Санкт-Петербургское государственное бюджетное
профессиональное образовательное учреждение
«Академия управления городской средой, градостроительства и печати»

УТВЕРЖДАЮ
Заместитель директора
по учебно-производственной работе
_____ О.В. Фомичева
«26» декабря 2023 г.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ
по выполнению практических работ
по МДК.01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении
ПМ.01 ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ (ИНФОРМАЦИОННЫХ) СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

для специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Санкт-Петербург
2023 г.

Методические рекомендации рассмотрены на заседании методического совета СПб ГБПОУ «АУГСГиП»

Протокол № 2 от «29» ноября 2023 г.

Методические рекомендации одобрены на заседании цикловой комиссии общетехнических дисциплин и компьютерных технологий

Протокол № 4 от «21» ноября 2023 г.

Председатель цикловой комиссии: Караченцева М.С. _____

Разработчики: преподаватели СПб ГБПОУ «АУГСГиП»

С О Д Е Р Ж А Н И Е

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Рабочая тетрадь для выполнения практических работ предназначена для организации работы на практических занятиях по темам 4.1-4.14 МДК. МДК.01.04. «Эксплуатация автоматизированных (информационных) систем в защищенном исполнении» ПМ.01 «Эксплуатация автоматизированных (информационных) систем в защищённом исполнении» являющегося важной составной частью в системе подготовки специалистов среднего профессионального образования по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем».

Практические занятия являются неотъемлемым этапом изучения тем 4.1-4.14 МДК. МДК.01.04. «Эксплуатация автоматизированных (информационных) систем в защищенном исполнении» и проводятся с целью:

формирования практических умений в соответствии с требованиями к уровню подготовки обучающихся, установленными рабочей программой учебной дисциплины;

обобщения, систематизации, углубления, закрепления полученных теоретических знаний;

готовности использовать теоретические знания на практике.

Практические занятия по темам 4.1-4.14 МДК. МДК.01.04. «Эксплуатация автоматизированных (информационных) систем в защищенном исполнении» способствуют формированию следующих общих и профессиональных компетенций:

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.

ОК 09. Использовать информационные технологии в профессиональной деятельности.

ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.

ПК 1.2. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.

ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.

В Рабочей тетради предлагаются к выполнению практические работы, предусмотренные рабочей программой ПМ.01 «Эксплуатация автоматизированных (информационных) систем в защищённом исполнении».

При разработке содержания практических работ учитывался уровень сложности освоения студентами соответствующей темы, общих и профессиональных компетенций, на формирование которых направлен ПМ.01.

Выполнение практических работ в рамках тем 4.1-4.14 МДК. МДК.01.04. «Эксплуатация автоматизированных (информационных) систем в защищенном исполнении» ПМ.01 «Эксплуатация автоматизированных (информационных) систем в защищённом исполнении» позволяет освоить комплекс работ эксплуатации автоматизированных систем: их установку, настройку и поддержку.

Рабочая тетрадь для выполнения практических заданий по темам 4.1-4.14 МДК. МДК.01.04. «Эксплуатация автоматизированных (информационных) систем в защищенном исполнении» ПМ.01 «Эксплуатация автоматизированных (информационных) систем в защищённом исполнении» имеет практическую направленность и значимость. Формируемые в процессе их проведения умения могут быть использованы студентами в будущей профессиональной деятельности.

Рабочая тетрадь предназначена для студентов колледжа, изучающих темы 4.1-4.14 МДК. МДК.01.04. «Эксплуатация автоматизированных (информационных) систем в защищенном исполнении» ПМ.01 «Эксплуатация автоматизированных (информационных) систем в защищённом исполнении» и может использоваться как на учебных занятиях, которые проводятся под руководством преподавателя, так и для самостоятельного выполнения практических работ, предусмотренных рабочей программой во внеаудиторное время.

Практические занятия проводятся в учебном кабинете, не менее двух академических часов, обязательным этапом является самостоятельная деятельность студентов.

Практические занятия в соответствии с требованием ФГОС включают такой обязательный элемент, как использование персонального компьютера.

Оценки за выполнение практических работ выставляются по пятибалльной системе. Оценки за практические работы являются обязательными текущими оценками по темам 4.1-4.14 МДК. МДК.01.04. «Эксплуатация автоматизированных (информационных) систем в защищенном исполнении» ПМ.01 «Эксплуатация автоматизированных (информационных) систем в защищённом исполнении» и выставляются в журнале теоретического обучения.

1 ПЕРЕЧЕНЬ ПРАКТИЧЕСКИХ РАБОТ ПО ТЕМАМ 4.1-4.14 МДК. МДК.01.04. «ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ (ИНФОРМАЦИОННЫХ) СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ» ПМ.01 «ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ (ИНФОРМАЦИОННЫХ) СИСТЕМ В ЗАЩИЩЁННОМ ИСПОЛНЕНИИ»

№ раздела, темы	Формируемые ОК и ПК	Тема практического занятия	Кол-во часов
Тема 4.3. Угрозы безопасности информации в автоматизированных системах	ОК 1, ОК 10 ПК 1.2 З6 У1	**Практическая работа № 1.** Категорирование информационных ресурсов	2
		Практическая работа № 2. Анализ угроз безопасности информации	2
		Практическая работа № 3. Построение модели угроз	2
Тема 4.7. Особенности разработки информационных систем персональных данных	ОК 1, ОК 10 ПК 1.2 З6 У1	**Практическая работа №4.** Определения уровня защищенности ИСПДн и выбор мер по обеспечению безопасности ПДн.	2
Тема 4.12. СЗИ от НСД	У3, У4 ПК 1.2	**Практическая работа №5.** Установка и настройка СЗИ от НСД	2
	У3, У4 ПК 1.2	**Практическая работа №6.** Защита входа в систему (идентификация и аутентификация пользователей)	2
	У3, У4 ПК 1.2	**Практическая работа №7.** Разграничение доступа к устройствам	2
	У3, У4 ПК 1.2	**Практическая работа №8.** Управление доступом	2
Тема 4.14. Документация на защищаемую автоматизированную систему	ОК 1, ОК 10 ПК 1.2 З6 У1	**Практическая работа №9.** Оформление основных эксплуатационных документов на автоматизированную систему.	2

2 ОПИСАНИЕ ПОРЯДКА ВЫПОЛНЕНИЯ ПРАКТИЧЕСКИХ РАБОТ

2.1. Практическая работа № 1. Категорирование информационных ресурсов

Цели: изучить правила категорирования информационных ресурсов.

Теоретические вопросы

1. Категорирование защищаемых ресурсов.
2. Упрощенный алгоритм оценки защищенности объекта информатизации.
3. Правила категорирования критичности информационного ресурса.
4. Цели категорирования информационных ресурсов.
5. Категории конфиденциальности защищаемой информации.
6. Требуемые степени доступности функциональных задач.

Задание 1. Изучите предложенную классификацию информационных ресурсов:

Государственные (национальные) информационные ресурсы Государственные информационные ресурсы - информационные ресурсы, полученные и оплаченные из федерального бюджета.	1)федеральные ресурсы; 2) информационные ресурсы, находящиеся в совместном ведении Российской Федерации и субъектов РФ: • библиотечная сеть России; • архивный фонд Российской Федерации; • государственная система статистики; • государственная система научно-технической информации 3) информационные ресурсы субъектов РФ.
Информационные ресурсы организаций и предприятий Информационные ресурсы предприятий – информационные ресурсы, созданные или накопленные в организациях и на предприятиях.	• центры-генераторы; • центры распределения; • информационные агентства; • базы данных.
Персональные информационные ресурсы Персональные информационные ресурсы – информационные ресурсы, созданные и управляемые каким-либо человеком и содержащие данные, относящиеся к его личной деятельности.	

Определите вид следующих информационных ресурсов в соответствии с даннойклассификацией:

1. http://portal.gersen.ru
2. http://school-collection.edu.ru
3. http://fcior.edu.ru
4. http://e-lib.gasu.ru
5. http://books.ifmo.ru
6. http://window.edu.ru
7. http://ivanurgant.com/
8. http://www.schwarzenegger.com/
9. http://zim-angel.ucoz.ru/
10. http://www.educom.ru/ru/works/

Задание 2. Раскройте суть основных параметров информационного ресурса:

№	**Параметр информационного ресурса**	**Характеристика параметра**
1.	**Содержание**	
2.	**Охват**	
3.	**Время**	
4.	**Источник**	
5.	**Качество**	
6.	**Соответствие потребностям**	
7.	**Способ фиксации**	
8.	**Язык**	
9.	**Стоимость**	

Задание 3. Опишите правила категорирования критичности информационного ресурса.

Задание 4. Приведите категории конфиденциальности, целостности и доступностиинформационных ресурсов.

Задание 5. Охарактеризуйте информационные ресурсы заданного предприятия. Заполнитетаблицу:

Наименование информационного ресурса (информации)	Категория конфиден-циальности (В/Н/-) и вид тайны (БТ/КТ/ДСП)	Категория целостности (В/Н/-)	Размещение ресурса (АРМ, устройство, каталог, файл)	Ответствен-ный за определение требований к защищен-ности ресурса
1				
2				
3				
4				
…				
…				

2.2. Практическая работа № 2 Анализ угроз безопасности информации

Задание 1. Охарактеризуйте виды угроз информационной безопасности. Приведите примеры:

Нарушение физической целостности	
Нарушение логической целостности	
Нарушение содержания информации	
Нарушение конфиденциальности	
Нарушение прав собственности наинформации	

Задание 2. Заполните таблицу «Характер происхождения угроз информационнойбезопасности»:

Умышленные факторы	Естественные факторы

Задание 3. Заполните таблицу «Предпосылки появления угроз информационнойбезопасности»:

Объективные предпосылки	Субъективные предпосылки

Задание 4. Проведите анализ защищенности объекта защиты информации по следующимразделам:

1. Виды возможных угроз
2. Характер происхождения угроз
3. Классы каналов несанкционированного получения информации
4. Источники появления угроз
5. Причины нарушения целостности информации
6. Потенциально возможные злоумышленные действия

7. Класс защищенности автоматизированной системы

Приоритет	Виды угроз	Субъекты угроз			
		Стихия	Нарушитель	Злоумышленник	
				На территории	Вне территории
1	Травмы и гибель людей	+	+	+	+
2	Повреждение оборудование, техники	+	+	+	+
3	Повреждение систем жизнеобеспечения	+	+	+	+
4	Несанкционированное изменение технологического процесса		+	+	
5	Использование нерегламентированных технических и программных средств		+	+	
6	Дезорганизация функционирования предприятия	+		+	
7	Хищение материальных ценностей			+	
8	Уничтожение или перехват данных путем хищения носителей информации			+	
9	Устное разглашение конфиденциальной информации		+		
10	Несанкционированный съем информации			+	+
11	Нарушение правил эксплуатации средств защиты		+	+	

2.3. Практическая работа № 3. Построение модели угроз

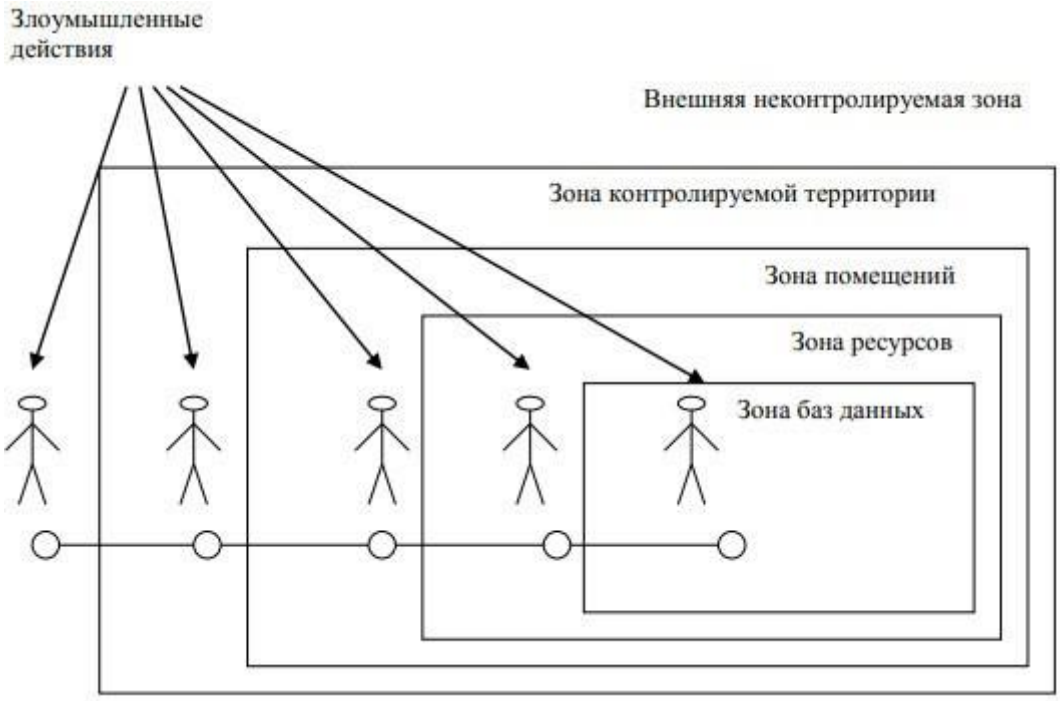
Цель: анализ и построение модели информационной безопасности.

Теоретические вопросы

1. Классы каналов несанкционированного получения информации.
2. Моделирование угроз безопасности информации.
3. Модель нарушителя информационной безопасности.

Задание 1. Приведите примеры каналов несанкционированного получения информации.

Задание 2. Структурированная схема потенциально возможных злоумышленных действий вавтоматизированных системах обработки данных:



Определите выделенные зоны для заданного объекта.

Задание 3. Проведите анализ потенциальных каналов утечки на указанном объекте. Составьтеперечень каналов утечки информации на защищаемом объекте с указанием места расположенияпо образцу:

Каналы утечки информации с объекта защиты			Место расположения
1.	Оптический канал	Окно со стороны проспекта	каб. №1
		Окно со стороны проспекта	каб. №2
		Окно со стороны проспекта	каб. №3
2.	Радиоэлектронный канал	Стоянка автотранспорта на просп.	указать
		Система часофикации	указать
		Телефон	указать
		Розетки	указать
		ПЭВМ	указать
		Воздушная линия электропередачи	указать
		Система оповещения	указать
		Система пожарной сигнализации	указать
3.	Акустический канал	Теплопровод подземный	указать
		Водопровод подземный	указать
		Стены помещения	указать
		Батареи	указать
		Окна контролируемого помещения	указать
4.	Материально-вещественный канал	Документы на бумажных носителях	указать
		Персонал предприятия	указать
		Производственные отходы	указать

Задание 4. Постройте модель угроз защищаемого объекта:

№ элемента	Цена информации	Путь проникновения	Оценка реальности	Величина угрозы	Ранг угрозы

2.4. Практическая работа № 4 Определения уровня защищенности ИСПДн и выбор мер по обеспечению безопасности ПДн.

Цели: научиться определять уровень защищенности информационных систем персо-

нальныхданных и выбирать меры по обеспечению безопасности персональных данных.

Теоретические вопросы

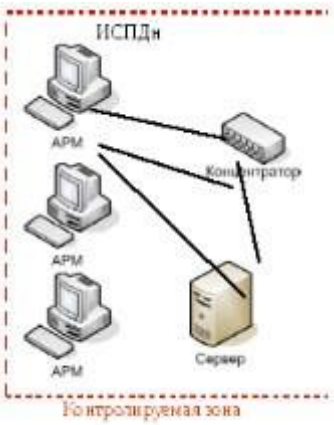
1. Общие требования по защите персональных данных.
2. Состав и содержание организационных и технических мер по защите информационныхсистем персональных данных.
3. Порядок выбора мер по обеспечению безопасности персональных данных.
4. Требования по защите персональных данных, в соответствии с уровнем защищенности.

Задание 1. Оцените характеристики ИСПДн, обусловливающие возникновение угрозбезопасности ПДн:

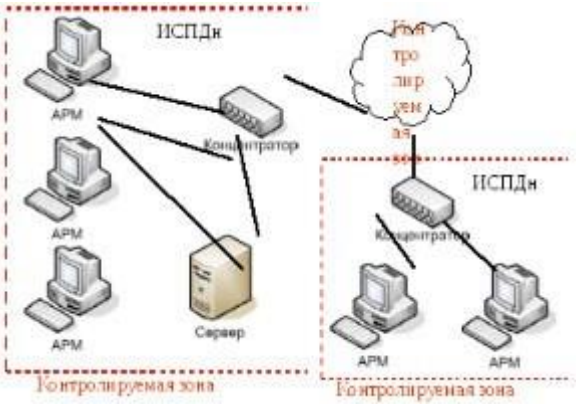
1) структура ИСПДн:

автономные ИСПДн АРМ:

локальные ИСПДн:



распределенные ИСПДн):



категория обрабатываемых в ИСПДн персональных данных:

ИСПДн-С - информационная система, обрабатывающая специальные категории персональных данных, если в ней обрабатываются персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных;

ИСПДн–Б - информационная система, обрабатывающая биометрические персональные данные, если в ней обрабатываются сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных, и не обрабатываются сведения, относящиеся к специальным категориям персональных данных;

ИСПДн-И - информационная система, обрабатывающая иные категории персональных данных, если в ней не обрабатываются персональные данные специальные, общедоступные и биометрические;

ИСПДн-О - информационная система, обрабатывающая общедоступные персональные данные, если в ней обрабатываются персональные данные субъектов персональных данных, полученные только из общедоступных источников персональных данных, созданных в соответствии со статьей 8 Федерального закона "О персональных данных".

Объем обрабатываемых в ИСПДн персональных данных:

менее чем 100 000 субъектов;

более чем 100 000 субъектов.

наличие подключений ИСПДн к сетям связи общего пользования/сетям МИО: не имеющие подключение;

имеющие подключение.

характеристики подсистемы безопасности ИСПДн;

режимы обработки персональных данных:

однопользовательские ИСПДн; многопользовательские ИСПДН.

режимы разграничения прав доступа пользователей ИСПДн:

с разграничением доступа; без разграничения доступа;

условия размещения технических средств ИСПДн:

в пределах контролируемой зоны; вне контролируемой зоны.

по территориальному размещению:

распределенная ИСПДн, которая охватывает несколько областей, краев, округов или государство в целом;

городская ИСПДн, охватывающая не более одного населенного пункта (города, поселка); корпоративная распределенная ИСПДн, охватывающая многие подразделения одной

организации;

локальная (кампусная) ИСПДн, развернутая в пределах нескольких близко расположенных зданий;

локальная ИСПДн, развернутая в пределах одного здания.

Задание 2. Изучите документ «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных». ФСТЭК России от 15.02.2008 г.

Задание 3. Изучите категории нарушителей, описанные в документе ФСТЭК России «Базовая модель». Для конкретной информационной системы определите перечень вероятных нарушителей ИСПДн с учетом всех исключений.

Категория нарушителя	Перечень лиц	Описание категории нарушителя
1	Работники предприятия,не имеющие санкционированного доступа к ИСПДн	имеет доступ к фрагментам информации, содержащей ПДн и распространяющейся по внутренним каналам связиИСПДн; • располагает фрагментами информации о топологииИСПДн (коммуникационной части подсети) и об используемых коммуникационных протоколах и их сервисах; располагает именами и возможностью выявленияпаролей зарегистрированных пользователей; изменяет конфигурацию технических средств ИСПДн,вносит в нее программно-аппаратные закладки и обеспечивать съем информации, используя непосредственное подключение к техническим средствамИСПДн.
2	Пользователи ИСПДн	• обладает всеми возможностями лиц первой категории; • знает, по меньшей мере, одно легальное имя доступа; обладает всеми необходимыми атрибутами (например,паролем), обеспечивающими доступ к некоторому подмножеству ПДн; располагает конфиденциальными данными, к которымимеет доступ.
3	Администраторы ППО ИСПДн	Обладает всеми возможностями лиц первой и второйкатегорий; располагает информацией о топологии ИСПДн на базе локальной и (или) распределенной информационной системы, через которую осуществляется доступ, и о составетехнических средств ИСПДн; имеет возможность прямого (физического) доступа кфрагментам технических средств ИСПДн.

4	Администраторы локальной сети	Обладает всеми возможностями лиц предыдущихкатегорий; обладает полной информацией о системном и прикладном программном обеспечении, используемом всегменте (фрагменте) ИСПДн; обладает полной информацией о технических средствахи конфигурации сегмента (фрагмента) ИСПДн; имеет доступ к средствам защиты информации и протоколирования, а также к отдельным элементам, используемым в сегменте (фрагменте) ИСПДн; имеет доступ ко всем техническим средствам сегмента(фрагмента) ИСПДн; обладает правами конфигурирования и административной настройки некоторого подмножестватехнических средств сегмента (фрагмента) ИСПДн.
5	Зарегистрированные пользователи с	Обладает всеми возможностями лиц предыдущихкатегорий;
	полномочиями системного администратора ИСПДн Администраторы информационной безопасности	обладает полной информацией о системном иприкладном программном обеспечении ИСПДн; обладает полной информацией о технических средствахи конфигурации ИСПДн; имеет доступ ко всем техническим средствам обработкиинформации и данным ИСПДн; обладает правами конфигурирования и административной настройки технических средств ИСПДн
6	Работники сторонних организаций, обеспечивающие поставку, сопровождениеи ремонт технических средств ИСПДн	обладает всеми возможностями лиц предыдущихкатегорий; • обладает полной информацией об ИСПДн; имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн; не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных(инспекционных).
7	Программисты- разработчики (поставщики) прикладного программного обеспечения и лица, обеспечивающие егосопровождение на защищаемом объекте	обладает информацией об алгоритмах и программахобработки информации на ИСПДн; обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в программное обеспечение ИСПДнна стадии ее разработки, внедрения и сопровождения; может располагать любыми фрагментами информации отопологии ИСПДн и технических средствах обработки и защиты ПДн, обрабатываемых в ИСПДн.

8	Разработчики и лица, обеспечивающие поставку, сопровождениеи ремонт технических средств на ИСПДн	обладает возможностями внесения закладок в технические средства ИСПДн на стадии их разработки,внедрения и сопровождения; может располагать любыми фрагментами информации отопологии ИСПДн и технических средствах обработки и защиты информации в ИСПДн.

Задание 4. Изучите модели безопасности, описанные в документе ФСТЭК России «Базовая модель». Составьте перечень всех возможных угроз по документу ФСТЭК России «Базовая модель».

Перечень всех возможных угроз безопасности ПДн

Возможные угрозы безопасности ПДн
1. Угрозы от утечки по техническим каналам
1.1. Угрозы утечки акустической информации
1.2. Угрозы утечки видовой информации
1.3. Угрозы утечки информации по каналам ПЭМИН
2. Угрозы несанкционированного доступа к информации
2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информациипутем физического доступа к элементам ИСПДн
2.1.1. Кража ПЭВМ
2.1.2. Кража носителей информации
2.1.3. Кража ключей и атрибутов доступа
2.1.4. Кражи, модификации, уничтожения информации
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи
2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте,уничтожении) узлов ПЭВМ
2.1.7. Несанкционированное отключение средств защиты
2.2. Угрозы хищения, несанкционированной модификации или блокирования информации засчет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)
2.2.1. Действия вредоносных программ (вирусов)
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональныхданных
2.2.3. Установка ПО, не связанного с исполнением служебных обязанностей
2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и систем защиты ПДн в ее составе из-за сбоев в программномобеспечении, а также от сбоев аппаратуры, из-за ненадежности элементов, сбоев электропитания и стихийного (ударов молний, пожаров, наводнений и т. п.) характера
2.3.1. Утрата ключей и атрибутов доступа
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками
2.3.3. Непреднамеренное отключение средств защиты
2.3.4. Выход из строя аппаратно-программных средств

2.3.5. Сбой системы электроснабжения
2.3.6. Стихийное бедствие
2.4. Угрозы преднамеренных действий внутренних нарушителей
2.4.1. Доступ к информации, копирование, модификация, уничтожение, лицами, недопущенными к ее обработке
2.4.2. Разглашение информации, копирование, модификация, уничтожение сотрудниками,допущенными к ее обработке
2.5.Угрозы несанкционированного доступа по каналам связи
2.5.1.Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн ипринимаемой из внешних сетей информации:
2.5.1.1. Перехват за переделами с контролируемой зоны
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями
2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями.
2.5.2.Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытыхпортов и служб, открытых соединений и др.
2.5.3.Угрозы выявления паролей по сети
2.5.4.Угрозы навязывание ложного маршрута сети
2.5.5.Угрозы подмены доверенного объекта в сети
2.5.6.Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях
2.5.7.Угрозы типа «Отказ в обслуживании»
2.5.8.Угрозы удаленного запуска приложений
2.5.9.Угрозы внедрения по сети вредоносных программ

Задание 5. Изучите документ «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», разработанный ФСТЭК России.

Задание 6. Заполните таблицу, проставив в виде «+» показатели высокого, среднего и низкого уровня защищённости для всех технических и эксплуатационных характеристик ИСПДн. Например,:

Показатели исходной защищенности ИСПДн

Технические и эксплуатационныехарактеристики ИСПДн	**Уровень защищенности**		
	Высокий	**Средний**	**Низкий**
1. По территориальному размещению:			
Распределенная ИСПДн, которая охватывает несколько областей, краев,округов или государство в целом;	–	–	+
Городская ИСПДн, охватывающая неболее одного населенного пункта (города, поселка);	–	–	+

корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации;	–	+	–
локальная (кампусная) ИСПДн, развернутая в пределах несколькихблизко расположенных зданий;	–	+	–
Локальная ИСПДн, развернутая впределах одного здания	+	–	–
2. По наличию соединения с сетями общего пользования:			
ИСПДн, имеющая многоточечныйвыход в сеть общего пользования;	–	–	+
ИСПДн, имеющая одноточечныйвыход в сеть общего пользования;	–	+	–
ИСПДн, физически отделенная отсети общего пользования	+	–	–
3. По встроенным (легальным) операциям с записями баз персональных данных:			
чтение, поиск;	+	–	–
запись, удаление, сортировка;	–	+	–
модификация, передача	–	–	+
4. По разграничению доступа к персональным данным:			
ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцемИСПДн, либо субъект ПДн;	–	+	–
ИСПДн, к которой имеют доступ все сотрудники организации, являющейсявладельцем ИСПДн;	–	–	+
ИСПДн с открытым доступом	–	–	+
Технические и эксплуатационныехарактеристики ИСПДн	**Уровень защищенности**		
	Высокий	**Средний**	**Низкий**
5. По наличию соединений с другими базами ПДн иных ИСПДн:			

интегрированная ИСПДн (организация использует несколько баз ПДн ИСПДн, при этом организация не является владельцемвсех используемых баз ПДн);	–	–	+
ИСПДн, в которой используется однабаза ПДн, принадлежащая организации – владельцу данной ИСПДн	+	–	–
6. По уровню обобщения (обезличивания) ПДн:			
ИСПДн, в которой предоставляемые пользователю данные являются обезличенными (на уровне организации, отрасли, области, региона и т.д.);	+	–	–
ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличеныпри предоставлении пользователю в организации;	–	+	–
ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн)	–	–	+
7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн безпредварительной обработки:			
ИСПДн, предоставляющая всю базу данных с ПДн;	–	–	+
Количество «+» в колонках	5	5	7
РЕЗУЛЬТАТ (Y_1)	5		

Задание 7. Изучите документ Приказ ФСТЭК России от 18.02.2013 № 21"Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных".

Задание 8. Составьте модель защиты, заключающаяся в выборе мер, закрывающих актуальные угрозы безопасности. Модель защиты, в соответствии с пунктом 9 Приказа ФСТЭК России от 18.02.2013 № 21, составляется по следующему алгоритму:

определяется базовый набор мер, а именно составляется перечень тех мер, которые отмечены плюсами для соответствующего УЗ в приложении к Приказу ФСТЭК России от 18.02.2013 № 21;

адаптация базового набора мер. На этом этапе из базового набора мер исключаются те, которые не актуальны из-за особенностей конкретной ИСПДн (например, исключаются меры по защите виртуализации, если виртуализация не используется); уточнение адаптированного базового набора мер. На этом этапе добавляются ранее не выбранные меры, если в соответствии с частной моделью угроз какие-либо из актуальных угроз остались незакрытыми.

Для адаптации мер необходимо соотнести возможные угрозы безопасности ПДн к мерам по приложению Приказа №21 ФСТЭК. Для этого необходимо воспользоваться таблицей:

Соответствие угроз безопасности ПДн мерам по обеспечению безопасности ПДн.

Возможные угрозы безопасности ПДн	**Меры по Приказу №21 ФСТЭК**	
1. Угрозы от утечки по техническим каналам	XII. Защита технических средств (ЗТС)	
1.1. Угрозы утечки акустической информации		
1.2. Угрозы утечки видовой информации		ЗТС.4
1.3. Угрозы утечки информации по каналам ПЭМИН		ЗТС.1
2. Угрозы несанкционированного доступа кинформации		
2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн		
2.1.1. Кража ПЭВМ		ЗТС.3
2.1.2. Кража носителей информации	IV. Защита машинных носителей персональныхданных (ЗНИ)	ЗНИ.1ЗНИ.2
2.1.3. Кража ключей и атрибутов доступа		ЗНИ.5
2.1.4. Кражи, модификации, уничтожениянформации		ЗНИ.8
2.1.5. Вывод из строя узлов ПЭВМ, каналовсвязи	XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)	ЗИС.3
2.1.6. Несанкционированный доступ к информации при техническом обслуживании(ремонте, уничтожении) узлов ПЭВМ	V. Регистрация событий безопасности (РСБ) II. Управление доступом субъектов доступа к объектамдоступа (УПД)	РСБ.1-3
2.1.7. Несанкционированное отключениесредств защиты		ЗТС.3
2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) спримененением программно-аппаратных и программных средств (в том числе программно-математических воздействий)	XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)	ЗИС.3
2.2.1. Действия вредоносных программ (вирусов)	VI. Антивирусная защита (АВЗ)	АВЗ.1-2

2.2.2. Недекларированные возможностисистемного ПО и ПО для обработки персональных данных	III. Ограничение программнойсреды (ОПС)	ОПС.2
2.2.3. Установка ПО, не связанного с исполнением служебных обязанностей		ОПС.3
2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и систем защиты ПДн в ее составе из-за сбоев в программном обеспечении, а также от сбоев аппаратуры, из-за ненадежности элементов, сбоев электропитания и стихийного (ударов молний,пожаров, наводнений и т. п.) характера	X. Обеспечение доступностиперсональных данных (ОДТ)	ОДТ.4
2.3.1. Утрата ключей и атрибутов доступа	I. Идентификация и аутентификация субъектов доступа и объектов доступа(ИАФ)	ИАФ.4
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками	V. Регистрация событийбезопасности (РСБ)	РСБ.7
2.3.3. Непреднамеренное отключение средствзащиты	VIII. Контроль (анализ) защищенности персональныхданных (АНЗ)	АНЗ.3
2.3.4. Выход из строя аппаратно-программных средств	IX.Обеспечение целостностиинформационной системы и персональных данных (ОЦЛ)	ОЦЛ.1
2.3.5. Сбой системы электроснабжения		
2.3.6. Стихийное бедствие		
2.4. Угрозы преднамеренных действий внутренних нарушителей		
2.4.1. Доступ к информации, копирование,модификация, уничтожение, лицами, не допущенными к ее обработке	X. Обеспечение доступностиперсональных данных (ОДТ)	ОЦЛ.2
2.4.2. Разглашение информации, копирование,модификация, уничтожение сотрудниками, допущенными к ее обработке		ОЦЛ.2
2.5.Угрозы несанкционированного доступа поканалам связи		
2.5.1.Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:	XIII. Защита информационнойсистемы, ее средств, систем связи и передачи данных (ЗИС)	
2.5.1.1. Перехват за переделами контролируемой зоны		ОЦЛ.4
2.5.1.2. Перехват в пределах контролируемойзоны внешними нарушителями		ОЦЛ.1
2.5.1.3.Перехват в пределах контролируемойзоны внутренними нарушителями.		ОЦЛ.1

2.5.2.Угрозы сканирования, направленные навыявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	VIII. Контроль (анализ) защищенности персональныхданных (АНЗ)	АНЗ.1-2
2.5.3.Угрозы выявления паролей по сети	XIII. Защита информационнойсистемы, ее средств, систем связи и передачи данных (ЗИС)	АНЗ.3
2.5.4.Угрозы навязывание ложного маршрутасети		ЗИС.3
2.5.5.Угрозы подмены доверенного объекта всети		ЗИС.11
2.5.6.Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях		
2.5.7.Угрозы типа «Отказ в обслуживании»		
2.5.8.Угрозы удаленного запуска приложений		
2.5.9.Угрозы внедрения по сети вредоносных программ	VI. Антивирусная защита(АВЗ)	

2.5. Практическая работа № 5 Установка и настройка СЗИ от НСД

Цель: познакомиться с системами защиты информации от несанкционированного доступа.

Теоретические вопросы

1. Меры противодействия несанкционированному доступу.
2. Идентификация и аутентификация пользователей.
3. Ограничение доступа на вход в систему.
4. Разграничение доступа.
5. Регистрация событий (аудит).
6. Модель защищенной компьютерной системы.
7. Системы защиты информации от несанкционированного доступа.

Задание 1. Изучите возможности системы защиты информации от несанкционированногодоступа «Страж NT»:

- назначение,
- запуск и регистрация системы защиты,
- создание пользователей,
- реализация мандатной модели разграничения доступа,
- реализация дискреционной модели разграничения доступа,
- обеспечение замкнутости программной среды,
- контроль целостности,
- организация учета съемных носителей информации,

- регистрация событий,

- гарантированное удаление данных.

Задание 2. Изучите возможности системы защиты информации от несанкционированногодоступа «Dallas Lock»:

- назначение,

- запуск и регистрация системы защиты,

- создание пользователей,

- реализация мандатной модели разграничения доступа,

- реализация дискреционной модели разграничения доступа,

- обеспечение замкнутости программной среды,

- контроль целостности,

- регистрация событий,

- гарантированное удаление данных,

- печать штампа,

- реализация запрета загрузки ПЭВМ в обход.

Задание 3. Изучите возможности системы защиты информации от несанкционированногодоступа «Secret NET 5.0-C»:

- назначение,

- запуск и регистрация системы защиты,

- создание пользователей,

- реализация мандатной модели разграничения доступа,

- реализация дискреционной модели разграничения доступа,

- обеспечение замкнутости программной среды,

- контроль целостности,

- регистрация событий,

- гарантированное удаление данных,

- печать штампа,

- настройка механизма шифрования.

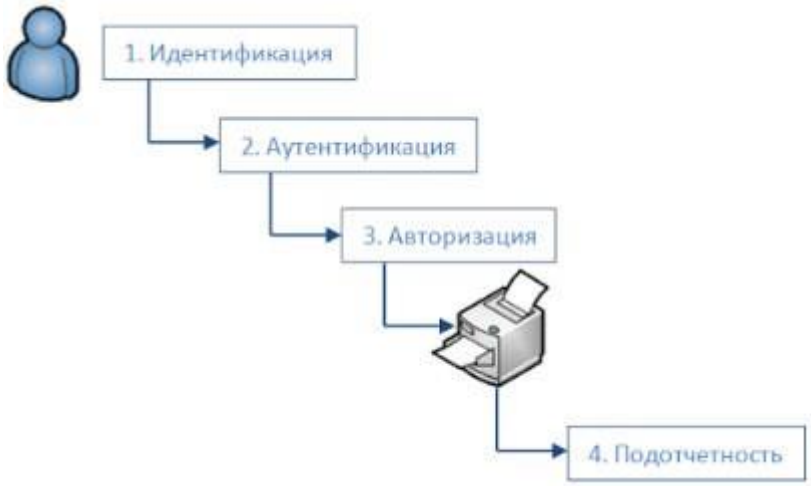
2.6. Практическая работа № 6 Защита входа в систему (идентификация и аутентификация пользователей)

Цели: изучить методы, применяемые для установления подлинности различных объектов и своевременного обнаружения несанкционированных действий пользователя; правила составления пароля; расчета среднего времени безопасности пароля.

Теоретические вопросы

1. Понятия идентификации, аутентификации, авторизации.
2. Логическое управление доступом.
3. Методы идентификации и аутентификации.

Задание 1. Опишите четыре шага, которые необходимо пройти субъекту для получения доступа к объекту:



Задание 2. Опишите правила выбора и использования пароля.

Задание 3. Поясните формулу:

Среднее время безопасности пароля определяется по формуле $\mathbf{T} = \left(d + \frac{m}{n}\right) \bullet \frac{S}{2}$

где d — промежуток времени между двумя неудачными попытками несанкционированного входа в систему, m — количество символов в пароле, n — скорость набора пароля (количество символов, набираемых в единицу времени), S — количество всевозможных паролей указанной длины.

Задание 4. С использованием одного из языков программирования составить программу,которая выполняет действия.

а) Пусть на экран выведены следующие три слова: «Sony», «Hewlett» и «Packard». Составить программу, которая записывает пароль следующим образом:

1. В строку <результат> в качестве первого символа записать букву, которая в алфавите стоит на месте, соответствующем сумме количеств символов в первом и третьем словах; если эта сумма больше 26, найти и использовать в качестве номера позиции искомой буквы в алфавите остаток от деления указанной суммы на 26.

2. В качестве второго символа записать букву, которая в алфавите предшествует букве, являющейся последним символом второго слова на экране; если это буква «a», записать «z».

3. Если третье слово содержит нечетное количество букв, то в качестве третьего символа записать букву, которая в алфавите следует за буквой, являющейся средним символом третьего слова; если это буква «z», записать «a». Если же третье слово содержит четное количество символов, то в качестве третьего символа записать букву, которая в алфавите предшествует букве, являющейся первым из двух средних символов третьего слова; если это буква «a», записать «z».

4. в качестве первого символа записать букву, которая в алфавите следует за

буквой, являющейся первым символом первого слова на экране; если это буква «z», записать «a».

5. Вывести полученную строку.

б) Дополнить полученную программу средствами аутентификации:

1. Ввести пароль пользователя. При вводе пароля пользователя обеспечить ввод пароля сотображением вместо каждого символа знаков «*».

2. Сравнить пароль пользователя с паролем, вычисленным ЭВМ.

3. Вывести результат аутентификации: пароль верен или неверен?

Задание 5. Определите степень защиты информации организации, защищенной с применением пароля, а также исследуйте методы противодействия атакамю

2.7. Практическая работа № 7 Разграничение доступа к устройствам

Задание 1. Опишите схему работы механизма разграничения доступа:

Задание 2. Для учетной записи «user» запретите использование оптических дисков и проверьте ограничение.

Задание 3. Для учетной записи «Конфиденциальный» разрешите вывод на печать документов с категорией конфиденциально. Попытайтесь распечатать документ с категорией конфиденциальности «Конфиденциально» («D:\temp\Конф.txt») и документ с категорией конфиденциальности «Не конфиденциально» («D:\Неконф.txt»).

Задание 4. Создайте замкнутую программную среду в «жестком режиме» для ресурса

«C:/Program Files/Internet Explorer» для учетной записи «user».

Задание 5. Настройте контроль целостности для ресурса «D:\».

Ответ:

2.8. Практическая работа № 8 Управление доступом

Задание 1. Поясните фрагмент матрицы доступа:

	Файл	Программа	Линия связи	Реляционная таблица
Пользователь 1	orw с системной консоли	e	rw с 8:00 до 18:00	
Пользователь 2				a

Задание 2. Заполните таблицу:

Разрешения доступа к общим папкам

Разрешение	**Позволяет**
Изменение	
(Чтение)	
(Полный доступ)	

Задание 3. Пусть пользователю User101 назначены разрешения для получения доступа кресурсам как отдельному пользователю и как члену группы. Определите, какие результирующие разрешения будут у User101 в следующих ситуациях:

1. User101 — член групп Group1, Group2 и Group3. Для папки ПапкаА у Group1 есть разрешение Read (Чтение), у Group3 — Full Control (Полный доступ), а для Group2 разрешений не назначено. Какими результирующими разрешениями будет обладать User101для ПапкиА?

2. User101 также является членом группы Sales, которой назначено разрешение Read для ПапкаВ. Для User101 как отдельного пользователя, отменено разрешение Full Control для ПапкаВ. Какие результирующие разрешения будет иметь User101 для ПапкаВ?

Задание 4. Определите результирующие разрешения пользователей, спланируйте совместное использование папок и разрешений доступа к ним, назначьте разрешения доступа к папке, подключитесь к ней, закройте к ней доступ и проверьте эффекты от сочетания разрешений доступа к общей папке и разрешений NTFS:

3. Открыт доступ к папке Data. Группа Sales имеет для нее разрешение read (Чтение), а для вложенной в нее папки ^ Sales — NTFS-разрешение Full Control (Полный доступ). Каким будет результирующее разрешение группы Sales для доступа к папке Sales при подключении по сети к папке Data?

4. Папка Users (Пользователи) содержит личные папки пользователей. Каждая личная папка содержит данные, доступные только пользователю, именем которого она названа. Папка Users доступна группе Users с разрешением Full Control (Полный доступ). Userl и User2 имеют разрешения NTFS Full

Control только для своих личных папок: никаких разрешений NTFS для остальных. Эти пользователи — члены группы Users. ^ Какими разрешениями доступа к папке Userl будет обладать Userl при подключении к общей папке Users? Какими будут его разрешения для папки User2?

Задание 5. Закройте доступ к заданной папке.

Ответ:

2.9 Практическая работа № 9 Оформление основных эксплуатационных документов на автоматизированную систему.

Цели: изучить правила оформления основных эксплуатационных документов на автоматизированную систему.

Теоретические вопросы

Основные эксплуатационные документы защищенных автоматизированных систем.

Разработка и ведение эксплуатационной документации защищенных автоматизированных систем.

Акт ввода в эксплуатацию на автоматизированную систему.

Технический паспорт на защищаемую автоматизированную систему.

Задание 1. Изучите основные требования следующих стандартов, определяющие построение системы, структуру конструкторских документов, их номенклатуру (комплектность), а также правила выполнения текстовых конструкторских документов:

ГОСТ 2.001-70 “ЕСКД.
Общие положения”.ГОСТ
2.101-68 “ЕСКД. Виды из-
делий».

ГОСТ 2.102-68 “ЕСКД . Виды и комплектность конструкторских документов”.ГОСТ 2.103-68 “ЕСКД. Стадии разработки”.

ГОСТ 2.104-68 “ЕСКД. Основные надписи”.

ГОСТ 2.105-68 “ЕСКД. Общие требования к текстовым документам”.ГОСТ 2.106-68 “ЕСКД. Текстовые документы».

ГОСТ 2.107-68 “ЕСКД. Спецификация”.

ГОСТ 2.108-68 “ЕСКД. Ведомость держателей подлинников».ГОСТ 2.109-68 “ЕСКД. Техническое условие”.

Задание 2. Разработайте эксплуатационную документацию на автоматизированную систему.