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 (профили) подготовки:
Организация и технология защиты информации
Уровень квалификации выпускника – бакалавр

Форма обучения – очная

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2021

Внедрение и эксплуатация средств защиты информации
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 – 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 (модулю), соотнесенных с индикаторами достижения компетенций

Компетенция (код и наименование)	**Индикаторы компетенций** (код и наименование)	**Результаты обучения**
ОПК-2.1 Способен проводить анализ функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба	*ОПК-2.1.1 Знает принципы построения систем защиты информации; критерии оценки эффективности и надежности средств защиты программного обеспечения автоматизированных систем; основные угрозы безопасности информации и модели нарушителя*	*Знать:* • *принципы построения систем защиты информации;* • *критерии оценки эффективности и надежности средств защиты программного обеспечения автоматизированных систем;* • *основные угрозы безопасности информации и модели нарушителя.*
	ОПК-2.1.2 Умеет анализировать угрозы безопасности информации, оценивать информационные риски; применять аналитические и компьютерные модели автоматизированных систем и систем защиты информации; анализировать программные и программно-аппаратные решения при проектировании системы защиты информации с целью выявления уязвимостей	*Уметь:* • *анализировать угрозы безопасности информации, оценивать информационные риски;* • *применять аналитические и компьютерные модели автоматизированных систем и систем защиты информации; анализировать программные и программно-аппаратные решения при проектировании системы защиты информации с целью выявления уязвимостей*
	ОПК-2.1.3 Владеет навыками расчета показателей эффективности защиты информации,	*Владеть:* • *навыками расчета показателей эффективности защиты информации, об-*

	обрабатываемой в автоматизированных системах; проведения анализа уязвимости программного и программно-аппаратных средств защиты информации	*рабатываемой в автоматизированных системах* • *проведения анализа уязвимости программного и программно-аппаратных средств защиты информации*
ОПК-2.3 *Способен разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности*	*ОПК-2.3.1* *Знает национальные, межгосударственные и международные стандарты в области защиты информации, нормативные правовые акты в области защиты информации, руководящие и методические документы уполномоченных федеральных органов исполнительной власти в области внедрения и эксплуатации средств защиты информации*	*Знать:* • *процедуру организации установки и настройки технических, программных (программно-технических) средств защиты информации, входящих в состав системы защиты информации;*
	ОПК-2.3.2 *Умеет документировать процедуры и результаты контроля функционирования системы защиты информации; проводить испытания программно-технических средств защиты информации от НСД и специальных воздействий на соответствие требованиям по безопасности информации и техническим условиям*	*Уметь:* • *документировать процедуры и результаты контроля функционирования системы защиты информации;* • *проводить испытания программно-технических средств защиты информации от НСД и специальных воздействий на соответствие требованиям по безопасности информации и техническим условиям*
	ОПК-2.3.3 *Владеет навыками внесения изменений в эксплуатационную документацию и организационно-распорядительные документы по системе защиты информации; навыками разработки программ и методик испытаний опытного образца программно-технического средства защиты информации от НСД и специальных воздействий на соответствие техническим условиям*	*Владеть:* • *навыками внесения изменений в эксплуатационную документацию и организационно-распорядительные документы по системе защиты информации;* • *навыками разработки программ и методик испытаний опытного образца программно-технического средства защиты информации от НСД и специальных воздействий на соответ-*

		ствие техническим условиям
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 (программ-нотехнических) 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 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*

1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Внедрение и эксплуатация средств защиты информации» относится к дисциплинам по выбору 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 и программного обеспечения».

В результате освоения дисциплины формируются знания, умения и владения, необходимые для изучения следующих дисциплин и прохождения практик: «Аудит информационной безопасности», «Системы управления информационной безопасностью», «Преддипломная практика».

2. Структура дисциплины

Структура дисциплины для очной формы обучения

Общая трудоёмкость дисциплины составляет _2_ з.е., _76__ ч., в том числе контактная работа обучающихся с преподавателем _40_ ч., промежуточная аттестация __ ч., самостоятельная работа обучающихся _36_ 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	*Основные этапы построения внедрения и эксплуатации средств защиты информации*	**7**	**4**		**6**			**9**	Опрос
2	*Оценка эффективности от внедрения и эксплуатации средств защиты информации.*	**7**	**4**		**6**			**9**	Опрос, выполнение практического задания
3	*Сертификация средств защиты информации.*	**7**	**4**		**6**			**9**	Опрос, выполнение практического задания
4	*Эксплуатация технических средств защиты информации*	**7**	**4**		**6**			**9**	Опрос, выполнение практического задания
	зачет								Зачет по билетам
	итого:		**16**		**24**			**36**	

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. Заключение 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* *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* *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* *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* *Занятия с использованием специализированного ПО* *Подготовка к занятиям с использованием ЭБС*

5. Оценка планируемых результатов обучения

5.1. Система оценивания

Форма контроля	**Макс. количество баллов**	
	За одну работу	**Всего**
Текущий контроль: *– опрос (темы 1-4)* *– практическое занятие (темы 1-4)*	*7 балла* *9 баллов*	*28 балла* *32 баллов*
Промежуточная аттестация *зачет*		*40 баллов*
Итого за дисциплину *зачет*		*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 – 4	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ОПК-2.3; ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ПК-13.1; ПК-13.2; ПК-13.3	Опрос
2.	Практические занятия 1 – 4	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ОПК-2.3; ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ПК-13.1; ПК-13.2; ПК-13.3	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.	В чем заключаются национальные интересы РФ в информационной сфере?	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ОПК-2.3; ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ПК-13.1; ПК-13.2; ПК-13.3
2.	Система защиты информации	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ОПК-2.3; ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ПК-13.1; ПК-13.2; ПК-13.3
3.	Обеспечение защиты информации с точки зрения риска.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ОПК-2.3; ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ПК-13.1; ПК-13.2; ПК-13.3
4.	Критерии оценки защищенной системы. Общее решение задачи проектирования оптимальной системы защиты	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ОПК-2.3; ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ПК-13.1; ПК-13.2; ПК-13.3
5.	Нормативно-правовая база функционирования систем защиты информации.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ОПК-2.3; ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ПК-13.1; ПК-13.2; ПК-13.3
6.	Угрозы безопасности информации	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ОПК-2.3; ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ПК-13.1; ПК-13.2; ПК-13.3
7.	Классификация методов и средств защиты информации	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ОПК-2.3; ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3;

		ПК-13.1; ПК-13.2; ПК-13.3
8.	Технические методы защиты	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ОПК-2.3; ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ПК-13.1; ПК-13.2; ПК-13.3
9.	Проектирование системы защиты информации	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ОПК-2.3; ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ПК-13.1; ПК-13.2; ПК-13.3
10.	Задачи, решаемые техническими методами защиты. Методы решения данных задач	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ОПК-2.3; ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ПК-13.1; ПК-13.2; ПК-13.3
11.	Комплексный подход к построению систем безопасности	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ОПК-2.3; ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ПК-13.1; ПК-13.2; ПК-13.3
12.	Предварительные испытания и опытная эксплуатация	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ОПК-2.3; ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ПК-13.1; ПК-13.2; ПК-13.3
13.	Описание технического решения	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ОПК-2.3; ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ПК-13.1; ПК-13.2; ПК-13.3
14.	Подсистема управления доступом	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ОПК-2.3; ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ПК-13.1; ПК-13.2; ПК-13.3
15.	Внедрение системы защиты информации.	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ОПК-2.3; ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ПК-13.1; ПК-13.2; ПК-13.3
16.	Классификация мер обеспечения безопасности	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ОПК-2.3; ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ПК-13.1; ПК-13.2; ПК-13.3
17.	Основные методы и средства защиты информации	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ОПК-2.3; ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ПК-13.1; ПК-13.2; ПК-13.3
18.	Аппаратные средства защиты информации	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ОПК-2.3; ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ПК-13.1; ПК-13.2; ПК-13.3
19.	Программные средства защиты информации	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ОПК-2.3; ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ПК-13.1; ПК-13.2; ПК-13.3
20.	Способы идентификации пользователя	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ОПК-2.3; ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ПК-13.1; ПК-13.2; ПК-13.3
21.	Специализированные программные средства защиты информации	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ОПК-2.3; ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ПК-13.1; ПК-13.2; ПК-13.3
22.	Архитектурные аспекты безопасности	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ОПК-2.3; ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ПК-13.1; ПК-13.2; ПК-13.3
23.	Анализ защищенности	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ОПК-2.3; ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ПК-13.1; ПК-13.2; ПК-13.3
24.	Организационно-правовое обеспечение защиты информации	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ОПК-2.3; ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ПК-13.1; ПК-13.2; ПК-13.3

25.	Защита информации от несанкционированного доступа	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ОПК-2.3; ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ПК-13.1; ПК-13.2; ПК-13.3

Промежуточная аттестация (примерные вопросы к экзамену) – проверка сформированности компетенций – ОПК-2.1; ОПК-2.3; ПК-13

№	Вопрос	Реализуемая компетенция
1.	Связь между уровнем развития общества и технологиями защиты информации	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ОПК-2.3; ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ПК-13.1; ПК-13.2; ПК-13.3
2.	Правовые основы в области защиты информации	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ОПК-2.3; ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ПК-13.1; ПК-13.2; ПК-13.3
3.	Основные задачи защиты информации	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ОПК-2.3; ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ПК-13.1; ПК-13.2; ПК-13.3
4.	Организационно-распорядительные документы по защите информации	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ОПК-2.3; ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ПК-13.1; ПК-13.2; ПК-13.3
5.	Обязанности должностных лиц, решающих задачи внедрения и эксплуатации средств защиты информации	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ОПК-2.3; ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ПК-13.1; ПК-13.2; ПК-13.3
6.	Проведение регламентных работ по эксплуатации средств защиты информации	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ОПК-2.3; ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ПК-13.1; ПК-13.2; ПК-13.3
7.	Обеспечение защиты информации при внедрении и эксплуатации средств защиты информации	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ОПК-2.3; ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ПК-13.1; ПК-13.2; ПК-13.3
8.	Диагностика работоспособности систем и средств защиты информации	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ОПК-2.3; ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ПК-13.1; ПК-13.2; ПК-13.3
9.	Восстановление работоспособности средств защиты информации	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ОПК-2.3; ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ПК-13.1; ПК-13.2; ПК-13.3
10.	Мониторинг защищенности информации при внедрении и эксплуатации средств защиты информации	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ОПК-2.3; ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ПК-13.1; ПК-13.2; ПК-13.3
11.	Внедрение средств защиты информации	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ОПК-2.3; ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ПК-13.1; ПК-13.2; ПК-13.3
12.	Эксплуатация средств защиты информации	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ОПК-2.3; ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ПК-13.1; ПК-13.2; ПК-13.3
13.	Разработка организационно-распорядительных документов при внедрении и эксплуатации средств защиты информации	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ОПК-2.3; ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ПК-13.1; ПК-13.2; ПК-13.3
14.	Анализ уязвимостей внедряемых средств защиты информации	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ОПК-2.3; ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ПК-13.1; ПК-13.2; ПК-13.3
15.	Тестирование средств защиты	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ОПК-

	информации после внедрения	2.3; ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ПК-13.1; ПК-13.2; ПК-13.3
16.	Обоснование необходимости защиты информации и внедрения средств защиты информации	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ОПК-2.3; ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ПК-13.1; ПК-13.2; ПК-13.3
17.	Проведение оценки показателей качества и эффективности после внедрения средств защиты информации	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ОПК-2.3; ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ПК-13.1; ПК-13.2; ПК-13.3
18.	Опытная эксплуатация и эксплуатация средств защиты информации	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ОПК-2.3; ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ПК-13.1; ПК-13.2; ПК-13.3
19.	Обеспечение защиты информации при внедрении и эксплуатации средств защиты информации	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ОПК-2.3; ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ПК-13.1; ПК-13.2; ПК-13.3
20.	Порядок выполнения работ при внедрении средств защиты информации	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ОПК-2.3; ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ПК-13.1; ПК-13.2; ПК-13.3
21.	Основные проблемы, присутствующие при внедрении и эксплуатации средств защиты информации	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ОПК-2.3; ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ПК-13.1; ПК-13.2; ПК-13.3
22.	Аппаратные и программные средства обеспечения защиты информации	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ОПК-2.3; ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ПК-13.1; ПК-13.2; ПК-13.3
23.	Меры безопасности, используемые при эксплуатации средств защиты информации	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ОПК-2.3; ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ПК-13.1; ПК-13.2; ПК-13.3
24.	Меры противодействия иностранным техническим разведкам при внедрении и эксплуатации средств защиты информации	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ОПК-2.3; ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ПК-13.1; ПК-13.2; ПК-13.3
25.	Анализ изменения контролируемой зоны при внедрении и эксплуатации средств защиты информации	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ОПК-2.3; ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ПК-13.1; ПК-13.2; ПК-13.3
26.	Реализация инженерно-технической защиты информации при внедрении и эксплуатации средств защиты информации	ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ОПК-2.3; ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ПК-13.1; ПК-13.2; ПК-13.3

Примерные тестовые задания проверка сформированности компетенций – ОПК-2.1; ОПК-2.3; ПК-13

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 (дата обращения: 29.04.2021).
3. *Wireshark Developer's* Guide [Электронный ресурс] : Режим доступа : https://www.wireshark.org/docs/wsdg_html_chunked/, свободный. – Загл. с экрана (дата обращения: 29.04.2021).

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

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.

9. Методические материалы

9.1. Планы практических занятий – проверка сформированности компетенций – ОПК-2

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 – ОПК-2.1; ОПК-2.3; ПК-13***

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

Список литературы:

1. *Тумбинская М.В. Комплексное обеспечение информационной безопасности на предприятии: учебник для вузов/ ТумбинскийМ.В., Петровский М.В. – Санкт-Петербург : Лань*, 2019.- 343с.
2. *Нестеров, С. А. Основы информационной безопасности : учебное пособие / С. А. Нестеров. — 5-е изд., стер. — Санкт-Петербург : Лань, 2019. — 324 с.*

Материально-техническое обеспечение занятия:

1. Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, ППП Cisco Packet Tracer и Wireshark.

Практическая работа № 2 (6 ч) ***Планирование затрат на внедрение и эксплуатацию средств защиты информации – ОПК-2.1; ОПК-2.3; ПК-13***

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.

Список литературы:

1. Тумбинская М.В. Комплексное обеспечение информационной безопасности на предприятии: учебник для вузов/ ТумбинскийМ.В., Петровский М.В. – Санкт-Петербург : Лань, 2019. 343с.
2. Нестеров, С. А. Основы информационной безопасности : учебное пособие / С. А. Нестеров. — 5-е изд., стер. — Санкт-Петербург : Лань, 2019. — 324 с.

Материально-техническое обеспечение занятия:

1. Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, ППП Cisco Packet Tracer и Wireshark.

Практические работы № 3 (6 ч) ***Анализ рисков информационной безопасности – ОПК-2.1; ОПК-2.3; ПК-13***

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.

Список литературы:

1. *Тумбинская М.В. Комплексное обеспечение информационной безопасности на предприятии: учебник для вузов/ ТумбинскийМ.В., Петровский М.В. – Санкт-Петербург : Лань, 2019. 343с.*
2. *Нестеров, С. А. Основы информационной безопасности : учебное пособие / С. А. Нестеров. — 5-е изд., стер. — Санкт-Петербург : Лань, 2019. — 324 с.*

Материально-техническое обеспечение занятия:

1. Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, ППП Cisco Packet Tracer .

Практическая работа № 4 (6 ч) ***Планирование затрат на информационную безопасность – ОПК-2.1; ОПК-2.3; ПК-13***

Задания:

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

Список литературы:

1. *Тумбинская М.В. Комплексное обеспечение информационной безопасности на предприятии: учебник для вузов/ ТумбинскийМ.В., Петровский М.В. – Санкт-Петербург : Лань, 2019. 343с.*
2. *Нестеров, С. А. Основы информационной безопасности : учебное пособие / С. А. Нестеров. — 5-е изд., стер. — Санкт-Петербург : Лань, 2019. — 324 с.*

Материально-техническое обеспечение занятия:

1. Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, ППП Cisco Packet Tracer и Wireshark.

Приложение 1

АННОТАЦИЯ ДИСЦИПЛИНЫ

Дисциплина «Внедрение и эксплуатация средств защиты информации» реализуется на факультете Информационных систем и безопасности для студентов 4-го курса, обучающихся по программе бакалавриата по направлению подготовки 10.03.01 Информационная безопасность (профили подготовки – Организация и технология защиты информации) кафедрой комплексной защиты информации.

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.

Дисциплина направлена на формирование следующих компетенций:

- ОПК-2.1 – Способен проводить анализ функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба
  - ОПК-2.1.1 – Знает принципы построения систем защиты информации; критерии оценки эффективности и надёжности средств защиты программного обеспечения автоматизированных систем; основные угрозы безопасности информации и модели нарушителя
  - ОПК-2.1.2 – Умеет анализировать угрозы безопасности информации, оценивать информационные риски; применять аналитические и компьютерные модели автоматизированных систем и систем защиты информации; анализировать программные и программно-аппаратные решения при проектировании системы защиты информации с целью выявления уязвимостей
  - ОПК-2.1.3 – Владеет навыками расчёта показателей эффективности защиты информации, обрабатываемой в автоматизированных системах; проведения анализа уязвимости программного и программно-аппаратных средств защиты информации
- ОПК-2.3 – Способен разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности
  - ОПК-2.3.1 – Знает национальные, межгосударственные и международные стандарты в области защиты информации, нормативные правовые акты в области защиты информации, руководящие и методические документы уполномоченных федеральных органов исполнительной власти в области внедрения и эксплуатации средств защиты информации
  - ОПК-2.3.2 – Умеет документировать процедуры и результаты контроля функционирования системы защиты информации; проводить испытания программно-технических средств защиты информации от НСД и специальных воздействий на соответствие требованиям по безопасности информации и техническим условиям
  - ОПК-2.3.3 – Владеет навыками внесения изменений в эксплуатационную документацию и организационно-распорядительные документы по системе защиты информации; навыками разработки программ и методик испытаний опытного образ-

ца программно-технического средства защиты информации от НСД и специальных воздействий на соответствие техническим условиям

- ПК-13 –- Способен принимать участие в формировании, организации и поддержания выполнения комплекса мер по обеспечению ин-формационной 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

В результате освоения дисциплины обучающийся должен:

Знать: принципы построения систем защиты информации; критерии оценки эффективности и надёжности средств защиты программного обеспечения автоматизированных систем; основные угрозы безопасности информации и модели нарушителя, процедуру организации установки и настройки технических, программных (программно-технических) средств защиты информации, входящих в состав системы защиты информации в соответствии с техническим проектом и инструкциями по эксплуатации;
Уметь: анализировать угрозы безопасности информации, оценивать информационные риски; применять аналитические и компьютерные модели автоматизированных систем и систем защиты информации; анализировать программные и программно-аппаратные решения при проектировании системы защиты информации с целью выявления уязвимостей; документировать процедуры и результаты контроля функционирования системы защиты информации; проводить испытания программно-технических средств защиты информации от НСД и специальных воздействий на соответствие требованиям по безопасности информации и техническим условиям; разрабатывать и реализовывать организационные меры, обеспечивающие эффективность системы защиты информации
Владеть: навыками расчёта показателей эффективности защиты информации, обрабатываемой в автоматизированных системах; проведения анализа уязвимости программного и программно-аппаратных средств защиты информации; навыками внесения изменений в эксплуатационную документацию и организационно-распорядительные документы по системе защиты информации; навыками разработки программ и методик испытаний опытного образца программно-технического средства защиты информации от НСД и специальных воздействий на соответствие техническим условиям; навыками организации и сопровождения аттестации объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации

По дисциплине предусмотрена промежуточная аттестация в форме зачёта.

Общая трудоёмкость освоения дисциплины составляет 2 зачётные единицы.

Приложение 2

УТВЕРЖДЕНО
Протокол заседания кафедры
№_____ от_____

ЛИСТ ИЗМЕНЕНИЙ

в рабочей программе дисциплины Внедрение и эксплуатация средств защиты информации

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