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

ВНЕДРЕНИЕ И ЭКСПЛУАТАЦИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Направление подготовки 10.03.01 Информационная безопасность
Направленность (профиль) Безопасность автоматизированных систем
(по отрасли или в сфере профессиональной деятельности)

Уровень высшего образования: бакалавриат
Форма обучения: очная

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2022

ВНЕДРЕНИЕ И ЭКСПЛУАТАЦИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ
Рабочая программа дисциплины

Составитель(и):
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
№ 8 от 31.03.2022

ОГЛАВЛЕНИЕ

1. Пояснительная записка

1.1. Цель и задачи дисциплины

Цель дисциплины – приобретение студентами знаний, навыков и умений, связанных с правовыми и программно-техническими внедрения и эксплуатации средств защиты информации организаций и учреждений.
Задачи дисциплины:
– формирование знаний в области программно-аппаратных средств защиты информации;
– уяснение основных понятий и определений, а также осветить круг вопросов касающихся персональной ответственности должностных лиц при внедрении и эксплуатации средств защиты информации;
– осветить круг вопросов, способствующих самостоятельному использованию полученных знаний для решения типовых задач.

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

Компетенция (код и наименование)	**Индикаторы компетенций** (код и наименование)	**Результаты обучения**
ПК-10 Способен проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	ПК-10.1 Знает нормативные правовые акты в области защиты информации, национальные, межгосударственные и международные стандарты в области защиты информации, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации	Знать: • нормативные правовые акты в области защиты информации; • межгосударственные и международные стандарты в области защиты информации; • руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации;
	ПК-10.2 Умеет анализировать данные о назначении, функциях, условиях функционирования объектов и систем обработки информации ограниченного доступа, установленных на объектах информатизации, и характере обрабатываемой на них информации	Уметь: • анализировать данные о назначении, функциях, условиях функционирования объектов и систем обработки информации ограниченного доступа; • анализировать данные о характере обрабатываемой на них информации
	ПК-10.3 Владеет навыком разработки аналитического обоснования необходимости создания системы защиты информации в организации	Владеть: • навыком разработки аналитического обоснования необходимости создания системы защиты информации
ПК-13 Способен принимать участие в формировании, организации и	ПК-13.1 Знает процедуру организации установки и настройки технических, программных (про-	Знать: • процедуру организации установки и настройки технических, программных

поддержания выполнения комплекса мер по обеспечению информационной безопасности, управлении процессом их реализации	граммно-технических) средств защиты информации, входящих в состав системы защиты информации организации, в соответствии с техническим проектом и инструкциями по эксплуатации	(программ-но-технических) средств защиты информации, входящих в состав системы защиты информации;
	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 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	Уметь: • разрабатывать и реализовывать организационные меры, обеспечивающие эффективность системы защиты информации
ПК-4 Способен обеспечивать работоспособность систем защиты информации при возникновении нештатных ситуаций	ПК-4.1 Знает методы и способы обеспечения отказоустойчивости автоматизированных систем, содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем	Знать: • методы и способы обеспечения отказоустойчивости автоматизированных систем; • методы и способы содержания и порядка деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем;
	ПК-4.2 Умеет применять типовые программные средства резервирования и восстановления информации, средства обеспечения отказоустойчивости в автоматизированных системах	Уметь: • применять типовые программные средства резервирования и восстановления информации, средства обеспечения отказоустойчивости в автоматизированных системах сетей
	ПК-4.3 Владеет навыками обнаружения, устранения неисправностей в работе системы защиты информации автоматизированной системы, резервирования программного обеспечения, технических средств, каналов передачи данных автоматизированной системы управления на случай возникновения нештатных ситуаций	Владеть: • навыками обнаружения, устранения неисправностей в работе системы защиты информации автоматизированной системы на случай возникновения нештатных ситуаций; • навыками резервирования программного обеспечения, технических средств, каналов передачи данных авто-

		матизированной системы управления на случай возникновения нештатных ситуаций

1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Внедрение и эксплуатация средств защиты информации» 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: «Методы и средства защиты информации от утечки по техническим каналам», «Аппаратные средства вычислительной техники», «Безопасность операционных систем».
В результате освоения дисциплины формируются знания, умения и владения, необходимые для изучения следующих дисциплин и прохождения практик: «Аудит информационной безопасности», «Информационная безопасность телекоммуникационных систем», «Преддипломная практика».

2. Структура дисциплины

Общая трудоёмкость дисциплины составляет _2_ з.е., 72 академических часа.

Структура дисциплины для очной формы обучения

Объем дисциплины в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Семестр	Тип учебных занятий	Количество часов
7	Лекции	**16**
7	Практические работы	**24**
	Всего:	**40**

Объем дисциплины в форме самостоятельной работы обучающихся составляет _32_ академических часа.

3. Содержание дисциплины

Тема 1. Основные этапы построения внедрения и эксплуатации средств защиты информации

Анализ. Разработка средств защиты информации. Внедрение и эксплуатация средств защиты информации. Способы реализации средств защиты информации. Совместимость средств защиты информации. Сопровождение этапов.

Тема 2. Оценка эффективности от внедрения и эксплуатации средств защиты информации.

Оценка реальных затрат и выигрыша от применения предполагаемых мер защиты. Величина ущерба от реализации угроз. Порядок ввода в действие средств защиты. Порядок пересмотра плана и состава средств защиты. Порядок модернизации средств защиты. Экономический эффект от внедрения и эксплуатации средств защиты информации.

Тема 3. Сертификация средств защиты информации.

Порядок сертификации. Порядок лицензирования. Перечень работ. Контроль за соблюдением требований. Участники сертификации средств защиты информации. Основными схемами проведения сертификации средств защиты информации. Подача заявки на сертификацию. Заклю-

чение договора с испытательной лабораторией. Подготовка исходных данных. Сертификационные испытания. Оформление результатов испытаний. Экспертиза результатов сертификационных испытаний.

Тема 4. Эксплуатация технических средств защиты информации

Этапы эксплуатации технических средств защиты информации. Виды, содержание и порядок проведения технического обслуживания средств защиты информации. Установка и настройка технических средств защиты информации. Диагностика, устранение отказов и восстановление работоспособности технических средств защиты информации. Организация ремонта технических средств защиты информации. Проведение аттестации объектов информатизации.

4. Образовательные технологии

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
1	**2**	**3**	**4**
1.	Основные этапы построения внедрения и эксплуатации средств защиты информации	Лекция 1. Практическое занятие 1. Самостоятельная работа	Традиционная лекция с использованием презентаций Опрос, тест Занятия с использованием специализированного ПО Подготовка к занятиям с использованием ЭБС
2	Оценка эффективности от внедрения и эксплуатации средств защиты информации.	Лекция 2. Практическое занятие 2. Самостоятельная работа	Традиционная лекция с использованием презентаций Опрос, тест Занятия с использованием специализированного ПО Подготовка к занятиям с использованием ЭБС
3	Сертификация средств защиты информации	Лекция 3. Практическое занятие 3. Самостоятельная работа	Традиционная лекция с использованием презентаций Опрос, тест Занятия с использованием специализированного ПО Подготовка к занятиям с использованием ЭБС
4	Эксплуатация технических средств защиты информации	Лекция 4. Практическое занятие 4. Самостоятельная работа	Традиционная лекция с использованием презентаций Опрос, тест Занятия с использованием специализированного ПО Подготовка к занятиям с использованием ЭБС

В период временного приостановления посещения обучающимися помещений и территории РГГУ для организации учебного процесса с применением электронного обучения и дистанционных образовательных технологий могут быть использованы следующие образовательные технологии:

– видео-лекции**;**

– онлайн-лекции в режиме реального времени;

– электронные учебники, учебные пособия, научные издания в электронном виде и доступ к иным электронным образовательным ресурсам;

– системы для электронного тестирования;

– консультации с использованием телекоммуникационных средств.

5. Оценка планируемых результатов обучения

5.1 Система оценивания

Форма контроля	**Макс. количество баллов**	
	За одну работу	**Всего**
Текущий контроль:		
– опрос, тестирование (темы 1-4)	*7 балла*	*28 баллов*
– практическое занятие (темы 1-4)	*9 баллов*	*32 баллов*
Промежуточная аттестация – зачёт (зачет по билетам)		*40 баллов*
Итого за семестр		100 баллов

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	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.

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
		Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».
82-68/ C	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	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. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».
49-0/ F,FX	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.	В чем заключаются национальные интересы РФ в информационной сфере?	ПК-10; ПК-13; ПК-4

2.	Система защиты информации	ПК-10; ПК-13; ПК-4
3.	Обеспечение защиты информации с точки зрения риска.	ПК-10; ПК-13; ПК-4
4.	Критерии оценки защищенной системы. Общее решение задачи проектирования оптимальной системы защиты	ПК-10; ПК-13; ПК-4
5.	Нормативно-правовая база функционирования систем защиты информации.	ПК-10; ПК-13; ПК-4
6.	Угрозы безопасности информации	ПК-10; ПК-13; ПК-4
7.	Классификация методов и средств защиты информации	ПК-10; ПК-13; ПК-4
8.	Технические методы защиты	ПК-10; ПК-13; ПК-4
9.	Проектирование системы защиты информации	ПК-10; ПК-13; ПК-4
10.	Задачи, решаемые техническими методами защиты. Методы решения данных задач	ПК-10; ПК-13; ПК-4
11.	Комплексный подход к построению систем безопасности	ПК-10; ПК-13; ПК-4
12.	Предварительные испытания и опытная эксплуатация	ПК-10; ПК-13; ПК-4
13.	Описание технического решения	ПК-10; ПК-13; ПК-4
14.	Подсистема управления доступом	ПК-10; ПК-13; ПК-4
15.	Внедрение системы защиты информации.	ПК-10; ПК-13; ПК-4
16.	Классификация мер обеспечения безопасности	ПК-10; ПК-13; ПК-4
17.	Основные методы и средства защиты информации	ПК-10; ПК-13; ПК-4
18.	Аппаратные средства защиты информации	ПК-10; ПК-13; ПК-4
19.	Программные средства защиты информации	ПК-10; ПК-13; ПК-4
20.	Способы идентификации пользователя	ПК-10; ПК-13; ПК-4
21.	Специализированные программные средства защиты информации	ПК-10; ПК-13; ПК-4
22.	Архитектурные аспекты безопасности	ПК-10; ПК-13; ПК-4
23.	Анализ защищенности	ПК-10; ПК-13; ПК-4
24.	Организационно-правовое обеспечение защиты информации	ПК-10; ПК-13; ПК-4
25.	Защита информации от несанкционированного доступа	ПК-10; ПК-13; ПК-4

Промежуточная аттестация (примерные вопросы к экзамену) – проверка сформированности компетенций – ПК-10; ПК-13; ПК-4

№	Вопрос	Реализуемая компетенция
1.	Связь между уровнем развития общества и технологиями защиты информации	ПК-10; ПК-13; ПК-4
2.	Правовые основы в области защиты информации	ПК-10; ПК-13; ПК-4
3.	Основные задачи защиты информации	ПК-10; ПК-13; ПК-4
4.	Организационно-распорядительные документы по защите информации	ПК-10; ПК-13; ПК-4
5.	Обязанности должностных лиц, решающих задачи внедрения и эксплуатации средств защиты информации	ПК-10; ПК-13; ПК-4
6.	Проведение регламентных работ по эксплуатации средств	ПК-10; ПК-13; ПК-4

	защиты информации	
7.	Обеспечение защиты информации при внедрении и эксплуатации средств защиты информации	ПК-10; ПК-13; ПК-4
8.	Диагностика работоспособности систем и средств защиты информации	ПК-10; ПК-13; ПК-4
9.	Восстановление работоспособности средств защиты информации	ПК-10; ПК-13; ПК-4
10.	Мониторинг защищенности информации при внедрении и эксплуатации средств защиты информации	ПК-10; ПК-13; ПК-4
11.	Внедрение средств защиты информации	ПК-10; ПК-13; ПК-4
12.	Эксплуатация средств защиты информации	ПК-10; ПК-13; ПК-4
13.	Разработка организационно-распорядительных документов при внедрении и эксплуатации средств защиты информации	ПК-10; ПК-13; ПК-4
14.	Анализ уязвимостей внедряемых средств защиты информации	ПК-10; ПК-13; ПК-4
15.	Тестирование средств защиты информации после внедрения	ПК-10; ПК-13; ПК-4
16.	Обоснование необходимости защиты информации и внедрения средств защиты информации	ПК-10; ПК-13; ПК-4
17.	Проведение оценки показателей качества и эффективности после внедрения средств защиты информации	ПК-10; ПК-13; ПК-4
18.	Опытная эксплуатация и эксплуатация средств защиты информации	ПК-10; ПК-13; ПК-4
19.	Обеспечение защиты информации при внедрении и эксплуатации средств защиты информации	ПК-10; ПК-13; ПК-4
20.	Порядок выполнения работ при внедрении средств защиты информации	ПК-10; ПК-13; ПК-4
21.	Основные проблемы, присутствующие при внедрении и эксплуатации средств защиты информации	ПК-10; ПК-13; ПК-4
22.	Аппаратные и программные средства обеспечения защиты информации	ПК-10; ПК-13; ПК-4
23.	Меры безопасности, используемые при эксплуатации средств защиты информации	ПК-10; ПК-13; ПК-4
24.	Меры противодействия иностранным техническим разведкам при внедрении и эксплуатации средств защиты информации	ПК-10; ПК-13; ПК-4

25.	Анализ изменения контролируемой зоны при внедрении и эксплуатации средств защиты информации	ПК-10; ПК-13; ПК-4
26.	Реализация инженерно-технической защиты информации при внедрении и эксплуатации средств защиты информации	ПК-10; ПК-13; ПК-4

Примерные тестовые задания проверка сформированности компетенций – ПК-10; ПК-13; ПК-4

1. Проектирование технологии представляет собой ...

a. информационный процесс, связанный с практической деятельностью менеджера по закупке сырья.

b. информационный процесс, связанный с интеллектуальной деятельностью менеджеров по продаже и характеризующейся различными видами связей: аналитическими выражениями, логическими и иерархическими связями.

c. информационный процесс, связанный с интеллектуальной деятельностью технолога и характеризующейся различными видами связей: аналитическими выражениями, логическими и иерархическими связями.

d. информационный процесс, связанный с интеллектуальной деятельностью маркетолога и характеризующейся различными видами связей: аналитическими выражениями, логическими и иерархическими связями.

2. Оптимальное проектирование нацелено на ...

a. удовлетворение разных, порой противоречивых потребностей людей.

b. создание эффективно работающего объекта.

c. базируется на системном подходе.

d. разработку функциональных показателей качества и показателей надёжности.

3. В российской практике проектирование ведётся ...

a. Поэтапно в соответствии со стадиями, регламентированными ГОСТ 2.103-68.

b. в соответствии со стадиями, регламентированными ГОСТ 2.103-98.

c. поэтапно в соответствии со стадиями, регламентированными ГОСТ 2.103-78.

d. поэтапно в соответствии со стадиями, регламентированными ГОСТ 2.103-98.

4. Техническое задание ...

a. исходный документ для разработки изделия.

b. исходный документ для испытания изделия.

c. ничего из перечисленного.

d. исходный документ для разработки и испытания изделия.

9. Системное проектирование ...

a. Обоснованный выбор окончательного варианта.

b. Удовлетворение разных, порой противоречивых потребностей людей.

c. Базируется на системном подходе.

d. Создание эффективно работающего объекта.

5. По подходу к проектированию различают ...

a. Оптимальное проектирование.

b. Все перечисленное.

c. Функциональное проектирование.

d. Системное проектирование.

6. Эскизный проект -это ...

a. совокупность конструкторских документов, содержащих технические и технико-экономические обоснования целесообразности дальнейшей разработки проекта.

b. совокупность конструкторских документов, которые должны содержать принципиальные конструктивные решения, дающие общее представление об устройстве и принципе работы изделия, данные, определяющие назначение, основные параметры и габаритные размеры проектируемого изделия.

c. программный продукт, вырабатываемый в ходе бизнес-планирования.

d. нормативно-техническая информация (справочники, каталоги и т.п.).

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Список источников и литературы

Литература

Основная

1. *Тумбинская М.В.* Защита информации на предприятии: учебное пособие/М.В.Тумбинская, М.В.Петровский.- С-Петербург: Лань, 2020.-184с.: ил. – учебники для вузов. Специальная литература.
2. Нестеров, С. А. Основы информационной безопасности: учебник для вузов / С. А. Нестеров. — Санкт-Петербург: Лань, 2021. — 324 с.
3. Голиков А. М. Основы проектирования защищенных телекоммуникационных систем: учебное пособие, Томск: ТУСУР, 2016. –396 с., http://biblioclub.ru

Дополнительная

1. Вопросы кибербезопасности. Научный, периодический, информационно-методический журнал с базовой специализацией в области информационной безопасности. URL: http://cyberrus.com/
2. Безопасность информационных технологий. Периодический рецензируемый научный журнал НИЯУ МИФИ. URL: http://bit.mephi.ru/

6.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет».

1. *http://rkn.gov.ru/*Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций.
2. *Nginx.org* – [Электронный ресурс]: Режим доступа: https://nginx.org/ru, свободный. – Загл. с экрана
3. *Wireshark Developer's* Guide [Электронный ресурс]: Режим доступа: https://www.wireshark.org/docs/wsdg_html_chunked/, свободный. – Загл. с экрана
4.

Национальная электронная библиотека (НЭБ) www.rusneb.ru
ELibrary.ru Научная электронная библиотека www.elibrary.ru
Электронная библиотека Grebennikon.ru www.grebennikon.ru
Cambridge University Press
ProQuest Dissertation & Theses Global
SAGE Journals
Taylor and Francis
JSTOR

6.3 Профессиональные базы данных и информационно-справочные системы

Доступ к профессиональным базам данных: https://liber.rsuh.ru/ru/bases

Информационные справочные системы:

1. Консультант Плюс

2. Гарант

7. Материально-техническое обеспечение дисциплины

Для обеспечения дисциплины используется материально-техническая база образовательного учреждения:

1) для лекционных занятий - учебная аудитория, доска, компьютер или ноутбук, проектор (стационарный или переносной) для демонстрации учебных материалов.

Состав программного обеспечения:
1. Windows
2. Microsoft Office
3. Kaspersky Endpoint Security

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

2) для практических занятий – компьютерный класс или лаборатория, доска, проектор (стационарный или переносной), компьютер или ноутбук для преподавателя, компьютеры для обучающихся.

Состав программного обеспечения:
1. Windows
2. Microsoft Office
3. Kaspersky Endpoint Security
4. Mozilla Firefox
5. Cisco Packet Tracer v.7.2

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 специализиро-

ванным 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.

9. Методические материалы

9.1 Планы практических занятий

Темы учебной дисциплины предусматривают проведение практических занятий, которые служат как целям текущего и промежуточного контроля подготовки 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 занятий, выдаваемые преподавателем на каждом занятии.

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

Тематика практических занятий соответствует программе дисциплины.

Практическая работа № 1. (6 ч) ***Система управления процессами внедрения и эксплуатацией средств защиты информации – ПК-10; ПК-13; ПК-4***

Задания:

1. Изучить материал по теме занятия: подходы к защите информации в организации, определение информации, подлежащей защите и состав защищаемой информации.

2. Определить систему управления, внедрения и эксплуатации средств защиты информации

Практическая работа № 2 (6 ч) ***Планирование затрат на внедрение и эксплуатацию средств защиты информации – ПК-10; ПК-13; ПК-4***

Задания:

1. Оцените величину нанесенного фирме ущерба и уровень защиты предприятия по частному функциональному критерию эффективности принимаемых мер.
2. Укажите перечень и последовательность действий персонала в данных ситуациях.

Практические работы № 3 (6 ч) ***Анализ рисков информационной безопасности – ПК-10; ПК-13; ПК-4***

Задания:

1. Составить перечень наиболее распространенных угроз информационной безопасности для данной организации.
2. Выполнить анализ угроз и их последствий, определение слабостей в защите.
3. Провести оценку рисков, заполнив типичную форму для анализа рисков.

Практическая работа № 4 (6 ч) ***Планирование затрат на информационную безопасность – ПК-10; ПК-13; ПК-4***

Задания:

1. Выполнить расчет показателей эффективности внедряемого решения.
2. Анализ затрат внедряемых решений и пересмотр политики информационной безопасности

Приложение 1. Аннотация
рабочей программы дисциплины

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Дисциплина «Внедрение и эксплуатация средств защиты информации» реализуется на факультете Информационных систем и безопасности кафедрой комплексной защиты информации.

Цель дисциплины – приобретение студентами знаний, навыков и умений, связанных с правовыми и программно-техническими внедрения и эксплуатации средств защиты ин-формации организаций и учреждений.
Задачи дисциплины:
– формирование знаний в области программно-аппаратных средств защиты информации;
– уяснение основных понятий и определений, а также осветить круг вопросов касающихся персональной ответственности должностных лиц при внедрении и эксплуатации средств защиты информации;
– осветить круг вопросов, способствующих самостоятельному использованию полученных знаний для решения типовых задач.
Дисциплина направлена на формирование следующих компетенций:

- ПК-10 Способен проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности
- ПК-13 Способен принимать участие в формировании, организации и поддержания выполнения комплекса мер по обеспечению информационной безопасности, управлении процессом их реализации
- ПК-4 Способен обеспечивать работоспособность систем защиты информации при возникновении нештатных ситуаций

В результате освоения дисциплины обучающийся должен:
Знать: нормативные правовые акты в области защиты информации; межгосударственные и международные стандарты в области защиты информации; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; процедуру организации установки и настройки технических, программных (программно-технических) средств защиты информации, входящих в состав системы защиты информации; методы и способы обеспечения отказоустойчивости автоматизированных систем; методы и способы содержания и порядка деятельности персонала по эксплуатации защищённых автоматизированных систем и подсистем безопасности автоматизированных систем;
Уметь: анализировать данные о назначении, функциях, условиях функционирования объектов и систем обработки информации ограниченного доступа; анализировать данные о характере обрабатываемой на них информации; разрабатывать и реализовывать организационные меры, обеспечивающие эффективность системы защиты информации; применять типовые программные средства резервирования и восстановления информации, средства обеспечения отказоустойчивости в автоматизированных системах сетей
Владеть: навыком разработки аналитического обоснования необходимости создания системы защиты информации; навыками организации и сопровождения аттестации объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации; навыками обнаружения, устранения неисправностей в работе системы защиты информации автоматизированной системы на случай возникновения нештатных ситуаций; навыками резервирования программного обеспечения, технических средств, каналов передачи данных автоматизированной системы управления на случай возникновения нештатных ситуаций

По дисциплине предусмотрена промежуточная аттестация в форме зачёта.
Общая трудоёмкость освоения дисциплины составляет 2 зачётные единицы.