0МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Астраханский государственный университет имени В. Н. Татищева»
(Астраханский государственный университет им. В. Н. Татищева)

СОГЛАСОВАНО	УТВЕРЖДАЮ
Руководитель ОПОП	И.о. Заведующего кафедрой информационной безопасности
А.П. Мешкова	В.А. Черкасова
«05» мая 2025 г.	«05» мая 2025 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Основы защиты информации

Составитель(-и)	**Шукралиева Д.Э. доцент кафедры информационной безопасности**
Согласовано с работодателями:	**Сафрыгин Ю.В., руководитель Управления Федерального казначейства по Астраханской области, советник государственной гражданской службы РФ 3 класса**
Направление подготовки	**38.05.01 Экономическая безопасность**
Направленность (профиль) ОПОП	**Экономико-правовое обеспечение экономической безопасности**
Квалификация (степень)	**специалитет**
Форма обучения	**заочная**
Год приема	**2022**
Курс	**4**
Семестры	**7**

Астрахань, 2025

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

1.1. Цель дисциплины: развить базовые и специальные компетенции в сфере ИБ для эффективного и безопасного использования информационно-коммуникационных технологий, в том числе в среде Интернет в образовательной деятельности.

1.2. Задачи освоения дисциплины (модуля):

– подготовить к безопасному использованию информационно-коммуникационных технологий в своей профессиональной деятельности;

– привить навыки использования разнообразных средств и методов обеспечения информационной безопасности, в том числе при работе в среде Интернет;

– мотивировать самообразование и профессиональное развитие в области защиты информации (ЗИ);

– способствовать развитию информационной культуры.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОПОП

2.1. Учебная дисциплина (модуль) «Основы защиты информации» Б1.В.01 относится к части, формируемой участниками образовательных отношений учебного плана направления подготовки 38.05.01 Экономическая безопасность. Профиль «Экономико-правовое обеспечение экономической безопасности» осваивается в 7 семестре, общая трудоемкость дисциплины – 2 ЗЕ, 72 часа, итоговая форма контроля – зачет.

2.2. Для изучения данной учебной дисциплины (модуля) необходимы следующие знания, умения, навыки и (или) опыт деятельности, формируемые предшествующими дисциплинами (модулями):

Знания: основных понятий информатики, архитектуры ЭВМ и устройства ПК, представления данных в ЭВМ, основных закономерностей создания и принципы функционирования систем экономической безопасности хозяйствующих субъектов.

Умения: использовать программные и аппаратные средства персонального компьютера, обосновывать актуальность и практическую значимость разрабатываемых мероприятий по обеспечению экономической безопасности.

Навыки и (или) опыт деятельности: навыки поиска информации в глобальной информационной сети Интернет и работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов, СУБД и т.п.): навыки прогнозирования возможных угроз экономической безопасности.

2.3. Последующие учебные дисциплины (модули) и (или) практики, для который необходимы знания, умения, навыки, формируемые данной учебной дисциплиной (модулем):

1. Защита и обработка конфиденциальной информации.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Процесс освоения дисциплины (модуля) направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО и ОПОП ВО по данному направлению подготовки /специальности:

а) профессиональных (ПК): ПК-3. Способен осуществлять разработку краткосрочной и долгосрочной экономической, внешнеэкономической, финансовой политик предприятий, учреждений, организаций различных организационно-правовых форм и их отдельных подразделений с учетом построения интегрированной системы управления рисками организации.

Таблица 1 – Декомпозиция результатов обучения

Код и наименование компетенции	Планируемые результаты обучения по дисциплине (модулю)		
	Знать (1)	Уметь (2)	Владеть (3)
ПК-3. Способен осуществлять разработку краткосрочной и долгосрочной экономической, внешнеэкономической, финансовой политик предприятий, учреждений, организаций различных организационно-правовых форм и их отдельных подразделений с учетом построения интегрированной системы управления рисками организации	ПК-3.1. Применяет инструменты стратегического управления организацией и механизм построения интегрированной системы управления рисками организации	ПК-3.2. Анализирует и учитывает риски организации при стратегическом управлении организацией	ПК-3.3. Разрабатывает политику организации различных организационно-правовых форм и их отдельных подразделений с учетом построения интегрированной системы управления рисками организации

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Общая трудоемкость дисциплины в соответствии с учебным планом составляет 2 зачетные единицы (72 часа). Трудоемкость отдельных видов учебной работы студентов заочной формы обучения приведена в таблице 2.1.

Таблица 2.1 – Трудоемкость отдельных видов учебной работы по формам обучения

Вид учебной и внеучебной работы	для заочной формы обучения
Объем дисциплины в зачетных единицах	2
Объем дисциплины в академических часах	72
Контактная работа обучающихся с преподавателем (всего)	6
- занятия лекционного типа, в том числе:	2
- занятия семинарского типа (семинары, практические, лабораторные)	4

Самостоятельная работа обучающихся (час.)	66
Форма промежуточной аттестации обучающегося (зачет/экзамен), семестр (ы)	зачёт – 7 семестр

Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий и самостоятельной работы, для каждой формы обучения представлено в таблице 2.2.

Таблица 2.2. Структура и содержание дисциплины (модуля)

для заочной формы обучения

Раздел, тема дисциплины (модуля)	Контактная работа, час.							СР, час.	Итого часов	Форма текущего контроля успеваемости, форма промежуточной аттестации
	Л		ПЗ		ЛР		КР / КП			
	Л	в т. ч. ПП	ПЗ	в т.ч. ПП	ЛР	в т. ч. ПП				
Раздел 1. Основные понятия в области ИБ и ЗИ, их взаимосвязь и правовые основы обеспечения ИБ: Конституция, ФЗ, УК, РД, приказы ФСТЭК и ФСБ								13	13	Опрос. Контрольная работа 1. Входной тест.
Раздел 2. Основы обеспечения ИБ при работе в среде Интернет. Противодействие деструктивному влиянию материалов, распространяющихся через Интернет, в том числе через социальные сети.	1				1			13	15	Опрос. Отчет по лабораторной работе 1. Промежуточный тест
Раздел 3. Основы криптографии. Ее использование для безопасной работы в среде Интернет					1			13	14	Опрос. Контрольная работа 2
Раздел 4. Средства обеспечения ИБ, в том числе при работе через Интернет					1			13	14	Опрос. Отчет по лабораторной работе 2. Итоговый тест
Раздел 5. Основные мотивы выдачи информации. Работа с персоналом	1				1			14	16	Опрос. Контрольная работа 3. Защита доклада
Итого	**2**				**4**			**66**	**72**	

Контроль промежуточной аттестации		**зачёт**

Примечание: Л – лекция; ПЗ – практическое занятие, семинар; ЛР – лабораторная работа; КР – курсовая работа; СР – самостоятельная работа.

Таблица 3 – Матрица соотнесения разделов, тем учебной дисциплины (модуля) и формируемых компетенций

для заочной формы

Раздел, тема дисциплины (модуля)	Кол-во часов	Код компетенции ПК-3	Общее количество компетенций
Раздел 1. Основные понятия в области ИБ и ЗИ, их взаимосвязь и правовые основы обеспечения ИБ: Конституция, ФЗ, УК, РД, приказы ФСТЭК и ФСБ	13	+	1
Раздел 2. Основы обеспечения ИБ при работе в среде Интернет. Противодействие деструктивному влиянию материалов, распространяющихся через Интернет, в том числе через социальные сети.	15	+	1
Раздел 3. Основы криптографии. Ее использование для безопасной работы в среде Интернет	14	+	1
Раздел 4. Средства обеспечения ИБ, в том числе при работе через Интернет	14	+	1
Раздел 5. Основные мотивы выдачи информации. Работа с персоналом	16	+	1
Итого	**72**		

Краткое содержание каждой темы дисциплины (модуля)

Раздел 1. Основные понятия в области ИБ и ЗИ, их взаимосвязь, правовые основы обеспечения ИБ: Конституция, ФЗ, УК, РД, приказы ФСТЭК и ФСБ

Тема 1.1 Сервисы ИБ и основные направления их обеспечения: организационно-правовое; программно-аппаратное; инженерно-техническое.

Определение понятий «Информация» «Информационная безопасность», «Субъекты информационных отношений». Объект и субъект защиты информации. Состав средств и мер защиты информации. Классификация средств и мер защиты информации. Основные сервисы ИБ. Концепция ИБ. Задачи системы безопасности.

Тема 1.2 Классификация информации по ее доступности: общедоступная информация и информация ограниченного доступа (конфиденциальная информация и государственная тайна). Информация, запрещенная к распространению.

Категорирование информации. Определение общедоступной информации. Определение информации ограниченного доступа. Право на доступ к информации. Понятие государственной тайны. Особенности работы с персоналом, владеющим конфиденциальной информацией. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Запрещенная к распространению информация. Нормативные акты, запрещающие распространение подобной информации.

Тема 1.3 Правовые основы обеспечения ИБ: Конституция, ФЗ, УК, РД, приказы ФСТЭК и ФСБ. Основы обеспечения безопасности персональных данных.

Правовое обеспечение безопасности правового статуса субъектов информационной сферы. Содержание и структура законодательства. Конституция РФ. Федеральные законы, нормативные правовые акты Президента РФ, подзаконные акты Правительства РФ. Приказы ФСТЭК и ФСБ. Общие положения ФЗ «О государственной тайне». Порядок отнесения сведений к государственной тайне (ГТ). Законодательство о персональных данных. Общие положения. Принципы и условия обработки персональных данных, их конфиденциальность.

Раздел 2. Основы обеспечения ИБ при работе в среде Интернет. Противодействие деструктивному влиянию материалов, распространяющихся через Интернет, в том числе через социальные сети.

Тема 2.1 Основы передачи информации в среде Интернет

Организация информации в сети Интернет. Службы сети Интернет.

Интернет-провайдер (ISP). Адресация. Переадресация. Доменные имена. Длинные доменные имена. Виды доменных имен. Протоколы передачи данных. Семейство протоколов TCP/IP.

Тема 2.2 Программное обеспечение для безопасной работы в среде Интернет

Интернет. Безопасность. Браузер «Tor». Антивирусное программное обеспечение. Программы блокировки баннерной рекламы. Программы-фильтры спама. Программы восстановления после сбоя.

Тема 2.3 Противодействие деструктивному влиянию материалов, распространяемых через социальные сети.

Понятие «социальная сеть». Структура социальной сети. Социальная сеть «Вконтакте». Социальная сеть «Одноклассники». Деструктивная информация.

Раздел 3. Основы криптографии

Тема 3.1. Основные понятия криптографии. Электронная подпись: формирование, получение сертификата, использование в защищенном документообороте

Введение. Криптография как механизм защиты. Понятие криптографии. Методы криптографии. Основные требования к шифрам для криптозащиты информации. Основные типы шифров. Надежность шифров. Электронная цифровая подпись (ЭЦП). определение, предназначение, состав.

Тема 3.2 Проверка выполнения требований законодательства уполномоченными органами

Технологические основы обработки конфиденциальных документов. Политика безопасности. Система сертификации. Порядок сертификации.

Тема 3.3 Использование криптографии для безопасной работы в среде Интернет

Криптографические методы защиты информации в среде Интернет. Шифрование электронной почты. Почтовые клиенты: Outlook, Thinderbird, The Bat. Сертификаты открытого и закрытого ключа.

Раздел 4. Средства обеспечения ИБ, в том числе при работе через Интернет

Тема 4.1. Основные принципы работы программно-аппаратных средств обеспечения ИБ

Предмет и задачи программно-аппаратной защиты информации, основные подходы к защите данных от НСД. Основные принципы обеспечения информационной безопасности вычислительных систем с помощью программно-аппаратных средств. Функциональные требования по защите вычислительных систем.

Тема 4.2. Классификация типовых программно-аппаратных средств обеспечения ИБ

Особенности программно-аппаратного обеспечения безопасности в интерактивной среде. Защита электронной почты от злонамеренных и нежелательных воздействий, фальшивая и анонимная почта. Защита информационной среды от нежелательных информационных материалов, средства фильтрации сетевой информации/

Раздел 5. Основные мотивы выдачи информации. Работа с персоналом

Тема 5.1 Понятие о лояльном сотруднике и нарушителе в информационной сфере.

Определение лояльного сотрудника. Определение нарушителя в информационной сфере. Кадровая безопасность и лояльность персонала. Информационная безопасность организации.

Тема 5.2 Представления о чертах характера возможного нарушителя и лояльного сотрудника. Верные и неверные представления.

Типы лояльных сотрудников. Модель лояльного сотрудника в сфере ИБ. Типы нарушителей в сфере ИБ. Модель нарушителя в сфере ИБ. Понятие о психологическом портрете нарушителя в сфере информационной безопасности.

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПРЕПОДАВАНИЮ И ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1. Указания для преподавателей по организации и проведению учебных занятий по дисциплине (модулю)

При подготовке к лекционным занятиям необходимо воспользоваться учебно-методической литературой (основной) из п.8.

При подготовке к лабораторным занятиям необходимо воспользоваться учебно-методической литературой (дополнительной) из п.8.

5.2. Указания для обучающихся по освоению дисциплины (модулю)

Во время самостоятельной работы необходимо воспользоваться учебно-методической литературой из п.8 (основной), (дополнительной), Интернет-ресурсами.

Таблица 4 – Содержание самостоятельной работы обучающихся

для заочной формы обучения

Номер радела (темы)	*Темы/вопросы, выносимые на самостоятельное изучение*	*Кол-во часов*	*Формы работы*
Раздел 1. Основные понятия в области ИБ и ЗИ, их взаимосвязь и правовые основы обеспечения ИБ: Конституция, ФЗ,	Подготовка к устному опросу. Изучение международных стандартов информационного обмена. Закон РФ «О персональных данных». Составление терминологического словаря. Подготовка к контрольной работе 1. Подготовка к входному тесту	13	Внеаудиторная, изучение учебных пособий

УК, РД, приказы ФСТЭК и ФСБ			
Раздел 2. Основы обеспечения ИБ при работе в среде Интернет. Противодействие деструктивному влиянию материалов, распространяющихся через Интернет, в том числе через социальные сети.	Подготовка к устному опросу. Конспект по определению требований к защищенности информации. Подготовка отчета по лабораторной работе 1	13	Внеаудиторная, изучение учебных пособий
Раздел 3. Основы криптографии. Ее использование для безопасной работы в среде Интернет	Подготовка к устному опросу. Подготовка к контрольной работе 2	13	Внеаудиторная, изучение учебных пособий
Раздел 4. Средства обеспечения ИБ, в том числе при работе через Интернет	Подготовка к устному опросу. Подготовка отчета по лабораторной работе 2. Подготовка к итоговому тесту	13	Внеаудиторная, изучение учебных пособий
Раздел 5. Основные мотивы выдачи информации. Работа с персоналом	Подготовка к устному опросу. Самостоятельное изучение массовидных явлений: мода, паника, стресс, страх. Разработать требования к речи сотрудника по ИБ Подготовка к контрольной работе 3.Подготовка доклада по нормативно-правовым актам, касающимся защиты любых видов тайн, прав на информацию, запретов на распространение информации	14	Внеаудиторная, изучение учебных пособий

5.3. Виды и формы письменных работ, предусмотренных при освоении дисциплины, выполняемые обучающимися самостоятельно

Правила оформления текста пояснительной записки реферата

На титульном листе прописываются: название университета, факультета, кафедры, название дисциплины, темы реферата, Ф.И.О. студента, номер группы, Ф.И.О. преподавателя и оставляется место для проставления оценки и подписи преподавателя . Внизу пишется город и год написания.

Текстовая часть

Изложение текста и оформление работы следует выполнять в соответствии с требованиями.

Текст ПЗ оформляется на одной стороне листа формата А4.

Основной текст набирается шрифтом *Times New Roman 12,* с выравниванием *по ширине*, абзацный отступ должен быть одинаковым по всему тексту и равен *1,25 см*; строки разделяются *полуторным интервалом*.

Поля страницы: верхнее -2,5см, нижнее – 2,5 см, левое – 3,5 см, правое – 1,0 см.

Структурные элементы пояснительной записки **СОДЕРЖАНИЕ, ВВЕДЕНИЕ, ЗАКЛЮЧЕНИЕ, СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ, ПРИЛОЖЕНИЕ** должны начинаться с нового листа.

Их заголовки оформляются ***прописными буквами, шрифтом 14 Ж***, располагаются *в середине строки без точки в конце*. Дополнительный *интервал после* заголовка - 12 *пт*.

Основную часть работы разделяют на разделы, подразделы и, при необходимости, на пункты.

Каждый раздел необходимо начинать с нового листа. Разделы нумеруют арабскими цифрами в пределах всего текста. После номера и в конце заголовка раздела *точка не ставится*.

Если заголовок состоит из двух предложений, их разделяют точкой. *Переносы слов в заголовках не допускаются.*

Заголовки разделов оформляются ***с прописной буквы, шрифтом 14 Ж,*** с абзацного отступа *1,25* см. Дополнительный *интервал после заголовка - 6 пт.*

(Если заголовок раздела занимает две и большее число строк, то интервал между этими строками – *полуторным*).

Подразделы нумеруются в пределах каждого раздела. Номер подраздела состоит из номера раздела и порядкового номера подраздела, разделенных точкой. После номера подраздела точку не ставят.

Заголовки подразделов печатаются с абзацного отступа, ***с прописной буквы шрифтом 12 Ж,*** без точки в конце заголовка.

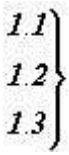
Дополнительный *интервал перед* заголовком подраздела – *6 пт, после* заголовка - 6 *пт*.

Пункты нумеруются в пределах каждого подраздела. Номер пункта состоит из номеров раздела, подраздела и пункта, разделенных точкой. После номера пункта точку не ставят.

Нельзя писать заголовок в конце страницы, если на ней не умещаются, по крайней мере, две строки текста, идущего за заголовком.

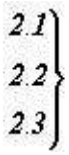
Пример оформления заголовков текста:

1 Разработка аппаратных средств



Нумерация пунктов первого раздела отчета

2 Технические характеристики



Нумерация пунктов второго раздела отчета

В пояснительной записке после титульного листа помещается лист **СОДЕРЖАНИЕ**, в котором указываются номера и наименования разделов, подразделов и приложений ТД с указанием номеров страниц, где они начинаются.

Разделы, подразделы записываются в содержании в точном соответствии с их наименованиями без сокращений *строчными буквами кроме первой прописной.*

Перечисления

В тексте пояснительной записки перечисления производятся с абзацного отступа, каждое с новой строки с *дефисом***.**

Примеры написания:

- текст пояснительной записки (ПЗ) (с рисунками, таблицами и т. п.);

- приложения;

- перечень терминов;

- перечень сокращений;

- перечень литературы.

При необходимости ссылки в тексте отчета на один из элементов перечисления вместо дефиса ставятся строчные буквы в порядке русского алфавита, начиная с буквы а (за исключением букв з, й, о, ч, ъ, ы, ь).

Для дальнейшей детализации перечислений необходимо использовать арабские цифры, после которых ставится скобка, а запись производится с абзацного отступа, как показано в примере.

При необходимости дальнейшей детализации перечислений используются арабские цифры и строчные буквы русского алфавита, после которых ставятся скобки:

а)…;

б)…;

1)…;

2)…;

в).

Примеры написания:

1) текст пояснительной записки (ПЗ) (с рисунками, таблицами и т. п.);
2) приложения;
3) перечень терминов;
4) перечень сокращений;
5) перечень литературы.

Примеры написания:

а) текст пояснительной записки (ПЗ) (с рисунками, таблицами и т. п.);

б) приложения;

в) перечень терминов;

г) перечень сокращений;

д) перечень литературы.

Сокращения слов

Сокращение слов в тексте, как правило, не допускается. Исключение составляют сокращения, общепринятые в русском языке: т. е. (то есть), и т. п. (и тому подобное), и т. д. (и так далее), и др. (и другие).

При необходимости применения специфических терминов или сокращений нужно дать их разъяснение при первом упоминании. Например «…создание систем автоматического проектирования (САПР)». В последующем тексте принятые сокращения пишутся без скобок.

Формулы

Составной частью текста пояснительной записки являются математические формулы и соотношения. Формулы создаются в редакторе формул.

Формулы располагают в середине строки и выделяют из текста свободными строками.

Пример оформления расчетов:

Количество населения в заданном пункте и подчиненных окрестностях с учетом среднего прироста населения определяется по формуле (3.1):

$$H_t = H_0\left(1 + \frac{\Delta H}{100}\right)^t, \qquad ((3.1)$$

где H_0 – число жителей на время проведения переписи населения, тыс. чел.;

ΔH – средний годовой прирост населения в данной местности, % (принимается 2…3%);

t – период, определяемый как разность между назначенным годом перспективного проектирования и годом проведения переписи населения, год.

$$H_t = 32{,}6\left(1 + \frac{2}{100}\right)^8 = 38{,}2 \text{ тыс. чел.}$$

Расшифровка формулы, при необходимости, приводится непосредственно под формулой. В конце формулы ставится запятая, пояснение значений символов дают с новой строки в той последовательности, в какой они приведены в формуле.

Формулы нумеруются в пределах раздела. Номер формулы состоит из номера раздела и порядкового номера формулы в этом разделе. Номер формулы в круглых скобках помещается в крайнем правом положении на строке.

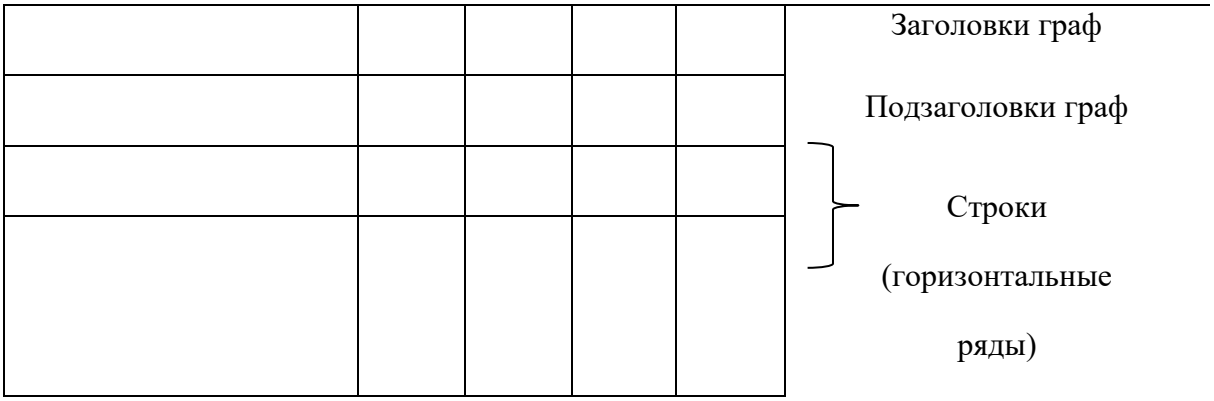
Ссылка в тексте на формулу: «…в формуле (3.1)».

Таблицы

Цифровой материал оформляется в виде таблиц. Таблицу следует располагать непосредственно после ссылки на нее.

Размеры таблиц выбираются произвольно, в зависимости от представляемого материала. Высота строк таблицы должна быть не менее 8 мм

Таблица 2.1 – Наименование таблицы



Заголовки граф и строк таблицы должны начинаться с прописной буквы, а подзаголовки граф – со строчной буквы, если они составляют одно предложение с заголовком. Если подзаголовки граф имеют самостоятельное значение, то их начинают с прописной буквы.

Заголовки указывают в единственном числе. В конце заголовков и подзаголовков таблицы точки не ставят.

Разделять заголовки боковика и граф диагональными линиями не допускается. Графу

«Номер по порядку» в таблицу включать не допускается.

Таблицы нумеруются в пределах раздела. Номер таблицы состоит из номера раздела и порядкового номера таблицы в этом разделе. Номер и наименование таблицы следует помещать над таблицей слева через тире.

Пример оформления таблицы:

Таблица 3.1– Длина участков трассы

Протяженность участка проектируемой трассы, км	Тип кабеля
0,084	ДПС-04-24А06-7,0
0,167	ДПС-04-24А06-7,0
0,301	ДПС-04-24А06-7,0
0,779	ДПС-04-24А06-7,0
Общая длина кабеля: 1,331 км	ДПС-04-24А06-7,0

Примечание – Толщину линий таблицы задайте 1 пт.

Таблицу с большим числом строк допускается переносить на другой лист. При этом в первой части таблицы нижнюю горизонтальную линию не проводят. Над второй частью слева пишут: «Продолжение Таблицы 2.1».

Продолжение Таблицы 2.1

Дата	Наименование	Стоимость

Рисунки

Графический материал располагают, возможно, ближе к тексту, в котором о нём упоминается.

Все рисунки нумеруются в пределах раздела и должны иметь наименование, Номер рисунка и его наименование располагают под рисунком следующим образом:

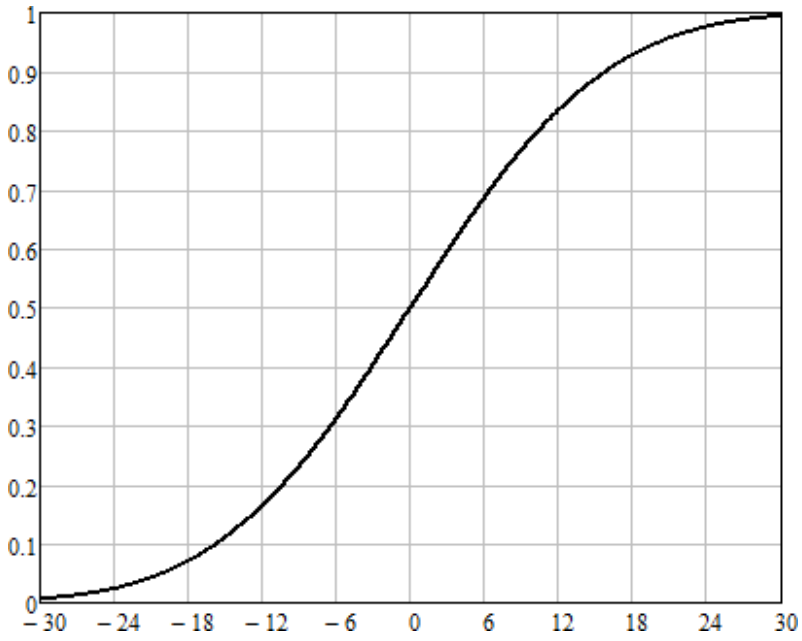


Рисунок 2.12 – Кривая коэффициента восприятия речи

Ссылка в тексте на рисунок: «…в соответствии с рисунком 4.3».

Если в разделе ВВЕДЕНИЕ есть рисунки, то они нумеруются как :
Рисунок В.1 – Название рисунка

Список использованных источников

Список использованных источников приводится в конце пояснительной записки. Список использованных учебников, справочников, статей, стандартов и др. следует располагать в порядке появления ссылок на источники в тексте работы и нумеровать арабскими цифрами без точки, печатать с абзацного отступа.

Список литературы должен быть составлен в алфавитном порядке. Список адресов серверов Internet указывается после литературных источников. При указании веб-адреса рекомендуется давать заголовок данного ресурса (заголовок веб-страницы).

При составлении списка литературы в алфавитном порядке следует придерживаться следующих правил:

1) законодательные акты и постановления правительства РФ;

2) специальная научная литература;

3) методические, справочные и нормативные материалы, статьи периодической печати.

Для многотиражной литературы при составлении списка указываются: полное название источника, фамилия и инициалы автора, издательство и год выпуска (для статьи – название издания и его номер). Полное название литературного источника приводится в начале книги на 2-3 странице.

Для законодательных актов необходимо указывать их полное название, принявший орган и дату принятия.

При указании адресов серверов Internet сначала указывается название организации, которой принадлежит сервер, а затем его полный адрес.

Примеры записей:

1 Глухов В. А. Исследование, разработка и построение системы электронной доставки документов в библиотеке: Автореф. дис. канд. техн. наук. – Новосибирск, 2000. – 18 с.

2 Экономика и политика России и государств ближнего зарубежья : аналит. обзор, апр. 2007, Рос. акад. наук, Ин-т мировой экономики и муждунар. отношений. – М. : ИМЭМО, 2007. – 39 с.

3 Фенухин В. И. Этнополитические конфликты в современной России: на примере Северо-Кавказкого региона : дис. … канд. полит. наук. – М., 2002. – с. 54–55.

4 Официальные периодические издания : электронный путеводитель / Рос. нац. б-ка, Центр правовой информации. [СПб], 200520076. URL: http://www.nlr.ru/lawcrnter/izd/index.html (дата обращения: 18.01.2007).

5 Логинова Л. Г. Сущность результата дополнительного образования детей // Образование: исследовано в мире: междунар. науч. пед. интернет-журн. 21.10.03. URL: http://www.oim.ru/reader.asp?nomer=366 (дата обращения: 17.04.07).

6 Рынок тренингов Новосибирска: своя игра [Электронный ресурс]. – Режим доступа: http://nsk.adme.ru/news/2006/07/03/2121.html (дата обращения: 17.10.08).

Оформление приложений

Нумерация приложений осуществляется русскими буквами, кроме букв Ё, Й, Ъ, Ь, Ы, О.

В разделе СОДЕРЖАНИЕ название приложения оформляется следующим образом:

ПРИЛОЖЕНИЕ А – Диаграмма классов

В самом приложении, слово **ПРИЛОЖЕНИЕ А** пишется жирным шрифтом по центру, на следующей строке пишется название приложения, по центру жирным шрифтом, например,

ПРИЛОЖЕНИЕ А
Диаграмма классов

Если приложение продолжается на следующей странице, то необходимо сверху по центру, нежирным шрифтом написать слова:

Продолжение Приложения А

Если в приложении, например, в приложении А есть таблицы, то они нумеруются как:

Таблица А.1– Название таблицы

Если в приложении есть рисунки, например, в приложении А, то они нумеруются как:

Рисунок А.1 – Название рисунка

6. ОБРАЗОВАТЕЛЬНЫЕ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

При реализации различных видов учебной работы по дисциплине могут использоваться электронное обучение и дистанционные образовательные технологии.

6.1. Образовательные технологии

Таблица 5 – Образовательные технологии, используемые при реализации учебных занятий

Раздел, тема дисциплины (модуля)	Форма учебного занятия		
	Лекция	Практическое занятие, семинар	Лабораторная работа
Раздел 1. Основные понятия в области ИБ и ЗИ, их взаимосвязь и правовые основы	Обзорная лекция	Не предусмотрено	выполнение контрольной работы, теста

обеспечения ИБ: Конституция, ФЗ, УК, РД, приказы ФСТЭК и ФСБ			
Раздел 2. Основы обеспечения ИБ при работе в среде Интернет. Противодействие деструктивному влиянию материалов, распространяющихся через Интернет, в том числе через социальные сети.	Лекция - презентация	Не предусмотрено	выполнение лабораторной работы, теста
Раздел 3. Основы криптографии. Ее использование для безопасной работы в среде Интернет	Лекция - презентация	Не предусмотрено	выполнение контрольной работы
Раздел 4. Средства обеспечения ИБ, в том числе при работе через Интернет	Лекция - презентация	Не предусмотрено	выполнение лабораторной работы, теста
Раздел 5. Основные мотивы выдачи информации. Работа с персоналом	Обзорная лекция	Не предусмотрено	выполнение контрольной работы

Учебные занятия по дисциплине могут проводиться с применением информационно-телекоммуникационных сетей при опосредованном (на расстоянии) интерактивном взаимодействии обучающихся и преподавателя в режимах on-line в формах: видеолекций, лекций-презентаций, видеоконференции, собеседования в режиме чат, форума, чата, выполнения виртуальных практических и/или лабораторных работ и др.

Максимальный объем занятий обучающегося с применением электронных образовательных технологий не должен превышать 25%.

6.2. Информационные технологии

– использование возможностей интернета в учебном процессе (использование сайта преподавателя (рассылка заданий, предоставление выполненных работ, ответы на вопросы, ознакомление обучающихся с оценками и т.д.));

– использование электронных учебников и различных сайтов (например, электронных библиотек, журналов и т. д.) как источников информации;

– использование возможностей электронной почты преподавателя;

– использование средств представления учебной информации (электронных учебных пособий и практикумов, применение новых технологий для проведения очных (традиционных) лекций и семинаров с использованием презентаций и т. д.);

– использование интегрированных образовательных сред, где главной составляющей являются не только применяемые технологии, но и содержательная часть, т. е. информационные ресурсы (доступ к мировым информационным ресурсам, на базе которых строится учебный процесс);

– использование виртуальной обучающей среды (LMS Moodle «Электронное обучение») или иных информационных систем, сервисов и мессенджеров.

6.3. Программное обеспечение, современные профессиональные базы данных и информационные справочные системы

6.3.1. Программное обеспечение

Наименование программного обеспечения	Назначение
Adobe Reader	Программа для просмотра электронных документов
Платформа дистанционного обучения LMS Moodle	Виртуальная обучающая среда
Mozilla FireFox	Браузер
Microsoft Office 2013, Microsoft Office Project 2013, Microsoft Office Visio 2013	Офисная программа
7-zip	Архиватор
Microsoft Windows 7 Professional	Операционная система
Kaspersky Endpoint Security	Средство антивирусной защиты

6.3.2. Современные профессиональные базы данных и информационные справочные системы

1. Электронный каталог Научной библиотеки АГУ на базе MARK SQL НПО «Информ-систем»: https://library.asu.edu.ru.
2. Электронный каталог «Научные журналы АГУ»: http://journal.asu.edu.ru/.
3. Универсальная справочно-информационная полнотекстовая база данных периодических изданий ООО «ИВИС»: http://dlib.eastview.com/
4. Электронно-библиотечная система elibrary. http://elibrary.ru
5. Справочная правовая система КонсультантПлюс: http://www.consultant.ru
6. Информационно-правовое обеспечение «Система ГАРАНТ»: http://garant-astrakhan.ru

7. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

7.1. Паспорт фонда оценочных средств

При проведении текущего контроля и промежуточной аттестации по дисциплине (модулю) «Основы защиты информации» проверяется сформированность у обучающихся компетенций, указанных в разделе 3 настоящей программы. Этапность формирования данных компетенций в процессе освоения образовательной программы определяется последовательным освоением дисциплин (модулей) и прохождением практик, а в процессе освоения дисциплины (модуля) – последовательным достижением результатов освоения содержательно связанных между собой разделов, тем.

Таблица 6 – Соответствие разделов, тем дисциплины (модуля), результатов обучения по дисциплине (модулю) и оценочных средств

№ п/п	Контролируемый раздел, тема дисциплины (модуля)	Код контролируемой компетенции	Наименование оценочного средства
1.	Раздел 1. Основные понятия в области ИБ и ЗИ, их взаимосвязь и правовые основы обеспечения ИБ: Конституция, ФЗ, УК, РД, приказы ФСТЭК и ФСБ	ПК-3	Вопросы для обсуждения. Контрольная работа 1. Входной тест.
2.	Раздел 2. Основы обеспечения ИБ при работе в среде Интернет. Противодействие деструктивному влиянию материалов, распространяющихся через Интернет, в том числе через социальные сети.	ПК-3	Вопросы для обсуждения. Лабораторная работа 1. Промежуточный тест
3.	Раздел 3. Основы криптографии. Ее использование для безопасной работы в среде Интернет	ПК-3	Вопросы для обсуждения. Контрольная работа 2
4.	Раздел 4. Средства обеспечения ИБ, в том числе при работе через Интернет	ПК-3	Вопросы для обсуждения. Лабораторная работа 2. Итоговый тест
5.	Раздел 5. Основные мотивы выдачи информации. Работа с персоналом	ПК-3	Вопросы для обсуждения. Контрольная работа 3. Доклад

7.2. Описание показателей и критериев оценивания компетенций, описание шкал оценивания

При решении комплексной ситуационной задачи можно использовать следующие критерии оценки:

Таблица 7 – Показатели оценивания результатов обучения в виде знаний

Шкала оценивания	Критерии оценивания

5 «отлично»	демонстрирует глубокое знание теоретического материала, умение обоснованно излагать свои мысли по обсуждаемым вопросам, способность полно, правильно и аргументированно отвечать на вопросы, приводить примеры
4 «хорошо»	демонстрирует знание теоретического материала, его последовательное изложение, способность приводить примеры, допускает единичные ошибки, исправляемые после замечания преподавателя
3 «удовлетвори тельно»	демонстрирует неполное, фрагментарное знание теоретического материала, требующее наводящих вопросов преподавателя, допускает существенные ошибки в его изложении, затрудняется в приведении примеров и формулировке выводов
2 «неудовлет-ворительно»	демонстрирует существенные пробелы в знании теоретического материала, не способен его изложить и ответить на наводящие вопросы преподавателя, не может привести примеры

Таблица 8 – Показатели оценивания результатов обучения в виде умений и владений

Шкала оценивания	Критерии оценивания
5 «отлично»	демонстрирует способность применять знание теоретического материала при выполнении заданий, последовательно и правильно выполняет задания, умеет обоснованно излагать свои мысли и делать необходимые выводы
4 «хорошо»	демонстрирует способность применять знание теоретического материала при выполнении заданий, последовательно и правильно выполняет задания, умеет обоснованно излагать свои мысли и делать необходимые выводы, допускает единичные ошибки, исправляемые после замечания преподавателя
3 «удовлетвори тельно»	демонстрирует отдельные, несистематизированные навыки, испытывает затруднения и допускает ошибки при выполнении заданий, выполняет задание при подсказке преподавателя, затрудняется в формулировке выводов
2 «неудовлет-ворительно»	не способен правильно выполнить задание

7.3. Контрольные задания или иные материалы, необходимые для оценки результатов обучения по дисциплине (модулю)

Раздел 1. Основные понятия в области ИБ и ЗИ, их взаимосвязь, правовые основы обеспечения ИБ: Конституция, ФЗ, УК, РД, приказы ФСТЭК и ФСБ

1. Вопросы для обсуждения.

1) Объект и субъект защиты информации. Состав средств и мер защиты информации.
2) Классификация средств и мер защиты информации.
3) Основные сервисы ИБ. Задачи системы безопасности.
4) Категорирование информации. Определение общедоступной информации. Определение информации ограниченного доступа.
5) Право на доступ к информации. Понятие государственной тайны.
6) Особенности работы с персоналом, владеющим конфиденциальной информацией.
7) Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.
8) Запрещенная к распространению информация. Нормативные акты, запрещающие распространение подобной информации.
9) Правовое обеспечение безопасности правового статуса субъектов информационной сферы.
10) Содержание и структура законодательства. Конституция РФ. Федеральные законы, нормативные правовые акты Президента РФ, подзаконные акты Правительства РФ. Приказы ФСТЭК и ФСБ.
11) Общие положения ФЗ «О государственной тайне». Порядок отнесения сведений к государственной тайне (ГТ).
12) Законодательство о персональных данных. Общие положения. Принципы и условия обработки персональных данных, их конфиденциальность.

2. Контрольная работа 1

Вопросы к контрольной работе 1

1) Определение понятий «Информация» «Информационная безопасность», «Субъекты информационных отношений». Объект и субъект защиты информации.
2) Состав средств и мер защиты информации. Классификация средств и мер защиты информации.
3) Основные сервисы ИБ. Концепция ИБ. Задачи системы безопасности.
4) Категорирование информации. Определение общедоступной информации. Определение информации ограниченного доступа. Право на доступ к информации.
5) Понятие государственной тайны. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.
6) Особенности работы с персоналом, владеющим конфиденциальной информацией.
7) Запрещенная к распространению информация. Нормативные акты, запрещающие распространение подобной информации.
8) Правовое обеспечение безопасности правового статуса субъектов информационной сферы. Содержание и структура законодательства.
9) Конституция РФ. Федеральные законы, нормативные правовые акты Президента РФ, подзаконные акты Правительства РФ. Приказы ФСТЭК и ФСБ.
10) Общие положения ФЗ «О государственной тайне».
11) Законодательство о персональных данных.

3. Тест входной

Банк тестовых заданий размещен на сайте центра цифрового обучения http://moodle.asu.edu.ru

1. По объекту воздействия угрозы бывают:

- воздействующие на информационную среду в целом

- воздействующие на отдельные элементы информационной среды
- активные
- пассивные

2. Выберите правильный вариант ответа. Событие, являющееся следствием одного или нескольких нежелательных или неожиданных событий (информационной безопасности), имеющих значительную вероятность компрометации бизнес-операции и создания угрозы
- инцидент
- нарушение
- сигнал

3. Идентифицированное появление определенного состояния системы, сервиса или сети, указывающего на возможное нарушение политики информационной безопасности, или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности называется
- событием (информационной безопасности)
- инцидентом (информационной безопасности)
- угрозой (информационной безопасности)

4. Первым шагом в управлении сетью является ее
- документирование
- ревизия
- оформление

5. Какова цель ревизии эффективности?
- Мониторинг и анализ работы сети.
- Определение того, работает ли сеть в соответствии со своим потенциалом.
- Идентификация типов оборудования и устройств, сети.
- Обеспечение информации о восстановлении после сбоя или катастрофического отказа.

Раздел 2. Основы обеспечения ИБ при работе в среде Интернет. Противодействие деструктивному влиянию материалов, распространяющихся через Интернет, в том числе через социальные сети.

1. Вопросы для обсуждения.

1) Организация информации в сети Интернет.
2) Службы сети Интернет.
3) Интернет-провайдер (ISP). Адресация. Переадресация. Доменные имена. Длинные доменные имена. Виды доменных имен.
4) Протоколы передачи данных.
5) Семейство протоколов TCP/IP.
6) Интернет. Безопасность. Браузер «Tor».
7) Антивирусное программное обеспечение. Программы блокировки баннерной рекламы. Программы-фильтры спама. Программы восстановления после сбоя.
8) Понятие «социальная сеть». Структура социальной сети.
9) Социальная сеть «Вконтакте». Социальная сеть «Одноклассники».
10) Деструктивная информация.

2. Лабораторная работа 1

Парольная защита

Под **несанкционированным доступом к информации** (НСД) согласно руководящим документам Гостехкомиссии будем понимать доступ к информации, нарушающий установленные правила разграничения доступа и осуществляемый с использованием штатных средств, предоставляемых СВТ или АС. НСД может носить случайный или намеренный характер.

Можно выделить несколько обобщенных категорий методов защиты от НСД, в частности:

- организационные;
- технологические;
- правовые.

К первой категории относятся меры и мероприятия, регламентируемые внутренними инструкциями организации, эксплуатирующей информационную систему. Пример такой защиты — присвоение грифов секретности документам и материалам, хранящимся в отдельном помещении, и контроль доступа к ним сотрудников. Вторую категорию составляют механизмы защиты, реализуемые на базе программно-аппаратных средств, например систем идентификации и аутентификации или охранной сигнализации. Последняя категория включает меры контроля за исполнением нормативных актов общегосударственного значения, механизмы разработки и совершенствования нормативной базы, регулирующей вопросы защиты информации. Реализуемые на практике методы, как правило, сочетают в себе элементы нескольких из перечисленных категорий. Так, управление доступом в помещения может представлять собой взаимосвязь организационных (выдача допусков и ключей) и технологических (установку замков и систем сигнализации) способов защиты.

Рассмотрим подробнее такие взаимосвязанные методы защиты от НСД, как идентификация, аутентификация и используемое при их реализации криптографическое преобразование информации.

Идентификация — это присвоение пользователям идентификаторов и проверка предъявляемых идентификаторов по списку присвоенных.

Аутентификация — это проверка принадлежности пользователю предъявленного им идентификатора. Часто аутентификацию также называют подтверждением или проверкой подлинности.

Под безопасностью (стойкостью) системы идентификации и аутентификации будем понимать степень обеспечиваемых ею гарантий того, что злоумышленник не способен пройти аутентификацию от имени другого пользователя, В этом смысле, чем выше стойкость системы аутентификации, тем сложнее злоумышленнику решить указанную задачу. Система идентификации и аутентификации является одним из ключевых элементов инфраструктуры защиты от НСД любой информационной системы.

Различают три группы методов аутентификации, основанных на наличии у каждого пользователя:

- индивидуального объекта заданного типа;
- знаний некоторой известной только ему и проверяющей стороне информации;
- индивидуальных биометрических характеристик.

Кпервой группе относятся методы аутентификации, использующие удостоверения, пропуска, магнитные карты и другие носимые устройства, которые широко применяются для контроля доступа в помещения, а также входят в состав программно-аппаратных комплексов защиты от НСД к средствам вычислительной техники.

Во вторую группу входят методы аутентификации, использующие пароли. По экономическим причинам они включаются в качестве базовых средств защиты во многие программно-аппаратные комплексы защиты информации. Все современные операционные системы и многие приложения имеют встроенные механизмы парольной защиты.

Последнюю группу составляют методы аутентификации, основанные на применении оборудования для измерения и сравнения с эталоном заданных индивидуальных характеристик пользователя: тембра голоса, отпечатков пальцев, структуры радужной оболочки глаза и др. Такие средства позволяют с высокой точностью аутентифицировать обладателя конкретного биометрического признака, причем "подделать" биометрические параметры практически невозможно. Однако широкое распространение подобных технологий сдерживается высокой стоимостью необходимого оборудования.

Если в процедуре аутентификации участвуют только две стороны, устанавливающие подлинность друг друга, такая процедура называется непосредственной аутентификацией (direct password authentication). Если же в процессе аутентификации участвуют не только эти стороны, но и другие, вспомогательные, говорят об аутентификации с участием доверенной стороны (trusted third party authentication). При этом третью сторону называют сервером аутентификации (authentication server) или арбитром (arbitrator).

Наиболее распространенные методы аутентификации основаны на применении многоразовых или одноразовых паролей. Из-за своего широкого распространения и простоты реализации парольные схемы часто в первую очередь становятся мишенью атак злоумышленников. Эти методы включают следующие разновидности способов аутентификации:

- по хранимой копии пароля или его свёртке (plaintext-equivalent);
- по некоторому проверочному значению (verifier-based);
- без непосредственной передачи информации о пароле проверяющей стороне (zero-knowledge);
- с использованием пароля для получения криптографического ключа (cryptographic).

Впервую разновидность способов входят системы аутентификации, предполагающие наличие у обеих сторон копии пароля или его свертки. Для организации таких систем требуется создать и поддерживать базу данных, содержащую пароли или сверки паролей всех пользователей. Их слабой стороной является то, что получение злоумышленником этой базы данных позволяет ему проходить аутентификацию от имени любого пользователя.

Способы, составляющие вторую разновидность, обеспечивают более высокую степень безопасности парольной системы, так как проверочные значения, хотя они и зависят от паролей, не могут быть непосредственно использованы злоумышленником для аутентификации.

Наконец, аутентификация без предоставления проверяющей стороне какой бы то ни было информации о пароле обеспечивает наибольшую степень защиты. Этот способ гарантирует безопасность даже в том случае, если нарушена работа проверяющей стороны (например, в программу регистрации в системе внедрен "троянский конь").

Особым подходом в технологии проверки подлинности являются криптографические протоколы аутентификации. Такие протоколы описывают последовательность действий, которую должны совершить стороны для взаимной аутентификации, кроме того, эти действия, как правило, сочетаются с генерацией и распределением криптографических ключей для шифрования последующего информационного обмена. Корректность протоколов аутентификации вытекает из свойств задействованных в них математических и криптографических преобразований и может быть строго доказана.

Обычные парольные системы проще и дешевле для реализации, но менее безопасны, чем системы с криптографическими протоколами. Последние обеспечивают более надежную защиту и дополнительно решают задачу распределения ключей. Однако используемые в них технологии могут быть объектом законодательных ограничений.

Для более детального рассмотрения принципов построения парольных систем сформулируем несколько основных определений.

Идентификатор пользователя — некоторое уникальное количество информации, позволяющее различать индивидуальных пользователей парольной системы (проводить их идентификацию). Часто идентификатор также называют именем пользователя или именем учетной записи пользователя.

Пароль пользователя — некоторое секретное количество информации, известное только пользователю и парольной системе, которое может быть запомнено пользователем и предъявлено для прохождения процедуры аутентификации. Одноразовый пароль дает возможность пользователю однократно пройти аутентификацию. Многоразовый пароль может быть использован для проверки подлинности повторно.

Учетная запись пользователя — совокупность его идентификатора и его пароля. База данных пользователей парольной системы содержит учетные записи всех пользователей данной парольной системы.

Под **парольной системой** будем понимать программно-аппаратный комплекс, реализующий системы идентификации и аутентификации пользователей АС на основе одноразовых или многоразовых паролей. Как правило, такой комплекс функционирует совместно с подсистемами разграничения доступа и регистрации событий. В отдельных случаях парольная система может выполнять ряд дополнительных функций, в частности генерацию и распределение кратковременных (сеансовых) криптографических ключей.

Основными компонентами парольной системы являются:

- интерфейс пользователя;
- интерфейс администратора;
- модуль сопряжения с другими подсистемами безопасности;
- база данных учетных записей.

Парольная система представляет собой "передний край обороны" всей системы безопасности. Некоторые ее элементы (в частности, реализующие интерфейс пользователя) могут быть расположены в местах, открытых для доступа потенциальному злоумышленнику. Поэтому парольная система становится одним из первых объектов атаки при вторжении злоумышленника в защищенную систему. Ниже перечислены типы угроз безопасности парольных систем:

1. Разглашение параметров учетной записи через:
   - подбор в интерактивном режиме;
   - подсматривание;
   - преднамеренную передачу пароля его владельцем другому лицу;
   - захват базы данных парольной системы (если пароли не хранятся в базе в открытом виде, для их восстановления может потребоваться подбор или дешифрование);
   - перехват переданной по сети информации о пароле;
   - хранение пароля в доступном месте.
2. Вмешательство в функционирование компонентов парольной системы через:
   - внедрение программных закладок;
   - обнаружение и использование ошибок, допущенных на стадии разработки;
   - выведение из строя парольной системы.

Некоторые из перечисленных типов угроз связаны с наличием так называемого человеческого фактора, проявляющегося в том, что пользователь может:

- выбрать пароль, который легко запомнить и также легко подобрать;
- записать пароль, который сложно запомнить, и положить запись в доступном месте;
- ввести пароль так, что его смогут увидеть посторонние:
- передать пароль другому лицу намеренно или под влиянием заблуждения.

В дополнение к выше сказанному необходимо отметить существование "парадокса человеческого фактора". Заключается он в том, что пользователь нередко стремится выступать скорее противником парольной системы, как, впрочем, и любой системы безопасности, функционирование которой влияет на его рабочие условия, нежели

союзником системы защиты, тем самым ослабляя ее. Защита от указанных угроз основывается на ряде перечисленных ниже организационно-технических мер и мероприятий.

Выбор паролей

В большинстве систем пользователи имеют возможность самостоятельно выбирать пароли или получают их от системных администраторов. При этом для уменьшения деструктивного влияния описанного выше человеческого фактора необходимо реализовать ряд требований к выбору и использованию паролей.

Таблица 1

Требование к выбору пароля	**Получаемый эффект**
Установление минимальной длины пароля	Усложняет задачу злоумышленника при попытке подсмотреть пароль или подобрать пароль методом «тотального опробования»
Использование в пароле различных групп символов	Усложняет задачу злоумышленника при попытке подобрать пароль методом «тотального опробования»
Проверка и отбраковка пароля по словарю	Усложняет задачу злоумышленника при попытке подобрать пароль по словарю
Установление максимального срока действия пароля	Усложняет задачу злоумышленника при попытке подобрать пароль методом «тотального опробования», в том числе без непосредственного обращения к системе защиты (режим off-line)
Установление минимального срока действия пароля	Препятствует попыткам пользователя заменить пароль на старый после его смены по предыдущему требованию
Ведение журнала истории паролей	Обеспечивает дополнительную степень защиты по предыдущему требованию
Применение эвристического алгоритма, бракующего пароли на основании данных журнала истории	Усложняет задачу злоумышленника при попытке подобрать пароль по словарю или с использованием эвристического алгоритма
Ограничение числа попыток ввода пароля	Препятствует интерактивному подбору паролей злоумышленником
Поддержка режима принудительной смены пароля пользователя	Обеспечивает эффективность требования, ограничивающего максимальный срок действия пароля
Использование задержки при вводе неправильного пароля	Препятствует интерактивному подбору паролей злоумышленником
Запрет на выбор пароля самими пользователями и автоматическая генерация паролей	Исключает возможность подобрать пароль по словарю. Если алгоритм генерации паролей не известен злоумышленнику, последний может подбирать пароли только методом «тотального опробования»
Принудительная смена пароля при первой регистрации пользователя в системе	Защищает от неправомерных действия системного администратора, имеющего доступ к паролю в момент создания учетной записи

2. Примеры.

Пример 1.

Задание определить время перебора всех паролей, состоящих из 6 цифр.

Алфавит составляют цифры n=10.

Длина пароля 6 символов k=6.

Таким образом, получаем количество вариантов: $C=n^k=10^6$

Примем скорость перебора s=10 паролей в секунду. Получаем время перебора всех паролей t= C/s=10^5секунд≈1667минут≈28часов≈1,2 дня.

Примем, что после каждого из m=3 неправильно введенных паролей идет пауза в v=5 секунд. Получаем время перебора всех паролей T=t*5/3=16667секунд≈2778минут≈46часов≈1,9 дня.

$T_{итог}$ = t+T = 1,2 + 1,9 = 3,1 дня

Пример 2.

Определить минимальную длину пароля, алфавит которого состоит из 10 символов, время перебора которого было не меньше 10 лет.

Алфавит составляют символы n=10.

Длина пароля рассчитывается: $k=\log_n C= \lg C$.

Определим количество вариантов C= t * s=10лет*10 паролей в сек. = 10*10*365*24*60*60≈3,15* 10^9 вариантов

Таким образом, получаем длину пароля: k=lg (3,15*10^9) = 9,5 Очевидно, что длина пароля должна быть не менее 10 символов.

3. Задания.

1. Определить время перебора всех паролей с параметрами. Алфавит состоит из n символов.

Длина пароля символов k.

Скорость перебора s паролей в секунду.

После каждого из m неправильно введенных паролей идет пауза в v секунд

вариант	n	k	s	m	v
1	33	10	100	0	0
2	26	12	13	3	2
3	52	6	30	5	10
4	66	7	20	10	3
5	59	5	200	0	0
6	118	9	50	7	12
7	128	10	500	0	0
8	150	3	200	5	3
9	250	8	600	7	3
10	500	5	1000	10	10

2. Определить минимальную длину пароля, алфавит которого состоит из n символов, время перебора которого было не меньше t лет.

Скорость перебора s паролей в секунду.

вариант	n	t	s
1	33	100	100
2	26	120	13
3	52	60	30
4	66	70	20

5	59	50	200
6	118	90	50
7	128	100	500
8	150	30	200
9	250	80	600
10	500	50	1000

3. Определить количество символов алфавита, пароль состоит из k символов, время перебора которого было не меньше t лет.

Скорость перебора s паролей в секунду.

вариант	k	t	s
1	5	100	100
2	6	120	13
3	10	60	30
4	7	70	20
5	9	50	200
6	11	90	50
7	12	100	500
8	6	30	200
9	8	80	600
10	50	50	1000

3. Подготовить отчет о выполнение лабораторной работы, который должен включать в себя:

- титульный лист с названиями университета, факультета, кафедры, учебной дисциплины и лабораторной работы, номером варианта, фамилиями и инициалами студента (студентов) и преподавателя, города и года выполнения работы;
- содержание отчета с постраничной разметкой;
- ответы на вопросы, данные в ходе подготовки к выполнению работы;
- сведения о выполнении работы по пунктам с включением содержания задания, копий экранных форм и ответов на вопросы.

3. Промежуточный тест

Банк тестовых заданий размещен на сайте центра цифрового обучения http://moodle.asu.edu.ru

1. По объекту воздействия угрозы бывают:

- воздействующиена информационную среду в целом
- воздействующие на отдельные элементы информационной среды
- активные
- пассивные

2. Выберите правильный вариант ответа. Событие, являющееся следствием одного или нескольких нежелательных или неожиданных событий (информационной безопасности), имеющих значительную вероятность компрометации бизнес-операции и создания угрозы

- инцидент
- нарушение
- сигнал

3. Идентифицированное появление определенного состояния системы, сервиса или сети, указывающего на возможное нарушение политики информационной

безопасности, или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности называется

- событием (информационной безопасности)
- инцидентом (информационной безопасности)
- угрозой (информационной безопасности)

4. Первым шагом в управлении сетью является ее

- документирование
- ревизия
- оформление

5. Какова цель ревизии эффективности?

- Мониторинг и анализ работы сети.
- Определение того, работает ли сеть в соответствии со своим потенциалом.
- Идентификация типов оборудования и устройств, сети.
- Обеспечение информации о восстановлении после сбоя или катастрофического отказа.

Раздел 3. Основы криптографии

1. Вопросы для обсуждения.

1) Криптография как механизм защиты. Понятие криптографии. Методы криптографии.
2) Основные требования к шифрам для криптозащиты информации. Основные типы шифров. Надежность шифров.
3) Электронная цифровая подпись (ЭЦП). определение, предназначение, состав.
4) Технологические основы обработки конфиденциальных документов. Политика безопасности.
5) Система сертификации. Порядок сертификации.
6) Криптографические методы защиты информации в среде Интернет.
7) Шифрование электронной почты. Почтовые клиенты: Outlook, Thinderbird, The Bat.
8) Сертификаты открытого и закрытого ключа.

2. Контрольная работа 2

Вопросы к контрольной работе 2

1. Организация информации в сети Интернет. Службы сети Интернет.Интернет-провайдер (ISP). Адресация. Переадресация. Доменные имена. Длинные доменные имена. Виды доменных имен. Протоколы передачи данных. Семейство протоколов TCP/IP.
2. Интернет. Безопасность. Браузер «Тор». Антивирусное программное обеспечение. Программы блокировки баннерной рекламы. Программы-фильтры спама. Программы восстановления после сбоя.
3. Понятие «социальная сеть». Структура социальной сети. Социальная сеть «Вконтакте». Социальная сеть «Одноклассники». Деструктивная информация.
4. Криптография как механизм защиты. Понятие криптографии. Методы криптографии.
5. Основные требования к шифрам для криптозащиты информации. Основные типы шифров. Надежность шифров.
6. Электронная цифровая подпись (ЭЦП): определение, предназначение, состав.
7. Технологические основы обработки конфиденциальных документов. Политика безопасности.
8. Система сертификации. Порядок сертификации.

9. Криптографические методы защиты информации в среде Интернет. Шифрование электронной почты. Почтовые клиенты: Outlook, Thinderbird, The Bat.
10. Сертификаты открытого и закрытого ключа.

Раздел 4. Средства обеспечения ИБ, в том числе при работе через Интернет

1. Вопросы для обсуждения.

1) Предмет и задачи программно-аппаратной защиты информации, основные подходы к защите данных от НСД.
2) Основные принципы обеспечения информационной безопасности вычислительных систем с помощью программно-аппаратных средств
3) . Функциональные требования по защите вычислительных систем.
4) Особенности программно-аппаратного обеспечения безопасности в интерактивной среде.
5) Защита электронной почты от злонамеренных и нежелательных воздействий, фальшивая и анонимная почта.
6) Защита информационной среды от нежелательных информационных материалов, средства фильтрации сетевой информации/

2. Лабораторная работа 2

Разграничение доступа к ресурсам в защищенных версиях операционной системы Windows

Цель работы: освоение средств защищенных версий операционной системы Windows, предназначенных для

· разграничения доступа субъектов к папкам и файлам;

Подготовка к выполнению работы: по материалам лекций вспомнить и подготовить для включения в отчет о лабораторной работе определения понятий

· *дискреционная политика безопасности*;

· *мандатная политика безопасности*;

· *субъект доступа*;

· *объект доступа*;

Подготовить для включения в отчет о лабораторной работе ответы на следующие вопросы:

1) в чем достоинства и недостатки дискреционной политики безопасности?

2) в чем достоинства и недостатки мандатной политики безопасности?

3) в чем заключается тождественность объектов и тождественность субъектов компьютерной системы?

4) кто определяет права доступа к папкам, файлам, принтерам при использовании дискреционной политики безопасности?

Порядок выполнения работы:

1. После собеседования с преподавателем и получения допуска к работе войти в систему с указанным общим именем учетной записи (с правами обычного пользователя).

2. Освоить средства разграничения доступа пользователей к папкам:

· выполнить команду «Свойства» контекстного меню папки, содержащей отчеты студентов о выполненных лабораторных работах;

· открыть вкладку «Безопасность» и включить в отчет сведения о субъектах, которым разрешен доступ к папке и о разрешенных для них видах доступа;

· с помощью кнопки «Дополнительно» открыть окно дополнительных параметров безопасности папки (вкладка «Разрешения»);

· включить в отчет сведения о полном наборе прав доступа к папке для каждого из имеющихся в списке субъектов;

· открыть вкладку «Владелец», включить в отчет сведения о владельце папки и о возможности его изменения обычным пользователем;

· открыть папку «Аудит», включить в отчет сведения о назначении параметров аудита, устанавливаемых на этой вкладке, и о возможности их установки обычным пользователем;

· закрыть окно дополнительных параметров безопасности и с помощью кнопки «Изменить» а затем кнопки «Добавить» открыть окно выбора пользователя или группы;

· с помощью кнопок «Дополнительно» и «Поиск» открыть список зарегистрированных пользователей и групп и выбрать пользователя с именем своей индивидуальной учетной записи, созданной при выполнении лабораторной работы №1 (или предварительно создав новую учетную запись);

· назначить ему права на полный доступ к папке с отчетами о выполненных лабораторных работах;

· включить в отчет копии экранных форм, использованных при выполнении заданий данного пункта.

3. Освоить средства разграничения доступа пользователей к файлам:

· выполнить команду «Свойства» контекстного меню файла с одним из отчетов о ранее выполненных лабораторных работах;

· повторить все задания п. 2, но применительно не к папке, а к файлу;

· включить в отчет ответ на вопрос, в чем отличие определения прав на доступ к файлам по сравнению с определением прав на доступ к папкам.

4. Ознакомиться с правами доступа к файлам и папкам, назначаемым операционной системой по умолчанию:

· выполнить команду «Свойства» - «Безопасность» контекстного меню одной из папок с документами зарегистрированного в системе пользователя (например, « Мои Документы»);

· включить в отчет сведения о правах доступа пользователей к данной папке и о ее владельце;

· повторить два предыдущих пункта для папки с документами другого зарегистрированного пользователя;

· повторить два предыдущих пункта для папки «Общие документы»;

· включить в отчет о лабораторной работе копии экранных форм, использованных при выполнении данного пункта, и ответы на вопросы

¨ как обеспечивается операционной системой разграничение доступа к личным документам пользователей (по умолчанию);

¨ где (по умолчанию) должны находиться документы, предназначенные для совместного использования.

5. Включить в отчет о лабораторной работе ответы на контрольные вопросы:

· какая политика безопасности лежит в основе разграничения доступа к объектам в защищенных версиях операционной системы Windows?

· в чем уязвимость принятой в защищенных версиях операционной системы Windows политики разграничения доступа?

· как работает механизм наследования при определении прав на доступ субъектов к объектам в защищенных версиях операционной системы Windows?

· какой стандартный механизм работы с личными и общими документами предлагается в защищенных версиях операционной системы Windows и насколько, на Ваш взгляд, он удобен?

· каковы основные виды доступа к файлам и папкам?

6. Подготовить отчет о выполнение лабораторной работы, который должен включать в себя:

- титульный лист с названиями университета, факультета, кафедры, учебной дисциплины и лабораторной работы, номером варианта, фамилиями и инициалами студента (студентов) и преподавателя, города и года выполнения работы;

- содержание отчета с постраничной разметкой;
- ответы на вопросы, данные в ходе подготовки к выполнению работы;
- сведения о выполнении работы по пунктам с включением содержания задания, копий экранных форм и ответов на вопросы;
- ответы на контрольные вопросы.

3. Итоговый тест

Банк тестовых заданий размещен на сайте центра цифрового обучения http://moodle.asu.edu.ru

1. Какова цель ревизии установленного оборудования?

- Идентификация типов оборудования и устройств, сети.
- Идентификация местонахождения каждого элемента сети.
- Мониторинг и анализ работы сети.
- Перенос информации на чертежи здания для создания карты нарезки.

2. Действия, процедуры и механизмы, способные обеспечить безопасность от возникновения угрозы, уменьшить уязвимость, ограничить воздействиеинцидента в системе безопасности, обнаружить инциденты и облегчить восстановление активов - это

- Защитные меры
- Комплексные меры
- Превентивные меры
- Организационные меры

3. Какова цель ревизии средств защиты сети?

- Согласование требований по защите сети со строительными нормами и
- нормами секретности.
- Оценка способностей клиентов пользоваться сетевым оборудованием и
- программным обеспечением.
- Выяснение способности сети гарантировать целостность данных.
- Определение состава аппаратно-программного комплекса, требующегося
- для обеспечения защиты сети.

4. Какие шаги следует предпринять для анализа и решения проблемы в сети после сбора данных о работе?

- Определить, является ли проблема периодической или устойчивой; составить список возможных причин; расставить приоритеты причин.
- Расставить приоритеты причин; используя средства управления сетью или метод замены, идентифицировать причины; отследить тенденции с целью предвидения возникновения проблем в будущем.
- Составить список возможных причин; расставить приоритеты причин; используя средства управления сетью или метод замены, идентифицировать причины.
- Определить, можно ли воспроизвести проблему; расставить приоритеты возможных причин; используя средства управления сетью или метод замены, идентифицировать причины.

5. Что из приведенного ниже должно быть включено в отчет о проведении оценки?

- Состав сетевой аппаратуры и программного обеспечения, которые не удовлетворяют промышленным стандартам.
- Журналы, показывающие тенденцию к уменьшению скорости трафика в определенных сегментах сети.

- Описание случаев и мест несанкционированного доступа к файлам.
- Описание типов пользователей, наиболее часто сталкивающихся с проблемами при пользовании сетью.

Раздел 5. Основные мотивы выдачи информации. Работа с персоналом

1. Вопросы для обсуждения.

1) Понятие о психологическом портрете лояльного сотрудника в сфере информационной безопасности.
2) Типы лояльных сотрудников. Модель лояльного сотрудника в сфере ИБ.
3) Типы нарушителей в сфере ИБ. Модель нарушителя в сфере ИБ.
4) Понятие о психологическом портрете нарушителя в сфере информационной безопасности.
5) Представления. Верные и неверные представления. Примеры.
6) Механизмы общения. Стереотипы мышления и поведения.
7) Личность и ложная личность. Деструктивное и конструктивное начало в личности. Авторитарная личность.
8) Агрессия. Причины агрессии и ненависти.
9) Лидерство. Позитивные и регрессивные виды лидерства.
10) Антилидер и аутсайдер в сфере информационной безопасности.
11) Диссидент в сфере информационной безопасности.
12) Три типа человеческой реакции: адаптация, агрессия, саморефлексия
13) Самоотождествление. Виды самоотождествлений.
14) Диссиденты. Диссиденты и хакеры. Общие черты. Примеры.
15) Методы социальной инженерии.

2. Контрольная работа 3

Вопросы к контрольной работе 3

1) Предмет и задачи программно-аппаратной защиты информации, основные подходы к защите данных от НСД.
2) Основные принципы обеспечения информационной безопасности вычислительных систем с помощью программно-аппаратных средств.
3) Функциональные требования по защите вычислительных систем.
4) Особенности программно-аппаратного обеспечения безопасности в интерактивной среде.
5) Защита электронной почты от злонамеренных и нежелательных воздействий, фальшивая и анонимная почта.
6) Защита информационной среды от нежелательных информационных материалов, средства фильтрации сетевой информации, распространяемой через сеть Интернет.
7) Определение лояльного сотрудника. Определение нарушителя в информационной сфере.
8) Кадровая безопасность и лояльность персонала. Информационная безопасность организации.
9) Типы лояльных сотрудников. Модель лояльного сотрудника в сфере ИБ. Типы нарушителей в сфере ИБ.
10) Модель нарушителя в сфере ИБ. Понятие о психологическом портрете нарушителя в сфере информационной безопасности.

3. Доклад

Тематика докладов

1. Виды информации.
2. Отрасли законодательства, регламентирующие деятельность по защите информации.
3. Государственная тайна как особый вид защищаемой информации и ее характерные признаки.

4. Конфиденциальная информация: персональные данные, служебная тайна, коммерческая тайна, банковская тайна, тайна следствия и судопроизводства, профессиональная тайна.
5. Требования к сотрудникам организации, допущенным к секретной (конфиденциальной) информации.
6. Органы лицензирования и сертификации в области ИБ.
7. Защита электронной почты от злонамеренных и нежелательных воздействий, фальшивая и анонимная почта
8. Порядок организации защиты ПДн
9. Понятие угрозы информационной безопасности. Классификация угроз ИБ
10. Классификация нарушителей информационной безопасности
11. Компьютеные «Вирусы». Их виды
12. Способы борьбы с компьютерными вирусами
13. Семейство протоколов TCP/IP.
14. Понятие и структура социальных сетей.
15. Распространение деструктивного материала через социальные сети и его влияние.
16. Передача информации в среде Интернет.
17. Программное обеспечение для безопасной работы в среде Интернет.
18. Основы конфиденциального документооборота
19. Технологические основы обработки конфиденциальных документов
20. Международные стандарты информационного обмена
21. Требования к сотрудникам организации, допущенным к секретной (конфиденциальной) информации.
22. Определение требований к защищенности информации
23. Понятие о психологическом портрете лояльного сотрудника в сфере информационной безопасности.
24. Типы лояльных сотрудников. Модель лояльного сотрудника в сфере ИБ.
25. Типы нарушителей в сфере ИБ. Модель нарушителя в сфере ИБ.
26. Электронная цифровая подпись (ЭЦП)
27. Криптография как механизм защиты
28. Почтовые клиенты: Outlook, Thinderbird, The Bat.
29. Криптографические методы защиты информации.
30. Политика безопасности.
31. Общие положения сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности.
32. Система сертификации.
33. Порядок сертификации.

Вопросы к зачёту

1. Определение понятий «Информация» «Информационная безопасность», «Субъекты информационных отношений».
2. Категорирование информации.
3. Виды возможных нарушений информационной системы. Общая классификация информационных угроз.
4. Объект и субъект защиты информации.
5. Определение понятия «Система информационной безопасности».
6. Допуск должностных лиц и граждан РФ к ГТ. Основания отказа должностному лицу или гражданину в допуске к ГТ.
7. Общие положения ФЗ «О государственной тайне». Порядок отнесения сведений к государственной тайне (ГТ).
8. Порядок засекречивания и рассекречивания. Сведения, не подлежащие отнесению к ГТ.

9. Степени секретности сведений, составляющих ГТ. Порядок распоряжения сведениями, составляющими ГТ.
10. Правовое урегулирование защиты информации. Стандарты ИБ Основы конфиденциального документооборота.
11. Особенности работы с персоналом, владеющим конфиденциальной информацией.
12. Регулирование правовых отношений в области защиты государственной тайны.
13. Конституция РФ. Федеральные законы, нормативные правовые акты в области информационной безопасности и защиты информации.
14. Законодательство о персональных данных. Принципы и условия обработки персональных данных, их конфиденциальность. Права субъектов персональных данных.
15. Право на доступ к персональным данным. Обязанности оператора при обработке персональных данных. Контроль и надзор.
16. Особенности программно-аппаратного обеспечения безопасности в интерактивной среде.
17. Предмет и задачи программно-аппаратной защиты информации.
18. Классификация типовых программно-аппаратных средств обеспечения ИБ
19. Понятие о психологическом портрете.
20. Понятие о психологическом портрете лояльного сотрудника в сфере информационной безопасности.
21. Типы лояльных сотрудников. Модель лояльного сотрудника в сфере ИБ.
22. Типы нарушителей в сфере ИБ. Модель нарушителя в сфере ИБ.
23. Понятие о психологическом портрете нарушителя в сфере информационной безопасности.
24. Представления.
25. Верные и неверные представления. Примеры.
26. Предположительный психологический портрет нарушителя в сфере информационной безопасности.
27. Предположительный психологический портрет лояльного сотрудника в сфере информационной безопасности.
28. Управление доступом пользователей в опреационных системах
29. Криптография – как механизм защиты информации. Безопасность информации и защита информации.
30. Основные требования к шифрам для криптозащиты информации. Основные типы шифров.
31. ЭЦП: определение, предназначение, состав.
32. Общие положения сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности.
33. Система сертификации.
34. Криптографические методы защиты информации в среде Интернет.
35. Почтовые клиенты: Outlook, Thinderbird, The Bat. Сертификаты открытого и закрытого ключа.
36. Организация информации в сети Интернет.
37. Службы и протоколы сети Интернет: название службы, назначение и соответствующий протокол.
38. Сетевая безопасность. Антивирусные программы. Описание, примеры, достоинства и недостатки.
39. Социальные сети. Понятие, структура, типы, назначение, возможности. Примеры.
40. Деструктивная информация и ее распространение в среде Интернет.
41. Антивирусное программное обеспечение.
42. Программы блокировки баннерной рекламы.
43. Программы-фильтры спама.

44. Программы восстановления после сбоя.

Таблица 9 – Примеры оценочных средств с ключами правильных ответов

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
ПК-3. Способен осуществлять разработку краткосрочной и долгосрочной экономической, внешнеэкономической, финансовой политик предприятий, учреждений, организаций различных организационно-правовых форм и их отдельных подразделений с учетом построения интегрированной системы управления рисками организации.				
1.	Задание закрытого типа	К угрозам информационной безопасности со стороны человеческого фактора НЕ относятся: 1) Действия уволенных или недовольных сотрудников 2) Анализаторы протоколов 3) Халатность 4) Низкая квалификация работников	2	2
2.		К техническим средствам обеспечения информационной безопасности и защиты информации относятся: 1) Недопущение ведения важных работ одним человеком 2) Резервирование особо важных компьютерных подсистем 3) Защита авторских прав программистов	2	2
3.		К техническим угрозам информационной безопасности НЕ относится: 1) Ошибки в программном обеспечении 2) Сетевые атаки, в том числе DoS- и DDoS-атаки 3) Промышленный шпионаж 4) Компьютерные вирусы, черви, троянские кони	3	2
4.		К организационным средствам обеспечения информационной безопасности и защиты информации относятся: 1) Совершенствование законодательства и судопроизводства 2) Тщательный подбор персонала 3) Установка средств обнаружения и тушения пожара, обнаружения утечек воды	2	2
5.		Цели защиты информации (указать несколько правильных ответов): 1) Целостность данных 2) Конфиденциальность данных 3) Доступность данных 4) Открытость данных	1,2,3	2
6.	Задание открытого типа	Какие меры относится к правовым мерам, направленным на обеспечение информационной безопасности и защиты информации?	Правовые нормы: разработка норм, устанавливающих ответственность за компьютерные	2

			преступления; защита авторских прав программистов; совершенствование законодательства и судопроизводства; общественный контроль за разработчиками компьютерных систем и приятие международных договоров, регламентирующих эту деятельность.	
7.		Какие меры относится к техническим мерам, направленным на обеспечение информационной безопасности и защиты информации?	Технические меры: защита от несанкционированного доступа к информационной системе; резервирование особо важных компьютерных подсистем; организация вычислительных сетей с возможностью перераспределения ресурсов при нарушении в работе отдельных звеньев; установка средств обнаружения и тушения пожара, обнаружение утечек воды; принятие конструкционных мер защиты от хищений, диверсий, взрывов; установка резервного электропитания, оснащение помещений замками, сигнализацией.	2
8.		В чем заключаются права обладателя информации в соответствии с ФЗ № 149 «Об информации, информационных технологиях и защите информации»?	Обладатель информации вправе: • разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа; • использовать информацию, в том числе распространять ее по своему усмотрению; • передавать информацию другим лицам по договору или на ином установленном законом основании.	2
9.		Какие меры относится к организационным мерам, направленным на обеспечение информационной безопасности и защиты информации?	Организационные меры: охрана вычислительного центра (ВЦ); тщательный подбор персонала; недопущение ведения	2

			важных работ одним человеком; наличие плана восстановления работоспособности ВЦ после выхода его из строя; обслуживание ВЦ сторонней организацией или лицами, незаинтересованными в сокрытии факторов нарушения работы центра; выбор места расположения центра.	
10.		Правило разграничения доступа	Правило разграничения доступа заключается в следующем: лицо допускается к работе с документом только в том случае, если уровень допуска субъекта доступа равен или выше уровня конфиденциальности документа, а в наборе категорий, присвоенных данному субъекту доступа, содержатся все категории, определенные для данного документа.	2
11.	Задания закрытого типа	Согласно Федеральному закону «Об информации, информационных технологиях и о защите информации» не может быть ограничен доступ к (указать несколько правильных ответов): 1) Информации о состоянии окружающей среды 2) Персональным данным граждан (физических лиц) 3) Информации о деятельности государственных органов и органом местного самоуправления, а также об использовании бюджетных средств	1,3	2
12.		Согласно Федеральному закону «Об информации, информационных технологиях и о защите информации» запрещается распространение информации, которая направлена на (указать несколько правильных ответов): 1) Пропаганду войны 2) Разжигание национальной вражды 3) Разжигание расовой или религиозной ненависти и вражды	1,2,3	2
13.		Конституция РФ содержит следующие нормы (указать несколько правильных ответов): 1) Конституция имеет высшую юридическую силу, прямое	1,3	2

		действие и применяется на всей территории Российской Федерации 2) Законы и иные правовые акты не должны противоречить Конституции РФ 3) Нормы международного права и международные договоры РФ являются частью ее правовой системы. Если международным договором РФ установлены иные правила, чем предусмотренные законом, то применяются правила международного договора		
14.		Согласно Федеральному закону «Об информации, информационных технологиях и о защите информации» защита информации есть принятие мер, направленных на (указать несколько правильных ответов): 1) Предотвращение неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения и иных неправомерных действий в отношении информации 2) Соблюдение конфиденциальности информации ограниченного доступа 3) Реализацию права доступа к информации	1,2,3	2
15.		Конституция РФ гарантирует следующие права и свободы (указать несколько правильных ответов): 1) Свободу мысли и слова 2) Право собираться мирно, без оружия, проводить собрания, митинги и демонстрации, шествия и пикетирование 3) Свободу массовой информации	1,2,3	2
16.	Задания открытого типа	Что понимается под тайной, секретностью и конфиденциальностью информации?	Тайна, или секретность и конфиденциальность информации, – это состояние информации в определенный период времени, которое характеризуется ограничением на ее распространение и доступ к ней в связи с ее защитой и охраной государством или иным обладателем документированной информации. Конфиденциальная информация (документы), составляющая тайну, за исключением государственной, –	2

			информация ограниченного доступа и распространения.	
17.		Каким требованиям должна отвечать информация, отнесенная к служебной тайне?	Информация может являться служебной тайной, если она отвечает следующим требованиям: • отнесена федеральным законом к служебной информации о деятельности государственных органов, доступ к которой ограничен по закону или в силу служебной необходимости; • является конфиденциальной информацией другого лица (коммерческая тайна, банковская тайна, секрет производства (ноу-хау), служебный секрет производства, персональные данные); • не является государственной тайной и не попадает под перечень сведений, составляющих государственную тайну; • получена представителем государственного органа или органа местного самоуправления только в силу исполнения обязанностей по службе в случаях и в порядке, установленных федеральным законодательством, и имеет действительную или потенциальную ценность в силу неизвестности ее третьим лицам.	4
18.		Основные направления обеспечения информационной безопасности в области обороны страны в соответствии с военной политикой Российской Федерации	В соответствии с военной политикой Российской Федерации основными направлениями обеспечения информационной безопасности в области обороны страны являются: а) стратегическое сдерживание и предотвращение военных конфликтов, которые могут возникнуть в результате применения информационных технологий;	4

			б) совершенствование системы обеспечения информационной безопасности Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов, включающей в себя силы и средства информационного противоборства; в) прогнозирование, обнаружение и оценка информационных угроз, включая угрозы Вооруженным Силам Российской Федерации в информационной сфере; г) содействие обеспечению защиты интересов союзников Российской Федерации в информационной сфере; д) нейтрализация информационно-психологического воздействия, в том числе направленного на подрыв исторических основ и патриотических традиций, связанных с защитой Отечества.	
19.		Дать определение информационной безопасности Российской Федерации	Информационная безопасность Российской Федерации - состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства	2
20.		Что понимается под системой защиты от несанкционированного использования и копирования	Под системой защиты от несанкционированного использования и копирования понимается комплекс программных или программно-аппаратных средств, предназначенных	2

			для усложнения или запрещения нелегального распространения, использования и (или) изменения программных продуктов и иных информационных ресурсов.	

Полный комплект оценочных материалов по дисциплине (модулю) (фонд оценочных средств) хранится в электронном виде на кафедре, утверждающей рабочую программу дисциплины (модуля), и в Центре мониторинга и аудита качества обучения.

Методические рекомендации по выполнению лабораторных и контрольных работ, проведению экзамена

Отчет по лабораторной работе

Отчет по лабораторной работе представляется в электронном виде. Защита отчета проходит в форме доклада студента по выполненной работе и ответов на вопросы преподавателя. В случае, если оформление отчета и поведение студента во время защиты соответствуют указанным требованиям, студент получает максимальное количество баллов.

Основаниями для снижения количества баллов в диапазоне от max до min являются:

- отсутствие списка использованной литературы,
- небрежное выполнение,
- отсутствие выводов.

Отчет не может быть принят и подлежит доработке в случае:

- отсутствия необходимых разделов,
- отсутствия необходимого графического материала,
- неверных результатов расчета.

В отчете по выполненной лабораторной работе должны быть указаны:

- тема лабораторной работы,
- пакет документов в соответствии с темой лабораторной работы,
- использованная литература.

Критерии оценки:

– оценка «отлично» выставляется обучающемуся, если студент продемонстрировал глубокие знания теоретического материала и умение их применять, обоснованно изложил свои мысли, сделал необходимые выводы;

– оценка «хорошо» выставляется обучающемуся, если студент продемонстрировал глубокие знания теоретического материала и умение их применять, обоснованно изложил свои мысли, сделал необходимые выводы, допущены некоторые неточности, имеется одна негрубая ошибка;

– оценка «удовлетворительно» выставляется обучающемуся, если студент ответил на вопросы преимущественно верно, имеются затруднения в формулировке выводов, имеются одна или две негрубые ошибки;

– оценка «неудовлетворительно» выставляется обучающемуся, если студент не дал ответы на поставленные вопросы, обоснования неверные, либо дан верный ответ без его обоснования, сделаны грубые ошибки, отсутствуют знания по основам математики.

Контрольные работы

Контрольная работа состоит из 2-х заданий.

Основаниями для снижения оценки за задание являются:

- ошибки в объяснениях и комментариях при верно выполненном задании;
- неполный ответ для теоретический заданий;
- небрежное выполнение;

- многократное переписывание контрольной работы.

Задание не может быть засчитано, если:

- даны два неверных ответа на теоретические вопросы.

Метод "золотого сечения"

Критерии оценки контрольных работ:

– оценка «отлично» выставляется обучающемуся, если студент продемонстрировал глубокие знания теоретического материала и умение их применять, обоснованно изложил свои мысли, сделал необходимые выводы и учел основные нормативно-правовые документы по информационной безопасности;

– оценка «хорошо» выставляется обучающемуся, если студент продемонстрировал глубокие знания теоретического материала и умение их применять, обоснованно изложил свои мысли, сделал необходимые выводы и учел основные нормативно-правовые документы по информационной безопасности, допущены некоторые неточности, имеется одна негрубая ошибка.

– оценка «удовлетворительно» выставляется обучающемуся, если студент ответил на вопросы преимущественно верно, имеются затруднения в формулировке выводов, имеются одна или две негрубые ошибки, учтены не все нормативно-правовые документы по информационной безопасности;

– оценка «неудовлетворительно» выставляется обучающемуся, если студент не дал ответы на поставленные вопросы, обоснования неверные, либо дан верный ответ без его обоснования, сделаны грубые ошибки, отсутствуют знания нормативно-правовых документов по информационной безопасности.

Критерии оценки теста:

- оценка «отлично» выставляется студенту, если он умеет безошибочно самостоятельно обрабатывать и интерпретировать данные при решении задач, как в стандартной, так и в нестандартной формулировке;
- оценка «хорошо» выставляется студенту, если он умеет безошибочно самостоятельно обрабатывать и интерпретировать данные при решении задач в стандартной ситуации или за верное решение 75% - 89% заданий теста;
- оценка «удовлетворительно» выставляется студенту, если он умеет при решении задач обрабатывать данные с опорой на справочные материалы и помощь преподавателя, верно выполняя при этом 60% - 74% работы.
- оценка «неудовлетворительно» выставляется студенту, если он не умеет правильно обрабатывать данные, выполнил менее 60% заданий теста.

- оценка «зачтено» выставляется студенту, если тест студента оценен не ниже чем «удовлетворительно»;

- оценка «не зачтено», если тест оценен ниже чем «удовлетворительно».

Экзамен

Экзамен заключается в письменном ответе на 2 теоретических вопроса и устном собеседовании по каждому теоретическому вопросу.

Основаниями для снижения оценки за теоретический вопрос являются:

- небрежное выполнение;
- неполный ответ;
- наличие мелких неточностей или незначительных искажений фактов;
- неточные объяснения при собеседовании;
- отсутствие ответов на заданные при собеседовании вопросы.

В соответствии с балльно-рейтинговой системой БАРС по дисциплине на экзамен отводится 100 баллов (40 баллов на текущие формы контроля, 10 баллов на бонусы и 50 баллов отводится на экзамен),

Оценивание студентов на экзамене осуществляется в соответствие с требованиями и критериями 100-балльной шкалы. Учитываются как результаты текущего контроля, так и знания, навыки и умения, непосредственно показанные студентами в ходе экзамена.

Критерии оценок на экзамене:

40-50 баллов – студент глубоко понимает пройденный материал, отвечает четко и всесторонне, умеет оценивать факты, самостоятельно рассуждает, отличается способностью обосновать выводы и разъяснять их в логической последовательности.

35-39 баллов – студент глубоко понимает пройденный материал, отвечает четко и всесторонне, умеет оценивать факты, самостоятельно рассуждает, отличается способностью обосновать выводы и разъяснять их в логической последовательности, но допускает отдельные неточности.

25-34 балла – студент глубоко понимает пройденный материал, отвечает четко и всесторонне, умеет оценивать факты, самостоятельно рассуждает, отличается способностью обосновать выводы и разъяснять их в логической последовательности, но допускает некоторые ошибки общего характера.

20-24 балла – студент хорошо понимает пройденный материал, но не может теоретически обосновать некоторые выводы.

15-19 баллов – студент отвечает в основном правильно, но чувствуется механическое заучивание материала.

11-14 баллов – в ответе студента имеются существенные недостатки, материал охвачен «половинчато», в рассуждениях допускаются ошибки.

10 баллов – ответ студента правилен лишь частично, при разъяснении материала допускаются серьезные ошибки.

6-9 баллов – студент имеет общее представление о теме, но не умеет логически обосновать свои мысли.

1-5 баллов – студент имеет лишь частичное представление о теме. 0 баллов – нет ответа.

Таблица 10 – Технологическая карта рейтинговых баллов по дисциплине (модулю)

№ п/п	Контролируемые мероприятия	Количество мероприятий / баллы	Максимальное количество баллов	Срок представления
Основной блок				
1.	*Ответ на занятии*	9/2	18	По расписанию
2.	*Выполнение лабораторной работы*	2/6	12	
3.	*Выполнение контрольной работы*	3/8	24	
4.	*Тест*	3/8	24	
5.	*Реферат*	1/12	12	
Всего			**90**	-
Блок бонусов				
6.	*Посещение занятий без пропусков*	1	3	
7.	*Своевременное выполнение всех заданий*	1	3	
8.	*Активность студента на занятии*	1	4	
Всего			**10**	-
ИТОГО			**100**	-

Таблица 11 – Система штрафов (для одного занятия)

Показатель	Балл
Опоздание на занятие	- 1
Нарушение учебной дисциплины	- 1
Неготовность к занятию	- 2
Пропуск занятия без уважительной причины	- 2

Таблица 12 – Шкала перевода рейтинговых баллов в итоговую оценку за семестр по дисциплине (модулю)

Сумма баллов	Оценка по 4-балльной шкале	
90–100	5 (отлично)	Зачтено
85–89	4 (хорошо)	
75–84		
70–74		
65–69	3 (удовлетворительно)	
60–64		
Ниже 60	2 (неудовлетворительно)	Не зачтено

При реализации дисциплины (модуля) в зависимости от уровня подготовленности обучающихся могут быть использованы иные формы, методы контроля и оценочные средства, исходя из конкретной ситуации.

8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

8.1. Основная литература

1. Основы информационной безопасности : Учебное пособие для вузов / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. - М. : Горячая линия - Телеком, 2011. – URL : http://www.studentlibrary.ru/book/ISBN5935172925.html (ЭБС «Консультант студента»).
2. Информационная безопасность: защита и нападение [Электронный ресурс] / Бирюков А.А. - М. : ДМК Пресс, 2012. - URL : http://www.studentlibrary.ru/book/ISBN9785940746478.html (ЭБС «Консультант студента»).
3. Технические, организационные и кадровые аспекты управления информационной безопасностью: Учебное пособие для вузов / Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. - Вып. 4. - М. : Горячая линия - Телеком, 2013. - (Серия "Вопросы управления информационной безопасностью"). - URL: http://www.studentlibrary.ru/book/ISBN9785991202749.html (ЭБС «Консультант студента»).

8.2. Дополнительная литература:

1. Хорев, П.Б. Программно-аппаратная защита информации : рек. кафедрой информационной безопасности Российского государственного социального университета для студентов вузов, обучающихся по направлениям "Информационная безопасность" и "Информатика и вычислительная техника" / П. Б. Хорев. - М. : ФОРУМ, 2009. - 352 с. - (Высшее образование). - ISBN 978-5-91134-353-8. (12 экз.)

2. Мельников, В.П. Информационная безопасность и защита информации [Текст] : учеб.пособие для вузов / В.П. Мельников, С.А. Клейменов, А.М. Петраков; под ред. С.А. Клейменова. – 4-е изд., стер. – М. : Академия, 2009. – 332 с. (19 экз.)

3. Информационная безопасность и защита информации / Шаньгин В.Ф. - М. : ДМК Пресс, 2014. - URL: http://www.studentlibrary.ru/book/ISBN9785940747680.html (ЭБС «Консультант студента»).
4. Защита информации: учебное пособие / Ю.М. Краковский - Ростов н/Д : Феникс, 2016. - (Высшее образование). URL: - http://www.studentlibrary.ru/book/ISBN9785222269114.html (ЭБС «Консультант студента»).

8.3. Интернет-ресурсы, необходимые для освоения дисциплины (модуля)

1. **Электронно-библиотечная система (ЭБС) ООО «Политехресурс» «Консультант студента».** Многопрофильный образовательный ресурс «Консультант студента» является электронной библиотечной системой, предоставляющей доступ через

сеть Интернет к учебной литературе и дополнительным материалам, приобретенным на основании прямых договоров с правообладателями. Каталог в настоящее время содержит около 15000 наименований. www.studentlibrary.ru.

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Для проведения лекционных занятий необходима мультимедийная аудитория, оснащенная компьютерной презентационной техникой.

Для проведения публичной защиты проектов, необходима мультимедийная аудитория с проектором.

Рабочая программа дисциплины (модуля) при необходимости может быть адаптирована для обучения (в том числе с применением дистанционных образовательных технологий) лиц с ограниченными возможностями здоровья, инвалидов. Для этого требуется заявление обучающихся, являющихся лицами с ограниченными возможностями здоровья, инвалидами, или их законных представителей и рекомендации психолого-медико-педагогической комиссии. Для инвалидов содержание рабочей программы дисциплины (модуля) может определяться также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).

10. ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ (МОДУЛЯ) ПРИ ОБУЧЕНИИ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Рабочая программа дисциплины (модуля) при необходимости может быть адаптирована для обучения (в том числе с применением дистанционных образовательных технологий) лиц с ограниченными возможностями здоровья, инвалидов. Для этого требуется заявление обучающихся, являющихся лицами с ограниченными возможностями здоровья, инвалидами, или их законных представителей и рекомендации психолого-медико-педагогической комиссии. При обучении лиц с ограниченными возможностями здоровья учитываются их индивидуальные психофизические особенности. Обучение инвалидов осуществляется также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).

Для лиц с нарушением слуха возможно предоставление учебной информации в визуальной форме (краткий конспект лекций; тексты заданий, напечатанные увеличенным шрифтом), на аудиторных занятиях допускается присутствие ассистента, а также сурдопереводчиков и тифлосурдопереводчиков. Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменно отвечает на вопросы, письменно выполняет практические задания. Доклад (реферат) также может быть представлен в письменной форме, при этом требования к содержанию остаются теми же, а требования к качеству изложения материала (понятность, качество речи, взаимодействие с аудиторией и т. д.) заменяются на соответствующие требования, предъявляемые к письменным работам (качество оформления текста и списка литературы, грамотность,

наличие иллюстрационных материалов и т.д.). Промежуточная аттестация для лиц с нарушениями слуха проводится в письменной форме, при этом используются общие критерии оценивания. При необходимости время подготовки к ответу может быть увеличено.

Для лиц с нарушением зрения допускается аудиальное предоставление информации, а также использование на аудиторных занятиях звукозаписывающих устройств (диктофонов и т.д.). Допускается присутствие на занятиях ассистента (помощника), оказывающего обучающимся необходимую техническую помощь. Текущий контроль успеваемости осуществляется в устной форме. При проведении промежуточной аттестации для лиц с нарушением зрения тестирование может быть заменено на устное собеседование по вопросам.

Для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, на аудиторных занятиях, а также при проведении процедур текущего контроля успеваемости и промежуточной аттестации могут быть предоставлены необходимые технические средства (персональный компьютер, ноутбук или другой гаджет); допускается присутствие ассистента (ассистентов), оказывающего обучающимся необходимую техническую помощь (занять рабочее место, передвигаться по аудитории, прочитать задание, оформить ответ, общаться с преподавателем).