МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Российский государственный гуманитарный университет»
(ФГБОУ ВО «РГГУ»)

ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ
ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ СИСТЕМ И БЕЗОПАСНОСТИ
Кафедра комплексной защиты информации

ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Направление подготовки 10.03.01 Информационная безопасность
Направленность (профили) подготовки:
Безопасность автоматизированных систем
Уровень квалификации выпускника – бакалавр

Форма обучения – очная

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2021

Защита от несанкционированного доступа к информации в автоматизированных системах
Рабочая программа дисциплины
Составитель:
Кандидат военных наук, доцент кафедры КЗИ Д.Н. Баранников

Ответственный редактор
Кандидат технических наук, и.о. зав. кафедрой КЗИ Д.А. Митюшин

УТВЕРЖДЕНО
Протокол заседания кафедры
комплексной защиты информации
№_10_ от__20.05.2021 г._____

ОГЛАВЛЕНИЕ

1. Пояснительная записка

1.1. Цель и задачи дисциплины

Цель дисциплины – получение знаний по существующим угрозам информационной безопасности, применению современных методов и способов защиты информации от несанкционированного доступа (НСД); формирование навыков, необходимых для защиты информации от НСД в современных информационных системах.
Задачи дисциплины:
– овладение методами решения профессиональных задач по защите информации от НСД;
– формирование навыков работы с современными средствами защиты информации от НСД.

1.2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций

Компетенция (код и наименование)	**Индикаторы компетенций** (код и наименование)	**Результаты обучения**
ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности	*ОПК-5.1 Знает основы законодательства Российской Федерации, нормативные правовые акты, нормативные и методические документы в области информационной безопасности и защиты информации, правовые основы организации защиты государственной тайны и конфиденциальной информации, правовую характеристику преступлений в сфере компьютерной информации и меры ответственности за утрату, разглашение, модификацию и уничтожение защищаемой информации*	*Знать:* • *Основы законодательства РФ, нормативные правовые акты;* • *Нормативные и методические документы в области информационной безопасности и защиты информации;* • *Правовые основы организации защиты государственной тайны и конфиденциальной информации;* • *Правовую характеристику преступлений в сфере компьютерной информации и меры ответственности за утрату, разглашение, модификацию и уничтожение защищаемой информации;*
	ОПК-5.2 Умеет обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей, предпринимать необходимые меры по восстановлению нарушенных прав	*Уметь:* • *обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей;* • *предпринимать необходимые меры по восстановлению нарушенных прав;*
	ОПК-5.3 Владеет навыками разрабатывать практы локальных правовых документов, регламентирующих работу по обеспечению информационной безопасности в организации	*Владеть:* • *навыками разработки локальных правовых документов, регламентирующих работу по обеспечению информационной безопасности в организации*

ПК-13 Способен принимать участие в формировании, организации и поддержания выполнения комплекса мер по обеспечению информационной безопасности, управлении процессом их реализации	*ПК-13.1* *Знает процедуру организации установки и настройки технических, программных (программно-технических) средств защиты информации, входящих в состав системы защиты информации организации, в соответствии с техническим проектом и инструкциями по эксплуатации*	*Знать:* • *процедуру организации установки и настройки технических, программных (программно-технических) средств защиты информации, входящих в состав системы защиты информации организации, в соответствии с техническим проектом и инструкциями по эксплуатации;*
	ПК-13.2 *Владеет навыками организации и сопровождения аттестации объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации*	*Владеть:* • *навыками организации процесса аттестации объектов вычислительной техники и выделенных помещений;* • *навыками сопровождения аттестации объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации сетей*
	ПК-13.3 *Умеет разрабатывать и реализовывать организационные меры, обеспечивающие эффективность системы защиты информации*	*Уметь:* • *разрабатывать и реализовывать организационные меры, обеспечивающие эффективность системы защиты информации*
ПК-8 Способен осуществлять мониторинг и аудит защищенности информации в автоматизированных системах	*ПК-8.1* *Знает основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах, организационные меры по защите информации*	*Знать:* • *основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах;* • *организационные меры по защите информации;*
	ПК-8.2 *Умеет анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах; вести протоколы и журналы учета при осуществлении аудита систем защиты информации автоматизирован-*	*Уметь:* • *анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем;* • *выявлять потенциальные уязвимости безопасности информации в автоматизированных системах;* • *вести протоколы и журналы учета при осуществлении аудита систем защиты информации автоматизированных*

	ных систем	*систем*
	ПК-8.3 *Владеет навыками выработки рекомендаций для принятия решения о модернизации системы защиты информации автоматизированной системы*	*Владеть:* • *навыками выработки рекомендаций для принятия решения о модернизации системы защиты информации автоматизированной системы*

1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Защита от несанкционированного доступа к информации в автоматизированных системах» относится к части, формируемой участниками образовательных отношений, блока дисциплин учебного плана.

Для освоения дисциплины необходимы знания, умения и владения, сформированные в ходе изучения следующих дисциплин и прохождения практик: «Правовое обеспечение информационной безопасности», «Организационной обеспечение информационной безопасности», «Информационные технологии».

В результате освоения дисциплины формируются знания, умения и владения, необходимые для изучения следующих дисциплин и прохождения практик: «Безопасность операционных систем», «Безопасность программного обеспечения автоматизированных систем», «Эксплуатационная практика», «Аттестация объектов информатизации».

2. Структура дисциплины

Структура дисциплины для очной формы обучения

Общая трудоёмкость дисциплины составляет _3_ з.е., _114__ ч., в том числе контактная работа обучающихся с преподавателем _60_ ч., промежуточная аттестация __ ч., самостоятельная работа обучающихся _54_ ч.

№ п/п	Темы дисциплины/	Семестр	Виды учебной работы (в часах)						Формы текущего контроля успеваемости, форма промежуточной аттестации *(по семестрам)*
			контактная					Самостоятельная работа	
			Лекции	Семинар	Практические занятия	Лабораторные занятия	Промежуточная аттестация		
1	*Введение в защиту информации от несанкционированного доступа*	**5**	**2**						Опрос, выполнение практического задания
2	*Требования к защите информации от несанкционированного доступа*	**5**	**2**		**6**			**9**	Опрос, выполнение практического задания
3	*Авторизация. Методы идентификации и аутентификации пользователя*	**5**	**4**		**6**			**9**	Опрос, выполнение практического задания
4	*Управление доступом к ресурсам*	**5**	**4**		**6**			**9**	Опрос, выполнение практического задания
5	*Разработка поли-тики безопасности информационной системы*	**5**	**4**		**6**			**9**	Опрос, выполнение практического задания
6	*Методика анализа защищённости ИС. Методы и средства выявления угроз её информационной безопасности*	**5**	**4**		**6**			**9**	Опрос, выполнение практического задания
7	*Применение средств аппаратной защиты*	**5**	**4**		**6**			**9**	Опрос, выполнение практического задания
	Зачет с оценкой								*зачет по билетам*
	итого:		**24**		**36**			**54**	

3. Содержание дисциплины

Тема 1. Введение в защиту информации от несанкционированного доступа
Основные термины и определения ЗИ от НСД. Классификация требований к системам защиты от НСД. Ответственность за НСД. Документы Гостехкомиссии (ФСТЭК) России по защите от НСД. Система государственных нормативных актов, стандартов, руководящих документов и требований по ЗИ от НСД. Особенности современных АС. Виды угроз современным АС. Классы защищённости СВТ и АС. Показатели защищённости межсетевых экранов и их увязка с классами защищённости АС.

Тема 2. Требования к защите информации от несанкционированного доступа
Формализованные требования к ЗИ от НСД. Классы защищённости СВТ. Классификация АС по защищённости от НСД. Состав первой группы защиты АС. Подсистемы механизма ЗИ от НСД. Требования к защите информации АС групп 1Г и 1В.

Тема 3. Методы идентификации и аутентификации пользователя
Понятие идентификации и аутентификации. Процедура авторизации. Формализованные и дополнительные требования к идентификации и аутентификации. Авторизация в контексте количества и вида зарегистрированных пользователей. Рекомендации по построению авторизации, исходя из вида и количества зарегистрированных пользователей. Классификация задач, решаемых механизмами идентификации и аутентификации. Критерии классификации. Механизмы парольной защиты. Функциональное назначение и реализация механизмов парольной защиты. Угрозы преодоления парольной защиты. Явные и скрытые угрозы. Основные механизмы ввода пароля. Биометрический и комбинированный способ ввода пароля. Способы усиления парольной защиты. Добавочные механизмы усиления парольной защиты и требования к ним. Двухуровневая авторизация на уровне ОС и BIOS. Сетевая авторизация. Протоколы аутентификации.

Тема 4. Управление доступом к ресурсам
Основные способы разделения доступа субъектов к совместно используемым объектам. Абстрактные модели доступа. Модели Биба, Гогена-Мезигера, Кларка-Вильсона, Сазерлендская модель. Дискреционная (матричная) модель. Многоуровневые (мандатные) модели. Понятия «владелец» и «собственник» информации.
Базовые модели доступа. Дискреционное разграничение доступа. Матрица доступа и домен безопасности. Список прав доступа ACL. Мандатное разграничение доступа. Ролевая модель разграничения доступа. Управления доступом на основе атрибутов. Выбор модели разграничения доступа.
Корректность и полнота реализации разграничительной политики доступа. Классификация субъектов и объектов доступа. Требования к механизмам управления доступом.
Централизованное и децентрализованное управление доступом. Протоколы аутентификации (AAA). RADIUS, TACACS.

Тема 5. Разработка политики безопасности информационной системы
Общие положения разработки политики безопасности. Нормативные документы по разработке политики безопасности. Важные аспекты при разработке политик безопасности. Средства защиты информации для государственных и коммерческих структур. Процесс разработки политики безопасности. Примерный состав группы по разработке политик безопасности. Требования к политикам безопасности. Типовые политики безопасности.
Реализация политик безопасности. Общие правила безопасности. Архитектура корпоративной системы защиты информации. Настройки основных компонент системы защиты компании.

Тема 6. Методика анализа защищённости ИС. Методы и средства выявления угроз её информационной безопасности

Типовая методика анализа защищённости ИС. Методы тестирование систем информационной безопасности. Методы количественной оценки систем информационной безопасности. Методы и средства анализа защищённости автоматизированной системы. Анализ защищённости внешнего периметра корпоративной сети. Анализ защищённости внутренней инфраструктуры сети. Инструментальные средства анализа защищённости. Методы предотвращения сетевых атак на периметр сети.

Тема 7. Применение средств аппаратной защиты

Необходимость и принципы использования аппаратных средств защиты. Угрозы перевода системы защиты в пассивное состояние, их реализация. Методы противодействия угрозам перевода системы защиты в пассивное состояние. Реализация программно-аппаратного контроля (мониторинга) активности системы защиты. Метод контроля целостности и активности программных компонент системы защиты программно-аппаратными средствами. Механизм удалённого мониторинга активности системы защиты, как альтернатива применению аппаратной компоненты защиты. Метод контроля вскрытия аппаратуры, общий подход. Реализация системы контроля вскрытия аппаратуры. Принципы комплексирования средств защиты информации

4. Образовательные технологии

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
1	**2**	**3**	**4**
1.	*Введение в защиту информации от несанкционированного доступа*	*Лекция 1.* *Самостоятельная работа*	*Традиционная лекция с использованием презентаций* *Подготовка к занятиям с использованием ЭБС*
2	*Требования к защите информации от несанкционированного доступа*	*Лекция 2.* *Самостоятельная работа*	*Традиционная лекция с использованием презентаций* *Подготовка к занятиям с использованием ЭБС*
3	*Авторизация. Методы идентификации и аутентификации пользователя*	*Лекция 3.* *Самостоятельная работа*	*Традиционная лекция с использованием презентаций* *Подготовка к занятиям с использованием ЭБС*
4	*Управление доступом к ресурсам*	*Лекция 4.* *Самостоятельная работа*	*Традиционная лекция с использованием презентаций* *Подготовка к занятиям с использованием ЭБС*
5	*Разработка политики безопасности информационной системы*	*Лекция 5* *Самостоятельная работа*	*Традиционная лекция с использованием презентаций* *Подготовка к занятиям с использованием ЭБС*
6	*Методика анализа защищённости ИС. Методы и средства*	*Лекция 6*	*Традиционная лекция с использованием презентаций*

	выявления угроз её информационной безопасности	*Самостоятельная работа*	*Подготовка к занятиям с использованием ЭБС*
7	*Применение средств аппаратной защиты*	*Лекция 7* *Самостоятельная работа*	*Традиционная лекция с использованием презентаций* *Подготовка к занятиям с использованием ЭБС*
8	*Анализ источников, каналов распространения и каналов утечки информации*	*Практическое занятие 1*	
9	*Запуск и регистрация в системе защиты*	*Практическое занятие 2*	
10	*Реализация дискреционной модели разграничения доступа*	*Практическое занятие 3*	
11	*Контроль целостности*	*Практическое занятие 4*	
12	*Гарантированное удаление данных*	*Практическое занятие 5*	
13	*Реализация мандатной модели разграничения доступа*	*Практическое занятие 6*	

5. Оценка планируемых результатов обучения

5.1. Система оценивания

Форма контроля	**Макс. количество баллов**	
	За одну работу	**Всего**
Текущий контроль: *– опрос (темы 1-3)* *– опрос (темы 4-7)* *– практическое занятие (темы 2-7)*	 *4 балла* *3 балла* *6 баллов*	 *12 баллов* *12 баллов* *36 баллов*
Промежуточная аттестация *экзамен*		*40 баллов*
Итого за дисциплину *Зачет с оценкой*		*100 баллов*

Перечень компетенций с указанием этапов их формирования в процессе освоения дисциплины представляется в виде таблицы:

№ п/п	***Контролируемые разделы дисциплины***	***Код контролируемой компетенции***	***Наименование оценочного средства***
1.	Темы 1 – 7	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3; ПК-8.1; ПК-8.2; ПК-8.3	Опрос
2.	Практические занятия 1 – 6	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3; ПК-8.1; ПК-8.2; ПК-8.3	План практического занятия

Полученный совокупный результат конвертируется в традиционную шкалу оценок и в шкалу оценок Европейской системы переноса и накопления кредитов (European Credit Transfer System; далее – ECTS) в соответствии с таблицей:

100-балльная шкала	Традиционная шкала		Шкала ECTS
95 – 100	отлично	зачтено	A
83 – 94			B
68 – 82	хорошо		C
56 – 67	удовлетворительно		D
50 – 55			E
20 – 49	неудовлетворительно	не зачтено	FX
0 – 19			F

5.2. Критерии выставления оценки по дисциплине

Баллы/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
100-83/ A,B	«отлично»/ «зачтено (отлично)»/ «зачтено»	Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации. Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения. Свободно ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».
82-68/ C	«хорошо»/ «зачтено (хорошо)»/ «зачтено»	Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей. Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами. Достаточно хорошо ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».
67-50/ D,E	«удовлетворительно»/ «зачтено (удовлетворительно)»/ «зачтено»	Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами. Демонстрирует достаточный уровень знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации.

Баллы/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
		Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».
49-0/ F,FX	«неудовлетворительно»/ не зачтено	Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами. Демонстрирует фрагментарные знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.

5.3. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине

Устный опрос

Устный опрос – это средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объёма знаний, обучающегося по определённому разделу, теме, проблеме и т.п.

Перечень устных вопросов для проверки знаний

№	Вопрос	Реализуемая компетенция
1.	Документы Гостехкомиссии (ФСТЭК) России по защите от НСД. Система государственных нормативных актов по ЗИ от НСД.	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3; ПК-8.1; ПК-8.2; ПК-8.3
2.	Виды угроз современным АС.	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3; ПК-8.1; ПК-8.2; ПК-8.3
3.	Классы защищённости СВТ и АС. Показатели защищённости межсетевых экранов и их увязка с классами защищённости АС.	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3; ПК-8.1; ПК-8.2; ПК-8.3
4.	Подсистемы механизма ЗИ от НСД. Требования к защите информации АС групп 1Г и 1В.	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3; ПК-8.1; ПК-8.2; ПК-8.3
5.	Понятие идентификации и аутентификации. Процедура авторизации.	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3; ПК-8.1;

		ПК-8.2; ПК-8.3
6.	Формализованные и дополнительные требования к идентификации и аутентификации. Авторизация в контексте количества и вида зарегистрированных пользователей. Рекомендации по построению авторизации, исходя из вида и количества зарегистрированных пользователей.	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3; ПК-8.1; ПК-8.2; ПК-8.3
7.	Механизмы парольной защиты. Функциональное назначение и реализация механизмов парольной защиты.	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3; ПК-8.1; ПК-8.2; ПК-8.3
8.	Угрозы преодоления парольной защиты.	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3; ПК-8.1; ПК-8.2; ПК-8.3
9.	Основные механизмы ввода пароля.	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3; ПК-8.1; ПК-8.2; ПК-8.3
10.	Двухуровневая авторизация на уровне ОС и BIOS. Сетевая авторизация.	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3; ПК-8.1; ПК-8.2; ПК-8.3
11.	Протоколы аутентификации.	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3; ПК-8.1; ПК-8.2; ПК-8.3
12.	Абстрактные модели доступа. Понятия «владелец» и «собственник» информации.	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3; ПК-8.1; ПК-8.2; ПК-8.3
13.	Дискреционное разграничение доступа.	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3; ПК-8.1; ПК-8.2; ПК-8.3
14.	Мандатное разграничение доступа.	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3; ПК-8.1; ПК-8.2; ПК-8.3
15.	Ролевая модель разграничения доступа.	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3; ПК-8.1; ПК-8.2; ПК-8.3
16.	Управления доступом на основе атрибутов. Выбор модели разграничения доступа.	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3; ПК-8.1; ПК-8.2; ПК-8.3
17.	Корректность и полнота реализации разграничительной политики доступа. Классификация субъектов и объектов доступа. Требования к механизмам управления доступом.	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3; ПК-8.1; ПК-8.2; ПК-8.3
18.	Централизованное и децентрализованное управление доступом.	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-

		13.2; ПК-13.3; ПК-8.1; ПК-8.2; ПК-8.3
19.	Общие положения разработки политики безопасности. Нормативные документы по разработке политики безопасности.	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3; ПК-8.1; ПК-8.2; ПК-8.3
20.	Процесс разработки политики безопасности. Требования к политикам безопасности.	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3; ПК-8.1; ПК-8.2; ПК-8.3
21.	Реализация политик безопасности. Архитектура корпоративной системы защиты информации. Настройки основных компонент системы защиты компании.	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3; ПК-8.1; ПК-8.2; ПК-8.3
22.	Типовая методика анализа защищённости ИС	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3; ПК-8.1; ПК-8.2; ПК-8.3
23.	Методы количественной оценки систем информационной безопасности.	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3; ПК-8.1; ПК-8.2; ПК-8.3
24.	Анализ защищённости внешнего периметра и внутренней инфраструктуры корпоративной сети.	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3; ПК-8.1; ПК-8.2; ПК-8.3
25.	Инструментальные средства анализа защищённости. Методы предотвращения сетевых атак на периметр сети.	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3; ПК-8.1; ПК-8.2; ПК-8.3
26.	Угрозы перевода системы защиты в пассивное состояние, их реализация. Методы противодействия угрозам перевода системы защиты в пассивное состояние.	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3; ПК-8.1; ПК-8.2; ПК-8.3
27.	Реализация программно-аппаратного контроля (мониторинга) активности системы защиты.	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3; ПК-8.1; ПК-8.2; ПК-8.3
28.	Метод контроля целостности и активности программных компонент системы защиты программно-аппаратными средствами.	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3; ПК-8.1; ПК-8.2; ПК-8.3
29.	Механизм удалённого мониторинга активности системы защиты, как альтернатива применению аппаратной компоненты защиты.	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3; ПК-8.1; ПК-8.2; ПК-8.3
30.	Метод контроля вскрытия аппаратуры, общий подход. Реализация системы контроля вскрытия аппаратуры.	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3; ПК-8.1; ПК-8.2; ПК-8.3
31.	Принципы комплексирования средств защиты информации	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-

		13.2; ПК-13.3; ПК-8.1; ПК-8.2; ПК-8.3
32.	Угрозы перевода системы защиты в пассивное состояние, их реализация.	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3; ПК-8.1; ПК-8.2; ПК-8.3
33.	Метод контроля вскрытия аппаратуры, общий подход.	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3; ПК-8.1; ПК-8.2; ПК-8.3
34.	Принципы комплексирования средств защиты информации	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3; ПК-8.1; ПК-8.2; ПК-8.3

Промежуточная аттестация (примерные вопросы к зачету)

№	Вопрос	Реализуемая компетенция
1.	Документы Гостехкомиссии (ФСТЭК) России по защите от НСД. Система государственных нормативных актов по ЗИ от НСД.	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3; ПК-8.1; ПК-8.2; ПК-8.3
2.	Виды угроз современным АС.	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3; ПК-8.1; ПК-8.2; ПК-8.3
3.	Классы защищённости СВТ и АС. Показатели защищённости межсетевых экранов и их увязка с классами защищённости АС.	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3; ПК-8.1; ПК-8.2; ПК-8.3
4.	Подсистемы механизма ЗИ от НСД. Требования к защите информации АС групп 1Г и 1В.	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3; ПК-8.1; ПК-8.2; ПК-8.3
5.	Понятие идентификации и аутентификации. Процедура авторизации.	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3; ПК-8.1; ПК-8.2; ПК-8.3
6.	Формализованные и дополнительные требования к идентификации и аутентификации. Авторизация в контексте количества и вида зарегистрированных пользователей. Рекомендации по построению авторизации, исходя из вида и количества зарегистрированных пользователей.	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3; ПК-8.1; ПК-8.2; ПК-8.3
7.	Механизмы парольной защиты. Функциональное назначение и реализация механизмов парольной защиты.	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3; ПК-8.1; ПК-8.2; ПК-8.3
8.	Угрозы преодоления парольной защиты.	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3; ПК-8.1; ПК-8.2; ПК-8.3
9.	Основные механизмы ввода пароля.	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3; ПК-8.1; ПК-8.2; ПК-8.3
10.	Двухуровневая авторизация на уровне ОС и BIOS. Сетевая авторизация.	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3; ПК-8.1; ПК-8.2; ПК-8.3
11.	Протоколы аутентификации.	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3;

		ПК-8.1; ПК-8.2; ПК-8.3
12.	Абстрактные модели доступа. Понятия «владелец» и «собственник» информации.	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3; ПК-8.1; ПК-8.2; ПК-8.3
13.	Дискреционное разграничение доступа.	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3; ПК-8.1; ПК-8.2; ПК-8.3
14.	Мандатное разграничение доступа.	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3; ПК-8.1; ПК-8.2; ПК-8.3
15.	Ролевая модель разграничения доступа.	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3; ПК-8.1; ПК-8.2; ПК-8.3
16.	Управления доступом на основе атрибутов. Выбор модели разграничения доступа.	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3; ПК-8.1; ПК-8.2; ПК-8.3
17.	Корректность и полнота реализации разграничительной политики доступа. Классификация субъектов и объектов доступа. Требования к механизмам управления доступом.	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3; ПК-8.1; ПК-8.2; ПК-8.3
18.	Централизованное и децентрализованное управление доступом.	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3; ПК-8.1; ПК-8.2; ПК-8.3
19.	Общие положения разработки политики безопасности. Нормативные документы по разработке политики безопасности.	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3; ПК-8.1; ПК-8.2; ПК-8.3
20.	Процесс разработки политики безопасности. Требования к политикам безопасности.	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3; ПК-8.1; ПК-8.2; ПК-8.3
21.	Реализация политик безопасности. Архитектура корпоративной системы защиты информации. Настройки основных компонент системы защиты компании.	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3; ПК-8.1; ПК-8.2; ПК-8.3
22.	Типовая методика анализа защищённости ИС	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3; ПК-8.1; ПК-8.2; ПК-8.3
23.	Методы количественной оценки систем информационной безопасности.	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3; ПК-8.1; ПК-8.2; ПК-8.3
24.	Анализ защищённости внешнего периметра и внутренней инфраструктуры корпоративной сети.	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3; ПК-8.1; ПК-8.2; ПК-8.3
25.	Инструментальные средства анализа защищённости. Методы предотвращения сетевых атак на периметр сети.	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3; ПК-8.1; ПК-8.2; ПК-8.3
26.	Угрозы перевода системы защиты в пассивное состояние, их реализация. Методы противодействия угрозам перевода системы защиты в пассивное состояние.	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3; ПК-8.1; ПК-8.2; ПК-8.3
27.	Реализация программно-аппаратного контроля (мониторинга) активности системы защиты.	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3; ПК-8.1; ПК-8.2; ПК-8.3
28.	Метод контроля целостности и активности программных компонент системы защиты программно-	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3;

	аппаратными средствами.	ПК-8.1; ПК-8.2; ПК-8.3
29.	Механизм удалённого мониторинга активности системы защиты, как альтернатива применению аппаратной компоненты защиты.	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3; ПК-8.1; ПК-8.2; ПК-8.3
30.	Метод контроля вскрытия аппаратуры, общий подход. Реализация системы контроля вскрытия аппаратуры.	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3; ПК-8.1; ПК-8.2; ПК-8.3
31.	Принципы комплексирования средств защиты информации	ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3; ПК-8.1; ПК-8.2; ПК-8.3

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Список источников и литературы

Литература

Основная

1. *Гаврилов, М. В.* Информатика и информационные технологии : учебник для прикладного бакалавриата / М. В. Гаврилов, В. А. Климов. – 4-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2019. – 383 с. – (Серия : Бакалавр. Прикладной курс). – ISBN 978-5-534-00814-2. – Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://www.biblio-online.ru/bcode/431772

2. Программно-аппаратная защита информации : учеб. пособие / П.Б. Хорев. — 2-е изд., испр. и доп. — Москва : ФОРУМ : ИНФРА-М, 2019. — 352 с. — (Высшее образование). - Текст : электронный. - URL: https://new.znanium.com/catalog/product/1025261 (дата обращения: 11.08.2019)

3. *Руководящий докумен*т. Защита от несанкционированного доступа к информации. Термины и определения. Утверждено решением председателя Гостехкомиссии России от 30 марта 1992 г. [Электронный ресурс] : Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/386-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g3, свободный. – Загл. с экрана.

4. *Руководящий документ*. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. [Электронный ресурс] : Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/384-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g, свободный. – Загл. с экрана.

5. *Руководящий документ*. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. [Электронный ресурс] : Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/385-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g2, свободный. – Загл. с экрана.

6. *Руководящий документ*. Средства вычислительной техники. Межсетевые экраны Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации. Утверждено решением председателя Госу-

дарственной технической комиссии при Президенте Российской Федерации от 25 июля 1997 г. [Электронный ресурс] : Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/383-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-25-iyulya-1997-g, свободный. – Загл. с экрана.
7. *Руководящий документ.* Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 4 июня 1999 г. N 114
8. *Базовая модель угроз* безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). (утв. ФСТЭК РФ 15.02.2008) [Электронный ресурс] : Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/379, свободный. – Загл. с экрана.
9. *Федеральный закон* «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ (ред. от 19.07.2018). [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_61798/, свободный. – Загл. с экрана.
10. Платонов В.В. Программно-аппаратные средства защиты информации (2-е изд., стер.), М. Академия, 2014, https://academia-library.ru/catalogue/4831/105545/
11. Душкин А.В.,Барсуков О.М.,Кравцов Е.В.,Славнов К.В. Программно-аппаратные средства обеспечения информационной безопасности: учеб. Пособие. – М.: Горячая линия – Телеком, 2016.- 248 с. https://znanium.com/bookread2.php?book=973806
12. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 1. Правовое обеспечение информационной безопасности: учеб. Пособие. – М.: МИЭТ, 2016. – 184 с. https://znanium.com/bookread2.php?book=536932
13. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 2. Организационное обеспечение информационной безопасности: учеб. пособие. – М.: МИЭТ, 2016. – 172 с. https://znanium.com/bookread2.php?book=536932

Дополнительная

1. Федеральный закон от 27 июля 2006 г. N 152-ФЗ «О персональных данных».
2. Федеральный закон от 27 декабря 2002 г. No 184-ФЗ «О техническомрегулировании».
3. Федеральный закон от 4 мая 2011 г. N 99-ФЗ «О лицензировании отдельных видов деятельности».
4.Федеральный закон от 30 декабря 2001 г. N 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».
5.Указ Президента Российской Федерации от 16 августа 2004 г. N 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
6. Указ Президента Российской Федерации от 6 марта 1997 г. N 188 «Об утверждении перечня сведений конфиденциального характера».
7. Указ Президента Российской Федерации от 17 марта 2008 г. N 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».
8. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. N 608.
9. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. N 21.
10. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

11. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. No 83.
12. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от12 июля 2012 г. N 84.
13. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. No 282.
14. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. N 17.
15. Требования о защите информации, содержащейся в информационных системахобщего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. No 416/489.
16. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭКРоссии от 6 декабря 2011 г. No 638.
17. Руководящий документ. Геоинформационные системы. Защита информации отнесанкционированного доступа. Требования по защите информации. Утвержден ФСТЭКРоссии, 2008.
18. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 2. Программное обеспечение базовых систем ввода-вывода персональных электронно-вычислительных машин. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.
19. Приказ ФАПСИ при Президенте Российской Федерации от 13 июня 2001 г. No 152 «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».
20. Сети нового поколения – NGN: Учебное пособие для вузов / В.И. Битнер, Ц.Ц. Михайлова. – Москва : Гор. линия-Телеком, 2011. – 226 с.: ил.; 60x88 1/16. – (Специальность). (обложка) ISBN 978-5-9912-0149-0, 500 экз. – Текст : электронный. - URL: https://new.znanium.com/catalog/product/308917 (дата обращения: 29.04.2021)
21. Бирюков, А. А. Информационная безопасность: защита и нападение / А.А. Бирюков. – 2-е изд., перераб. и доп. – Москва : ДМК Пресс, 2017. – 434 с. - ISBN 978-5-97060-435-9. – Текст : электронный. – URL: https://new.znanium.com/catalog/product/1028060 (дата обращения: 29.04.2021)

6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет».

1.Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
2.Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
3.Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/
4.Справочно-правовая система «Консультант Плюс» www.consultant.ru
5.Справочно-правовая система «Гарант» » www.garant.ru
6.Федеральный портал «Российское образование www.edu.ru
7.Федеральный правовой портал «Юридическая Россия» http://www.law.edu.ru/
8.Российский биометрический портал www.biometrics.ru

9.Федеральный портал «Информационно- коммуникационные технологии вобразовании» htpp\\:www.ict.edu.ru
10.Сайт Научной электронной библиотеки www.elibrary.ru

7 Материально-техническое обеспечение дисциплины

Для материально-технического обеспечения дисциплины необходимо:
1) для лекционных занятий – лекционный класс с видеопроектором и компьютером, на котором должно быть установлено следующее ПО:

№п/п	Наименование ПО	Производитель	Способ распространения
1	Microsoft Office 2010	Microsoft	лицензионное
2	Windows 10 Pro	Microsoft	лицензионное
3	Kaspersky Endpoint Security	Kaspersky	лицензионное

2) для практических занятий – компьютерный класс, оборудованный современными персональными компьютерами для каждого студента. На компьютере должны быть установлено следующее ПО:

№п/п	Наименование ПО	Производитель	Способ распространения
1	Microsoft Office 2010	Microsoft	лицензионное
2	Windows 10 Pro	Microsoft	лицензионное
3	Kaspersky Endpoint Security	Kaspersky	лицензионное
4	Cisco Packet Tracer v.7.2	Cisco Systems	свободное
5	Apache 2.0	Apache Software Foundation	свободное
6	Nginx	NGINX, Inc	свободное
7	WireShark	Wireshark Foundation	свободное

Для проведения занятий лекционного типа предлагаются тематические иллюстрации в формате презентаций PowerPoint.

Перечень БД и ИСС

№п/п	Наименование
1	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2020 г. Web of Science Scopus
2	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2020 г. Журналы Cambridge University Press ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis
3	Профессиональные полнотекстовые БД JSTOR Издания по общественным и гуманитарным наукам Электронная библиотека Grebennikon.ru
4	Компьютерные справочные правовые системы Консультант Плюс, Гарант

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов

В ходе реализации дисциплины используются следующие дополнительные

методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- для слепых и слабовидящих:

– лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;

– письменные задания выполняются на компьютере со специализированным программным обеспечением, или могут быть заменены устным ответом;

– обеспечивается индивидуальное равномерное освещение не менее 300 люкс;

– для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;

– письменные задания оформляются увеличенным шрифтом;

– экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

- для глухих и слабослышащих:

– лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования;

– письменные задания выполняются на компьютере в письменной форме;

– экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.

- для лиц с нарушениями опорно-двигательного аппарата:

– лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;

– письменные задания выполняются на компьютере со специализированным программным обеспечением;

– экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- для слепых и слабовидящих:

– в печатной форме увеличенным шрифтом;

– в форме электронного документа;

– в форме аудиофайла.

- для глухих и слабослышащих:

– в печатной форме;

– в форме электронного документа.

- для обучающихся с нарушениями опорно-двигательного аппарата:

– в печатной форме;

– в форме электронного документа;

– в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

- для слепых и слабовидящих:

– устройством для сканирования и чтения с камерой SARA CE;
– дисплеем Брайля PAC Mate 20;
– принтером Брайля EmBraille ViewPlus;

- для глухих и слабослышащих:

– автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих;
– акустический усилитель и колонки;

- для обучающихся с нарушениями опорно-двигательного аппарата:

– передвижными, регулируемыми эргономическими партами СИ-1;
– компьютерной техникой со специальным программным обеспечением.
– акустический усилитель и колонки;

- для обучающихся с нарушениями опорно-двигательного аппарата:

– передвижными, регулируемыми эргономическими партами СИ-1;
– компьютерной техникой со специальным программным обеспечением.

10. Методические материалы

9.1. Планы практических занятий – проверка сформированной компетенций – ОПК-5; ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13; ПК-13.1; ПК-13.2; ПК-13.3; ПК-8; ПК-8.1; ПК-8.2; ПК-8.3

Темы учебной дисциплины предусматривают проведение практических работ, которые служат как целям текущего и промежуточного контроля за подготовкой студентов, так и целям получения практических навыков применения методов выработки решений, закрепления изученного материала, развития умений, приобретения опыта решения конкретных проблем, ведения дискуссий, аргументации и защиты выбранного решения. Помощь в этом оказывают задания для практических работ, выдаваемые преподавателем на каждом занятии.

Целью практических работ является закрепление теоретического материала и приобретение практических навыков работы с соответствующим оборудованием, программным обеспечением и нормативными правовыми документами.

Тематика практических работ соответствует программе дисциплины.

Практическая работа 1 (6 ч.) Анализ источников, каналов распространения и каналов утечки информации – ОПК-5; ПК-13; ПК-8

Задания:

- Исследовать осциллограммы и спектры получаемых сигналов (как пиковый, так и мгновенный)
- Сделать иллюстрации исследованных сигналов и поместить их в отчет с описанием
- Оценить возможность передачи звука через телефонный капсуль прямого ТЛФ к полевому телефону
- Поместить в отчет схемы соединений с описанием сигналов и результатов

Список литературы:

1. Материалы лекций
2. Программно-аппаратная защита информации : учеб. пособие / П.Б. Хорев. — 2-е изд., испр. и доп. — Москва : ФОРУМ : ИНФРА-М, 2019. — 352 с. — (Высшее образование). - Текст: электронный. - URL: https://new.znanium.com/catalog/product/1025261 (дата обращения: 11.05.2021)

Материально-техническое обеспечение занятия:

1. Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows.

Практическая работа 2 (6 ч.) Запуск и регистрация в системе защиты – ОПК-5; ПК-13; ПК-8

Задания:

1. Зарегистрироваться в системе пользователем Администратор, введя пароль «12345».
2. Попытаться загрузить компьютер, затем, три раза подряд неправильно ввести пароль. Какова реакция СЗИ?

Список литературы:

1. Материалы лекций
2. Программно-аппаратная защита информации : учеб. пособие / П.Б. Хорев. — 2-е изд., испр. и доп. — Москва : ФОРУМ : ИНФРА-М, 2019. — 352 с. — (Высшее образование). - Текст : электронный. - URL: https://new.znanium.com/catalog/product/1025261 (дата обращения: 11.05.2021)

Материально-техническое обеспечение занятия:

1. Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, виртуальной машиной.

Практическая работа 3 (6 ч.) Реализация дискреционной модели разграничения доступа – ОПК-5; ПК-13; ПК-8

Задания:

1. С помощью «Администратора ресурсов» в режиме администрирования разграничить права доступа пользователей к созданным каталогам. Зарегистрироваться пользователем Кравченко. Убедиться, что каталог для этого пользователя не отображается.
2. Зарегистрироваться пользователем Котов и просмотреть содержимое каталога. Убедиться, что каталог для него не отображается.
3. Создать в каталоге пользователем Козлов короткий текстовый файл. Зарегистрироваться Администратором и просмотреть разрешения, которые установлены для вновь созданного файла.
4. Убедиться, что Кравченко сможет прочитать информацию, но не сможет изменить ее.

Список литературы:

1. Материалы лекций
2. Программно-аппаратная защита информации : учеб. пособие / П.Б. Хорев. — 2-е изд., испр. и доп. — Москва : ФОРУМ : ИНФРА-М, 2019. — 352 с. — (Высшее образование). - Текст : электронный. - URL: https://new.znanium.com/catalog/product/1025261 (дата обращения: 11.05.2021)

Материально-техническое обеспечение занятия:

1. Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows.

Практическая работа 4 (6 ч.) Контроль целостности – ОПК-5; ПК-13; ПК-8

Задания:

1. Зарегистрироваться в системе пользователем Администратор и настроить контроль целостности всех параметров файла с записью в журнал.
2. Выйти из системы. Зарегистрироваться другим пользователем и внести изменения файлов.
3. Зарегистрироваться Администратором, открыть «Журнал регистрации событий» в программе и найти записи журнала, в которых отражено изменение контрольной суммы файла.

Список литературы:

1. Материалы лекций
2. Программно-аппаратная защита информации : учеб. пособие / П.Б. Хорев. — 2-е изд., испр. и доп. — Москва : ФОРУМ : ИНФРА-М, 2019. — 352 с. — (Высшее образование). -

Текст : электронный. - URL: https://new.znanium.com/catalog/product/1025261 (дата обращения: 11.05.2021)

Материально-техническое обеспечение занятия:

1. Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, виртуальной машиной.

Практическая работа 5 (6 ч.) Гарантированное удаление данных – ОПК-5; ПК-13; ПК-8

Задания:

1. Работая пользователем, создать в каталоге короткий текстовый файл, содержащий произвольную строку символов.
2. Зарегистрироваться другим пользователем. Создать в каталоге текстовый файл, содержащий произвольную строку символов.
3. С использованием редактора WinHEX (или любого другого двоичного редактора), запущенного из основной операционной системы, открыть файл образа диска с установленной СЗИ «Страж NT». Найти и записать смещение, по которому расположены два созданных файла.
4. Удалить файлы, воспользовавшись комбинацией <Shift+Delete> в «Страж NT» (пользователем Администратор).
5. Попытаться найти содержимое удаленных файлов с использованием редактора WinHEX.

Список литературы:

1. Материалы лекций
2. Программно-аппаратная защита информации : учеб. пособие / П.Б. Хорев. — 2-е изд., испр. и доп. — Москва : ФОРУМ : ИНФРА-М, 2019. — 352 с. — (Высшее образование). - Текст : электронный. - URL: https://new.znanium.com/catalog/product/1025261 (дата обращения: 11.05.2021)

Материально-техническое обеспечение занятия:

1. Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows.

Практическая работа 6 (6 ч.) Реализация мандатной модели разграничения доступа – ОПК-5; ПК-13; ПК-8

Задания:

1. Назначить созданным учетным записям пользователей уровни допуска путем включения их в соответствующие группы.
2. Создать иерархическую структуру каталогов. Назначить созданным каталогам грифы ограничения доступа.

Список литературы:

1.Материалы лекций

2.Программно-аппаратная защита информации : учеб. пособие / П.Б. Хорев. — 2-е изд., испр. и доп. — Москва : ФОРУМ : ИНФРА-М, 2019. — 352 с. — (Высшее образование). - Текст : электронный. - URL: https://new.znanium.com/catalog/product/1025261 (дата обращения: 11.05.2021)

Материально-техническое обеспечение занятия:

1.Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, виртуальной машиной.

Результаты практических работ обучающиеся составляют по оговорённой преподавателем форме, в электронной виде с использованием ПКП MS Office 2007 и выше и передаётся преподавателю посредством оговорённого способа связи.

Приложение 1

АННОТАЦИЯ ДИСЦИПЛИНЫ

Дисциплина «Защита информации от несанкционированного доступа в автоматизированных системах» реализуется на факультете Информационных систем и безопасности для студентов 3-го курса, обучающихся по программе бакалавриата по направлению подготовки 10.03.01 Информационная безопасность (профили подготовки –Безопасность автоматизированных систем) кафедрой комплексной защиты информации.

Цель дисциплины: теоретическое изучение и практическое освоение принципов защиты информации от несанкционированного доступа в автоматизированных системах.
Задачи:
- формирование знаний в области выбора, анализа и применения защиты информации от несанкционированного доступа;
- уяснение основных понятий и определений в области защиты информации от несанкционированного доступа в автоматизированных системах;
- рассмотрение современных тенденций развития сетей связи.

Дисциплина направлена на формирование следующих компетенций:
- ОПК-5 – Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности
  - ОПК-5.1 – Знает основы законодательства Российской Федерации, нормативные правовые акты, нормативные и методические документы в области информационной безопасности и защиты информации, правовые основы организации защиты государственной тайны и конфиденциальной информации, правовую характеристику преступлений в сфере компьютерной информации и меры ответственности за утрату, разглашение, модификацию и уничтожение защищаемой информации
  - ОПК-5.2 – Умеет обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей, предпринимать необходимые меры по восстановлению нарушенных прав.
  - ОПК-5.3 – Владеет навыками по контролю над соблюдением установленного порядка выполнения работ, а также действующего законодательства Российской Федерации при решении вопросов, касающихся защиты информации.
- ПК-13 – Способен принимать участие в формировании, организации и поддержания выполнения комплекса мер по обеспечению информационной безопасности, управлении процессом их реализации
  - ПК-13.1 – Знает процедуру организации установки и настройки технических, программных (программно-технических) средств защиты информации, входящих в состав системы защиты информации организации, в соответствии с техническим проектом и инструкциями по эксплуатации.
  - ПК-13.2 – Владеет навыками организации и сопровождения аттестации объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации.
  - ПК-13.3 – Умеет разрабатывать и реализовывать организационные меры, обеспечивающие эффективность системы защиты информации.
- ПК-8 – Способен осуществлять мониторинг и аудит защищенности информации в автоматизированных системах

- ПК-8.1 – Знает основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах, организационные меры по защите информации
- ПК-8.2 – Умеет анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах; вести протоколы и журналы учета при осуществлении аудита систем защиты информации автоматизированных систем.
- ПК-8.3 – Владеет навыками выработки рекомендаций для принятия решения о модернизации системы защиты информации автоматизированной системы

В результате освоения дисциплины обучающийся должен:
Знать: основы законодательства РФ, нормативные правовые акты; нормативные и методические документы в области информационной безопасности и защиты информации; правовые основы организации защиты государственной тайны и конфиденциальной информации; правовую характеристику преступлений в сфере компьютерной информации и меры ответственности за утрату, разглашение, модификацию и уничтожение защищаемой информации; процедуру организации установки и настройки технических, программных (программно-технических) средств защиты информации, входящих в состав системы защиты информации организации, в соответствии с техническим проектом и инструкциями по эксплуатации; основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах; организационные меры по защите информации;
Уметь: обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей; предпринимать необходимые меры по восстановлению нарушенных прав; разрабатывать и реализовывать организационные меры, обеспечивающие эффективность системы защиты информации; анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем; выявлять потенциальные уязвимости безопасности информации в автоматизированных системах; вести протоколы и журналы учета при осуществлении аудита систем защиты информации автоматизированных систем
Владеть: навыками разработки локальных правовых документов, регламентирующих работу по обеспечению информационной безопасности в организации; навыками организации процесса аттестации объектов вычислительной техники и выделенных помещений; навыками сопровождения аттестации объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации; навыками выработки рекомендаций для принятия решения о модернизации системы защиты информации автоматизированной системы.

По дисциплине предусмотрена промежуточная аттестация в форме зачета с оценкой.

Общая трудоёмкость освоения дисциплины составляет 3 зачётные единицы.

Приложение 2

УТВЕРЖДЕНО
Протокол заседания кафедры
№_____ от_____

ЛИСТ ИЗМЕНЕНИЙ

в рабочей программе дисциплины Защита от НСД к информации в автоматизированных системах

по направлению подготовки 10.03.01 Информационная безопасность

на 20__/20__ учебный год

1. В _____ вносятся следующие изменения:
(элемент рабочей программы)
1.1. ……..;
1.2. ……...;
…
1.9. …… .

2. В _____ вносятся следующие изменения:
(элемент рабочей программы)
2.1. ……..;
2.2. ……...;
…
2.9. …… .

3. В _____ вносятся следующие изменения:
(элемент рабочей программы)
3.1. ……..;
3.2. ……...;
…
3.9. …… .

Составитель подпись расшифровка подписи
дата