бесперебойного питания.

Исполнителя работ необходимо наличие следующих действующих лицензий:

- ФСТЭК России на право осуществления деятельности по технической защите конфиденциальной информации;
- ФСТЭК России на проведение работ, связанных с созданием средств защиты информации;

- ФСБ России на право осуществлять разработки, производства шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем;
- ФСБ России на право осуществлять деятельность по распространению шифровальных средств;
- ФСБ России на право осуществлять деятельность по техническому обслуживанию шифровальных средств.

8. В разделе «Требования к документированию»

В соответствии с требованиями ГОСТ 34.201-89 «Виды, комплектность и обозначение документов при создании автоматизированных систем» на стадии разработки «Техническое задание» разрабатывается техническое (частное) техническое задание в соответствии с требованиями ГОСТ 34.602 «Техническое задание на создание АС» содержащее следующие разделы:

- общие сведения;
- назначение и цели создания (развития) системы;
- характеристика объектов автоматизации;
- требования к системе;
- состав и содержание работ по созданию системы;
- порядок контроля и приемки системы;
- требования к составу и содержанию работ по подготовке объекта автоматизации к вводу системы в действие;
- требования к документированию;
- источники разработки.

Оформление технического задания производится в соответствии с требованиями ГОСТ 2.105-95 «Общие требования к текстовым документам».

В ходе разработки должны быть подготовлены проекты ОРД по защите Информации предприятия в соответствии с приведенным перечнем (таблица 11).

Таблица 11 - Перечень разрабатываемых документов по этапам работ

Этапы работ	Вид разрабатываемых документов
Обследование существующей информационной системы	- аналитический отчет по проведению обследования информационной системы; - развернутый перечень Информации, обрабатываемых в ИС предприятия; - перечень сотрудников, допущенных к обработке Информации; - описание технологических процессов обработки информации в ИС.
Определение в существующей информационной системе подсистем, обрабатывающих персональные данные и уточнение их класса (при необходимости)	- акт классификации ИС.
Определение угроз безопасности, формирование модели угроз и модели нарушителя для ИС, формирование технических требований к СЗИ	- модель угроз безопасности Информации при их обработке в ИС, включая модель нарушителя; - техническое задание на создание системы защиты информации в ИС.
Проектирование СЗИ ИС	- технический проект на создание СЗИ; - пояснительная записка к техническому проекту СЗИ; - обоснование разработки СЗИ; - исходные данные на ИС; - ссылку на нормативные документы, с учетом которых будет разраба-

Этапы работ	Вид разрабатываемых документов
	тываться СЗИ и приниматься в эксплуатацию ИС; - конкретизированные мероприятия и требования к СЗИ (с учетом класса и требований руководящих документов ФСТЭК России и ФСБ России); - перечень предполагаемых к использованию сертифицированных средств защиты информации и схемы их внедрения; - состав, содержание и сроки проведения работ по этапам разработки и внедрения СЗИ; - пояснительную записку к техническому проекту; - ведомость технического проекта СЗИ; - программу и методику испытаний СЗИ; - список мероприятий по защите информации.
Разработка организационно-распорядительной документации	- (Из пункта 4.1.11) «Приказ об организации работ в Обществе по защите информации по требованиям информационной безопасности»: 1) Приложение. Положение об обработке персональных данных; 2) Приложение. Положение о структурном подразделении, отвечающем за защиту персональных данных; 3) Приложение. Положение об организации и проведении работ по обеспечению безопасности информации при их обработке в ИС. 4) Приложение. Перечень сотрудников и подразделений, допущенных к обработке персональных данных; 5) Приложение. Перечень информационных систем персональных данных. - «Приказ «О введении в действие документов, регламентирующих мероприятия по защите персональных данных, обрабатываемых в Обществе»: 1) Приложение. Комплект инструкций: «Инструкция по использованию антивирусных средств»; «Инструкция по организации парольной защиты»; «Инструкция по резервному копированию и восстановлению массивов информации»; «Инструкция по обеспечению безопасности и защиты информации от несанкционированного доступа»; «Инструкция по организации учета, использования и уничтожения машинных носителей данных, предназначенных для обработки и хранения персональных данных»; «Инструкция по обработке информации без использования средств автоматизации»; - «Инструкция администратора безопасности». 2) Приложение. Комплект регламентов: «Регламент о предоставлении прав доступа к персональным данным»; «Регламент реагирования на запросы субъектов персональных данных»; «Регламент обмена/выдачи информацией (к договорам между Обществом и сторонними организациями)». 3) Приложение. Комплект журналов: «Журнал инструктажа пользователей и обслуживающего персонала Общества»; «Журнал учета мероприятий по защите информации в Обществе»; «Журнал учета и выдачи машинных носителей данных, содержащих конфиденциальную информацию Общества»; «Журнал учета ремонтно-восстановительных работ на основных технических средствах Общества»; «Журнал учета выдачи информации на бумажных носителях третьим лицам»; «Журнал учета выдачи персональных ключей».

9. Источники разработки

Перечень документов и информационных материалов на основании которых разрабатывается техническое задание:

1 Конституция РФ.

2 Гражданский кодекс РФ.

3 Трудовой кодекс РФ.

4 ФЗ от 02.05.2006г. № 59-ФЗ «О порядке рассмотрения обращений граждан РФ».

5 ФЗ от 27.07.2006 N 149-ФЗ (ред. от 02.07.2013) «Об информации, информационных технологиях и о защите информации N 149-ФЗ.

6 Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (с изменениями от 25 июля 2011 г.).

7 ПП РФ от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

4. Оборудование и материалы (перечень используемого оборудования)

Состав раздаточного материала:

- коллекция макетов с конфиденциальными документами;
- коллекция документов для выявления конфиденциальных документов фирмы;
- карточка индивидуального ситуационного варианта к заданиям работы;
- учетные формы;
- рабочая тетрадь;
- перечень конфиденциальных документов (сведений) негосударственной фирмы;
- операционная схема;
- внутренняя опись документов, находящихся у исполнителя (студента);
- практикум.

5. Указания по технике безопасности

- ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории;
- убедиться в целостности электрических розеток и разъемов. В лаборатории необходимо быть в сменной обуви;
- включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

6. Задания

- выполнение операций процедуры приема пакетов;
- составление акта о повреждении или нарушении в оформлении пакета;
- выполнение операций процедуры учета пакетов;
- выполнение операций процедуры распределения и вскрытия пакетов;
- выполнение операций процедуры выделения конфиденциальных документов из документов входного потока.

7. Содержание отчета

По результатам выполнения практического занятия студенты оформляют и защищают в индивидуальном порядке в форме беседы результаты выполнения заданий.

Результатом работы является:

- журнал учёта входящих пакетов;
- журнал учёта входящих документов;

- акты по замечаниям.

8. Контрольные вопросы и тестовые задания

1. Какое назначение имеет стадия приема, первичной обработки, предварительного рассмотрения и распределения поступивших документов?
2. Каким угрозам подвергается документ в процессе его доставки адресату и приема адресатом?
3. Какие задачи защиты информации должны быть решены при выполнении процедур и операций данной стадии?
4. Какое назначение имеет каждая из выполняемых процедур?
5. Как осуществляется прием пакетов от курьеров и из почтового отделения связи?
6. Как осуществляется прием и учет пакетов, поступивших во внерабочее время?
7. Как осуществляется прием пакетов, имеющих повреждения или нарушения в оформлении?
8. Кому и как передаются пакеты, не подлежащие вскрытию?
9. Как проверяется комплектность поступивших документов?
10. Как осуществляется пересылка ошибочно присланных документов?
11. Как происходит выделение документов, содержащих негосударственную тайну, из общего потока открытых документов?

9. Список литературы

Основная литература:

1. Аверченков, В.И. Защита персональных данных в организации [Электронный ресурс] / В.И. Аверченков, М.Ю. Рытов, Т.Р. Гайнулин. - 2-е изд., стер. - М. : Флинта, 2017. - 124 с. - ISBN 978-5-9765-1273-3. - URL: <http://biblioclub.ru/index.php?page=book&id=93260>
2. Минин, И.В. Защита конфиденциальной информации при электронном документообороте: учебное пособие [Электронный ресурс] / И.В. Минин, О.В. Минин. - Новосибирск: НГТУ, 2018. - 20 с. - ISBN 978-5-7782-1829-1. - URL: <http://biblioclub.ru/index.php?page=book&id=228779>

Дополнительная литература:

1. Лузина, Т.В. Основы документооборота в таможенных органах : [16+] / Т.В. Лузина, С.С. Решетникова ; Министерство науки и образования РФ, ФГБОУ ВПО Тюменский государственный университет, Институт дистанционного образования, Институт психологии и др. – Тюмень : Издательство Тюменского государственного университета, 2016. – 524 с. : ил. – Режим доступа: по подписке. – URL: <http://biblioclub.ru/index.php?page=book&id=567333>

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 «Защищенный электронный документооборот»

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

61

СОДЕРЖАНИЕ

[Введение](#)

[Общая характеристика самостоятельной работы студента](#)

[Технологическая карта самостоятельной работы студента](#)

[Порядок выполнения самостоятельной работы](#)

[Список рекомендуемой литературы](#)

ВВЕДЕНИЕ

Целью изучения дисциплины «Защищённый электронный документооборот» является формирование у студентов набора профессиональных компетенций по направлению подготовки 10.03.01 Информационная безопасность позволяющих обучаемым администрировать подсистемы информационной безопасности объекта защиты, оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов, организовать контроль защищенности объекта в соответствии с нормативными документами.

Задачи освоения дисциплины:

- формирование способности обучаемых разрабатывать организационно-распорядительные документы по защите информации в автоматизированных системах.

1. Общая характеристика самостоятельной работы студента

Самостоятельная работа включает те разделы курса, которые не получили достаточного освещения на лекциях по причине ограниченности лекционного времени и большого объема изучаемого материала.

Методическое обеспечение самостоятельной работы по дисциплине состоит из:

- 1) Определения учебных вопросов, которые студенты должны изучить самостоятельно;
- 2) Подбора необходимой учебной литературы, обязательной для проработки и изучения;
- 3) Поиска дополнительной научной литературы, к которой студенты могут обращаться по желанию, если у них возникает интерес в данной теме;
- 4) Определения контрольных вопросов, позволяющих студентам самостоятельно проверить качество полученных знаний;
- 5) Организации консультаций преподавателя со студентами для разъяснения вопросов, вызвавших у обучающихся затруднения при самостоятельном освоении учебного материала.

Самостоятельная работа студента – это особым образом организованная деятельность, включающая в свою структуру такие компоненты, как:

- уяснение цели и поставленной учебной задачи;
- четкое и системное планирование самостоятельной работы;
- поиск необходимой учебной и научной информации;
- освоение собственной информации и ее логическая переработка;
- использование методов исследовательской, научно-исследовательской работы для решения поставленных задач;
- выработка собственной позиции по поводу полученной задачи;
- представление, обоснование и защита полученного решения;
- проведение самоанализа и самоконтроля

К основным видам самостоятельной работы студентов относится:

- работа с понятийным аппаратом;
- конспектирование первоисточников;
- проектирование фрагментов исследовательской деятельности;
- подготовка доклада по теме.

Контроль знаний студентов включает формы текущего и итогового контроля. Текущий контроль осуществляется в процессе изучения курса и включает в себя оценку работы студентов на практических занятиях (круглый стол, собеседование, групповые научные проекты, тестирование), а также подготовку домашнего задания.

2. Технологическая карта самостоятельной работы студента

Коды реализуемых компетенций	Вид деятельности студентов	Итоговый продукт самостоятельной работы	Средства и технологии оценки	Объем часов, в том числе		
				СРС	Контактная работа с преподавателем	Всего
6 семестр						
ПК-4 ИД-1 ПК-4 ИД-2	Подготовка к практическому занятию	Отчёт по практическому занятию	Собеседование	25.00	2.00	27.00
ПК-4 ИД-1 ПК-4 ИД-2	Подготовка к докладу	Отчет	Собеседование	25.00	2.00	27.00
ПК-4 ИД-1 ПК-4 ИД-2	Подготовка к лекции	Конспект лекций	Собеседование	24.00	2.00	26.00
Итого за 6 семестр				74.00	6.00	80.00
Итого				74.00	6.00	80.00

3. Порядок выполнения самостоятельной работы

3.1 Методические рекомендации по изучению теоретического материала

Комплексное изучение предлагаемой студентам учебной дисциплины «Защищенный электронный документооборот» предполагает овладение материалами лекций, учебников, программы, творческую работу студентов в ходе проведения лабораторных работ, 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 лабораторным работам

Работа с конспектом лекций

Просмотрите конспект сразу после занятий. Отметьте материал конспекта лекций, который вызывает затруднения для понимания. Попробуйте 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 практического занятия по дисциплине «Защищенный электронный документооборот»

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

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

Целью практического занятия является:

- закрепление методов приложения теории к решению практических задач 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 материала, 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.

- **Способ «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.

- **Схема 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 наискратчайшее 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 требуют 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.

Список рекомендуемой литературы

1. Перечень основной литературы:

1. Анацкая, А. Г. Защита электронного документооборота : учебное пособие / А. Г. Анацкая. — Омск : СиБАДИ, 2019. — 87 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/149493>

2. Кузнецова, И. В. Конфиденциальное делопроизводство и защищенный электронный документооборот : учебное пособие для бакалавров / И. В. Кузнецова, Г. А. Хачатрян. — Москва : Ай Пи Ар Медиа, 2020. — 192 с. — ISBN 978-5-4497-0588-4. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/97083.html>

2. Перечень дополнительной литературы:

Защищённый электронный документооборот: лабораторный практикум: практикум / авт.-сост. С. В. Говорова ; Министерство образования и науки Российской Федерации ; Федеральное государственное автономное образовательное учреждение высшего образования «Северо-Кавказский федеральный университет». - Ставрополь : СКФУ, 2017. - 223 с. : ил. - <http://biblioclub.ru/>. - Библиогр. в кн.

3 Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине (модулю)

1. Методические рекомендации по организации и проведению самостоятельной работы студентов по учебной дисциплине «Защищённый электронный документооборот».

2. Методические рекомендации по выполнению практических работ по учебной дисциплине «Защищённый электронный документооборот».

4 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

1. Сайт ФСТЭК России // Федеральная служба по техническому и экспортному контролю: [сайт]. — URL: <https://fstec.ru/> (дата обращения: 04.02.2023).

2. Сайт Роскомнадзора // Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций: [сайт]. — URL: <https://rkn.gov.ru/> (дата обращения: 04.02.2023).

3. Сайт ФСБ России // Федеральная служба безопасности Российской Федерации: [сайт]. — URL: <http://fsb.ru/> (дата обращения: 04.02.2023).

4. «Лань». Электронно-библиотечная система // Консорциум сетевых электронных библиотек ЭБС «Лань»: [сайт]. — URL: <https://e.lanbook.com/> (дата обращения: 04.02.2023).

5. Библиоклуб.РУ // ЭБС «Университетская библиотека ОНЛАЙН»: [сайт]. — URL: <https://www.biblioclub.ru/> (дата обращения: 04.02.2023).

6. Цифровой образовательный ресурс IPR SMART // ЭБС IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/> (дата обращения: 04.02.2023).

7. Znanium.com. // ЭБС Znanium: [сайт]. — URL: <https://znanium.com/> (дата обращения: 04.02.2023).

8. ЭБС «Юрайт». // Юрайт. Образовательная платформа: [сайт]. — URL: <http://www.biblio-online.ru> (дата обращения: 04.02.2023).

Поисковые интернет-системы Яндекс, Rambler, Google и др.

5 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем

При чтении лекций используется компьютерная техника, демонстрация презентационных мультимедийных материалов, программное обеспечение для проведения веб-конференции.

При проведении практических занятий используются информационно-справочные системы, интерактивная доска для совместной работы команд и сервис для совместной работы.

При реализации дисциплины с применением электронного обучения и дистанционных образовательных технологий материал может размещаться в системе электронного обучения. Для обеспечения удаленного доступа, в том числе в случае применения электронного обучения, дистанционных образовательных технологий, используется программное обеспечение для проведения веб-конференции, виртуализации рабочих столов и система электронного обучения.

6 Информационные справочные системы

Информационно-справочные и информационно-правовые системы, используемые при изучении дисциплины:

1. Государственный реестр сертифицированных средств защиты информации // Федеральная служба по техническому и экспортному контролю: [сайт]. — URL: <https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi00>
2. Реестр аккредитованных ФСТЭК России органов по сертификации и испытательных лабораторий // Федеральная служба по техническому и экспортному контролю: [сайт]. — URL: <https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/588-perechen-isytyatelnykh-laboratorij-n-ross-ru-0001-01bi00>
3. Банк данных угроз безопасности информации. // Федеральная служба по техническому и экспортному контролю: [сайт]. — URL: <https://bdu.fstec.ru/threat>
4. База данных общеизвестных уязвимостей информационной безопасности // Common Vulnerabilities and Exposures: [сайт]. — URL: <https://cve.mitre.org/>
5. MITRE ATT&CK® - База знаний о тактике и методах противника // Common Vulnerabilities and Exposures : [сайт]. — URL: <https://attack.mitre.org/>
6. Государственная система распространения правовых актов в электронном виде // Официальный интернет-портал правовой информации: [сайт]. — URL: <http://www.pravo.gov.ru/>
7. «КонсультантПлюс» (перечень информационных систем). // «КонсультантПлюс»: [сайт]. — URL: <http://www.consultant.ru/>
8. «ГАРАНТ» (комплект «ГАРАНТ-Максимум»). // ГАРАНТ.РУ Информационно-правовой портал: [сайт]. — URL: <https://www.garant.ru/>

7 Программное обеспечение:

1. Интерактивная онлайн-доска для совместной работы команд. <https://miro.com/ru/>
2. Открытое программное обеспечение для проведения веб-конференции BigBlueButton <https://bigbluebutton.org/>
3. Платформа Scantukan <https://www.scantukan.ru/>
4. Платформа для создания онлайн-курсов LMS Moodle. <https://moodle.org/?lang=ru>
5. Программное обеспечение создания презентаций Microsoft PowerPoint. <https://www.microsoft.com/ru-ru/microsoft-365/powerpoint>
6. Сервис для совместной работы Notion <https://www.notion.so/>

