Аннотация к рабочей программе дисциплины «Оценка защищённости информационных систем»

Цель преподавания дисциплины

Дисциплина "Защищённые информационные системы" преподается с целью обучения студентов основным способам, методам, принципам, технологиям и средствам оценки защищенности информационных систем с применением актуальных инструментальных средств с учетом требований нормативно-правовой базы Российской Федерации.

Задачи изучения дисциплины

В результате изучения дисциплины студенты должны:

- сформировать профессиональные навыки проведения оценки состояния защищенности информационных систем (ИБ) в ИС;
- понимать принципы построения защищенных ИС;
- познакомиться с уязвимостями, угрозами ИБ и видами деструктивного воздействия, характерными для современных ИС;
- изучить подходы и методы обеспечения ИБ ИС, а также анализировать риски ИБ.

Компетенции, формируемые в результате освоения дисциплины

Способен проводить теоретические и экспериментальные исследования защищённости информационных систем (ПК-3);
Способен управлять рисками информационной безопасности(ПК-8);
Способен контролировать защищённость информационных систем(ПК-9).

Разделы дисциплины

Нормативная база оценки защищенности ИТ. Основные аспекты построения системы информационной безопасности. Базовые вопросы проверки защищенности ИТ. Виды проверок.

Внутренний аудит ИБ. Внешний аудит ИБ. Системы анализа защищенности. Системы обнаружения и предотвращения вторжений.

МИНОБРНАУКИ РОССИИ
Юго-Западный государственный университет

УТВЕРЖДАЮ:
Декан факультета
фундаментальной и прикладной
(наименование ф-та полностью)
информатики

М.О. Таныгин
(подпись, инициалы, фамилия)
«31» 08 2021 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Оценка защищённости информационных систем
(наименование дисциплины)

ОПОП ВО 10.04.01 Информационная безопасность
шифр и наименование направление подготовки (специальности)

Защищённые информационные системы
наименование направленности (профиля, специализации)

форма обучения очная
очная, очно-заочная, заочная

Курск – 2021

Рабочая программа дисциплины составлена в соответствии с ФГОС ВО – магистратура по направлению подготовки 10.04.01 Информационная безопасность на основании учебного плана ОПОП ВО 10.04.01 Информационная безопасность, профиль «Защищённые информационные системы», одобренного Ученым советом университета (протокол № 6 «26» 02 2021 г.).

Рабочая программа дисциплины обсуждена и рекомендована к реализации в образовательном процессе для обучения студентов по ОПОП ВО 10.04.01 Информационная безопасность, профиль «Защищённые информационные системы» на заседании кафедры информационной безопасности № 1 «30» августа 2021 г.

Зав. кафедрой _____ Таныгин М.О.

Разработчик программы

к.т.н., доцент _____ Ефремов М.А.

(ученая степень и ученое звание, Ф.И.О.)

Директор научной библиотеки _____ Макаровская В.Г.

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.04.01 Информационная безопасность, профиль «Защищённые информационные системы», одобренного Ученым советом университета протокол №6 «26» 02 2021 г., на заседании кафедры ИБ №10 от 30.06.2022 г.

(наименование кафедры, дата, номер протокола)

Зав. кафедрой Таныгин М.О.

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.04.01 Информационная безопасность, профиль «Защищённые информационные системы», одобренного Ученым советом университета протокол №7 «28» 02 2022 г., на заседании кафедры ИБ, протокол №1 от 30.08.2023.

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.04.01 Информационная безопасность, профиль «Защищённые информационные системы», одобренного Ученым советом университета протокол №___«__»_____20___г., на заседании кафедры _____.

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.04.01 Информационная безопасность, профиль «Защищённые информационные системы», одобренного Ученым советом университета протокол

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.04.01 Информационная безопасность, профиль «Защищённые информационные системы», одобренного Ученым советом университета протокол №___«__»_____20___г., на заседании кафедры_____ .

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.04.01 Информационная безопасность, профиль «Защищённые информационные системы», одобренного Ученым советом университета протокол №___«__»_____20___г., на заседании кафедры _____ .

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.04.01 Информационная безопасность, профиль «Защищённые информационные системы», одобренного Ученым советом университета протокол №___«__»_____20___г., на заседании кафедры _____ .

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.04.01 Информационная безопасность, профиль «Защищённые информационные системы», одобренного Ученым советом университета протокол №___«__»_____20___г., на заседании кафедры_____ .

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

1. Цель и задачи дисциплины. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы

1.1. Цель преподавания дисциплины

Дисциплина "Защищённые информационные системы" преподается с целью обучения студентов основным способам, методам, принципам, технологиям и средствам оценки защищенности информационных систем с применением актуальных инструментальных средств с учетом требований нормативно-правовой базы Российской Федерации.

1.2. Задачи изучения дисциплины

В результате изучения дисциплины студенты должны:

- сформировать профессиональные навыки проведения оценки состояния защищенности информационных систем (ИБ) в ИС;
- понимать принципы построения защищенных ИС;
- познакомиться с уязвимостями, угрозами ИБ и видами деструктивного воздействия, характерными для современных ИС;
- изучить подходы и методы обеспечения ИБ ИС, а также анализировать риски ИБ.

1.3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы

Таблица 1.3 – Результаты обучения по дисциплине

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код комп	*наименование компетенции*		
ПК-3	Способен проводить теоретические и экспериментальные исследования защищённости информационных систем	ПК-3.3 Формулирует целевые критерии для оценивания эффективности исследуемых систем	***Знать:*** - основные целевые критерии для оценки эффективности исследуемых систем; - определение информации и её типы с точки зрения защищённости ИС; - принципы создания экспертной комиссии для проведения оценки эффективности исследуемых систем с учётом основных типов угроз нарушения: конфиденциальности, целостности, доступности информации. ***Уметь:*** - определять целевые критерии для оценки эффективности исследуемых систем; - определять тип информации; - самостоятельно организовывать экспертную комиссию для оценивания эффективности исследуемых систем ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками анализа целевых критериев для оценивания эффективности исследуемых систем; - навыками определения типа информации, подлежащей защите; - навыками организации экспертной оценки эффективности исследуемых систем.
		ПК-3.4 Определяет в результате натурных или математических экспериментов характеристики защищённых информационных систем	***Знать:*** - основные подходы к оценке качества защищённых ИС; - методики проведения натурных и математических экспериментов характеристики защищённых ИС; - методологические аспекты для выявления соответствия характеристик защищённых ИС требованиям, к ним предъявляемым. ***Уметь:*** - определять функциональные характеристики отдельных структурных компонентов ИС - определять на основе функционала компонентов защищённых ИС уровень защищённости системы в целом; - самостоятельно разрабатывать программы и методики проведения натурных и математических исследований средств и систем обеспечения информационной безопасности. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками анализа защищённых ИС и выявления характеристик, как всех систем в целом, так и их отдельных функциональных блоков;

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код комп	*наименование компетенции*		
			- навыками разработки технического облика средств обработки и передачи данных в информационных системах; - навыками разработки методик теоретических и экспериментальных исследований защищённости информационных систем.
ПК-8	Способен управлять рисками информационной безопасности	ПК-8.1 Формирует перечень угроз для защищаемой информационной системы	***Знать*** -определение угрозы защищённой ИС; -классификацию и общий анализ угроз; -отличие случайных и преднамеренных угроз; - стек технологий обеспечения информационной безопасности. ***Уметь:*** - проводить анализ возможных угроз и каналов утечки информации; - проводить анализ рисков; - проводить анализ, используя ГОСТ и международные стандарты; ***Владеть (или Иметь опыт деятельности):*** - навыками определения угроз для защищаемой ИС; - навыками проведения анализа рисков.
		ПК-8.2 Формирует критерии оценки каждого вида угроз в защищаемой системе	***Знать:*** - основные характеристики ИС; - классификацию угроз и критерии оценки каждого вида; - виды уязвимостей в ИС. ***Уметь:*** - собирать данные о самой ИС; - формировать критерии каждого вида угрозы в защищаемой системе; - найти потенциальные уязвимости в ИС. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками сбора данных о самой ИС; - навыками определения потенциальных угроз; - навыками выявления потенциальных уязвимостей в ИС.
		ПК-8.3 Классифицирует угрозы информационной безопасности исходя из существующих и оригинальных методик	***Знать:*** - классификацию угроз информационной безопасности; - методики формирования модели угроз для информационной системы; - качественные и количественные методики оценки риска ИБ. ***Уметь:*** - выделять и ранжировать угрозы информационной безопасности; - определять наиболее подходящую методику для определения угрозы ИБ исходя из существующих и оригинальных методик; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками формирования списка угроз, актуальных для конкретной информационной системы

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код комп	*наименование компетенции*		
			- навыками правильного применения выбранной методики.
		ПК-8.4 Формирует перечень нарушителей информационной безопасности и их возможностей	***Знать:*** - определение нарушителя информационной безопасности; - модель нарушителя информационной безопасности; - перечень нарушителей информационной безопасности. ***Уметь:*** - определять нарушителя информационной безопасности; -спрогнозировать вероятных нарушителей информационной безопасности; - оценить уровень информированности потенциального нарушителя о защищаемой системе (ЗС) и возможность влияния на ЗС; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками определения нарушителя информационной безопасности; - навыками прогнозирования вероятных нарушителей информационной безопасности; - навыками оценки уровня информированности потенциального нарушителя.
ПК-9	Способен контролировать защищённость информационных систем	ПК-9.1 Разрабатывает методику оценки уровня защищённости информационной системы	***Знать:*** - исходные данные в БД предполагаемой информационной системе; - требования к уровню защищённости информационной безопасности; - комплексные показатели оценки состояния ИС их интерпретацию; ***Уметь:*** - подготовить исходные данные в БД - проводить контроль реализации требований; - рассчитывать комплексные показатели оценки состояния ИС и их интерпретировать; - разрабатывать рекомендации на базе оценки уровня защищённости информационной системы; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками оценки данных БД; - навыками расчета комплексных показателей; - навыками разработки рекомендаций.
		ПК-9.2 Проводит оценку соответствия уровня защищённости требованиям политики безопасности и нормативным документам	***Знать:*** - характеристики систем стандартизации в области защиты информации; - оценочные стандарты и технические спецификации: «Оранжевая книга», российские и международные стандарты оценки уровня защищённости; - виды тестирования систем информационной безопасности; ***Уметь:*** - составить перечень понятий и определений, используемых в стандартах и спецификациях;

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код комп	*наименование компетенции*		
			- протестировать систему защиты с целью проверки эффективности используемых в ней механизмов защиты, их устойчивости к атакам, а также с целью поиска уязвимостей. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками составления перечня понятий и определений, используемых в стандартах и спецификациях; - навыками тестирования системы защиты с целью проверки эффективности.
		ПК-9.3 Разрабатывает систему мероприятий по оценке уровня защищённости информационной системы	***Знать:*** -требования по защите данных; - методы инструментального мониторинга защищенности информации; - способы и средства выявления каналов утечки информации. ***Уметь:*** - разрабатывать технический проект в части защиты информации; - проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации - разрабатывать эксплуатационную документацию и средства защиты информации, а также организационно- распорядительные документы. ***Владеть (****или* ***Иметь опыт деятельности):*** -навыками управления проектом; -навыками оценки на основе инструментального мониторинга защищенности информации; - навыками оформления необходимой документации.
		ПК-9.4 Определяет уязвимости защищённости телекоммуникационных систем и сетей	***Знать:*** - определение уязвимости информационных объектов и их классификацию; - понятие риска. Способы оценки рисков; - модель нарушителя информационной безопасности телекоммуникационных систем и сетей. ***Уметь:*** - выявлять потенциальные уязвимости защищённости телекоммуникационных систем; - проводить оценку рисков; - определять потенциальных нарушителей информационной безопасности телекоммуникационных систем и сетей. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками определения уязвимости защищённости телекоммуникационных систем и сетей; - навыками проведения оценки рисков; - навыками определения потенциальных нарушителей.

2. Указание места дисциплины в структуре основной профессиональной образовательной программы

Дисциплина «Оценка защищённости информационных систем» входит в часть, формируемую участниками образовательных отношений блока 1 «Дисциплины (модули»») основной профессиональной образовательной программы – программы магистратуры 10.04.01 Информационная безопасность профиль «Защищённые информационные системы». Дисциплина изучается на 2 курсе в 3 семестре.

3. Объем дисциплины в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоёмкость (объём) дисциплины составляет 3 зачётные единицы, 108 часов

Таблица 3 – Объем дисциплины

Виды учебной работы	Всего, часов
Общая трудоемкость дисциплины	108
Контактная работа обучающихся с преподавателем по видам учебных занятий (всего)	54.1
в том числе:	
лекции	18
лабораторные занятия	36
практические занятия	
Самостоятельная работа обучающихся (всего)	53.9
Контроль (подготовка к экзамену)	
Контактная работа по промежуточной аттестации (всего АттКР)	0.1
в том числе:	
зачет	0.1
зачет с оценкой	не предусмотрен
курсовая работа (проект)	не предусмотрена
экзамен (включая консультацию перед экзаменом)	не предусмотрена

4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1. Содержание дисциплины

Таблица 4.1.1 – Содержание дисциплины, структурированное по темам (разделам)

№ п/п	Раздел (тема) дисциплины	Содержание
1.	Нормативная база оценки защищенности ИТ	Существующие стандарты и методологии проверки и оценки защищенности ИТ и СУИБ: их отличия, сильные и слабые стороны. История развития
2.	Основные аспекты построения системы информационной безопасности	Регулирование ответственности нарушений информационной безопасности. Программа информационной безопасности. Контроль деятельности в области безопасности. Модели представления информационной защиты. Формирование требований к системе информационной безопасности. Этапы обеспечения информационной безопасности.
3.	Базовые вопросы проверки защищенности ИТ	Понятие процесса. Методы формализации процессов. Цели и задачи формализации процессов. Основные процессы. Понятие процессного подхода. Цели и задачи процессов оценки защищенности ИТ и СУИБ. Важность процесса с точки зрения управления ИБ. Участники процесса. Связи с другими процессами СУИБ.
4.	Виды проверок	Мониторинг ИБ. Самооценка ИБ. Внутренний и внешний аудиты ИБ. Анализ СУИБ со стороны высшего руководства организации.
5.	Внутренний аудит ИБ	Цели и задачи, организационные принципы, принципы обеспечения эффективности. Подразделение внутреннего аудита, контролирующее вопросы ОИБ в организации.
6.	Внешний аудит ИБ	Цели и задачи, принципы проведения, управление программой, этапы проведения. Компетентность аудиторов. Взаимоотношения представителей аудиторской группы и проверяемых организаций.
7.	Системы анализа защищенности	Виды систем, решаемые задачи, использование в целях оценки защищенности ИТ.
8.	Системы обнаружения и предотвращения вторжений	Виды систем, решаемые задачи, использование в целях оценки защищенности ИТ.

Таблица 4.1.2 – Содержание дисциплины и её методическое обеспечение

№ Пп/п	Раздел (тема) дисциплины	Виды деятельности			Учебно-методические материалы	Формы текущего контроля успеваемости *(по неделям семестра)*	Компетенции
		лек., час	№ лб.	№ пр.			

1	2	3	4	5	6	7	8
1.	Нормативная база оценки защищенности ИТ	2			У-1,2 МО-1	С,Т	ПК-3
2.	Основные аспекты построения системы информационной безопасности	2	1		У-1-3 МО-1,2	С,Т	ПК-3 ПК-8 ПК-9
3.	Базовые вопросы проверки защищенности ИТ	4	2		У-1-3 МО-1,2	С	ПК-8 ПК-9
4.	Виды проверок	2	3		У-1-3 МО-1,2	С	ПК-8 ПК-9
5.	Внутренний аудит ИБ	2			У-1-3 МО-1,2	С	ПК-8 ПК-9
6.	Внешний аудит ИБ	2			У-1-3 МО-1,2	С,Т	ПК-8 ПК-9
7.	Системы анализа защищенности	2	4		У-1-3 МО-1,2	С,Т	ПК-8 ПК-9
8.	Системы обнаружения и предотвращения вторжений	2	5		У-1-3 МО-1,2	С,Т	ПК-8 ПК-9
9.	Итого	18					

С – собеседование, Т – тест

4.2. Лабораторные работы и практические занятия

4.2.1. Лабораторные работы

Таблица 4.2.1 – Лабораторные работы

№	Наименование лабораторной работы	Объем, час.
1.	Разработка регламента защищенности к проектируемым информационным системам	4
2.	Контроль защищенности информационных систем	6
3.	Анализ типовых уязвимостей распределенных информационных систем	12
4.	Сетевые и узловые системы анализа защищенности;	6
5.	Сетевые и узловые системы обнаружения и предотвращений вторжений.	8
Итого		36

4.3. Самостоятельная работа студентов (СРС)

Таблица 4.5 – Самостоятельная работа студентов

№	Наименование раздела учебной дисциплины	Срок	Время на выполнение СРС, час.
1.	Нормативная база оценки защищенности ИТ	1-2 недели	4
2.	Основные аспекты построения системы информационной безопасности	2-3 недели	6
3.	Базовые вопросы проверки защищенности ИТ	4-5 недели	6

4.	Виды проверок	5-6 недели	6
5.	Внутренний аудит ИБ	7-10 недели	6
6.	Внешний аудит ИБ	11-14 недели	5.9
7.	Системы анализа защищенности	13-15 недели	10
8.	Системы обнаружения и предотвращения вторжений	16-18 недели	10
Итого			53.9

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Студенты могут при самостоятельном изучении отдельных тем и вопросов дисциплин пользоваться учебно-наглядными пособиями, учебным оборудованием и методическими разработками кафедры в рабочее время, установленное Правилами внутреннего распорядка работников.

Учебно-методическое обеспечение для самостоятельной работы обучающихся по данной дисциплине организуется:

библиотекой университета:

− библиотечный фонд укомплектован учебной, методической, научной, периодической, справочной и художественной литературой в соответствии с данной РПД;

− имеется доступ к основным информационным образовательным ресурсам, информационной базе данных, в том числе библиографической, возможность выхода в Интернет.

кафедрой:

− путем обеспечения доступности всего необходимого учебно-методического и справочного материала;

− путем предоставления сведений о наличии учебно-методической литературы, современных программных средств;

− путем разработки вопросов к экзамену, методических указаний к выполнению лабораторных работ.

типографией университета:

− путем помощи авторам в подготовке и издании научной, учебной, учебно-методической литературы;

− путем удовлетворения потребностей в тиражировании научной, учебной, учебно-методической литературы.

6. Образовательные технологии.

Технологии использования воспитательного потенциала дисциплины

Содержание дисциплины обладает значительным воспитательным потенциалом, поскольку в нем аккумулирован научный опыт человечества. Реализация воспитательного потенциала дисциплины осуществляется в рамках единого образовательного и воспитательного процесса и способствует непрерывному развитию личности каждого обучающегося. Дисциплина вносит значимый вклад в формирование общей и профессиональной культуры обучающихся. Содержание дисциплины способствует правовому, экономическому, профессионально-трудовому, воспитанию обучающихся.

Реализация воспитательного потенциала дисциплины подразумевает:

– целенаправленный отбор преподавателем и включение в лекционный материал, материал для практических и (или) лабораторных занятий содержания, демонстрирующего обучающимся образцы настоящего научного подвижничества создателей и представителей данной отрасли науки (производства, экономики, культуры), высокого профессионализма ученых (представителей производства, деятелей культуры), их ответственности за результаты и последствия деятельности для человека и общества; примеры подлинной нравственности людей, причастных к развитию науки и производства;

– применение технологий, форм и методов преподавания дисциплины, имеющих высокий воспитательный эффект за счет создания условий для взаимодействия обучающихся с преподавателем, другими обучающимися, (командная работа, разбор конкретных ситуаций)*;*

– личный пример преподавателя, демонстрацию им в образовательной деятельности и общении с обучающимися за рамками образовательного процесса высокой общей и профессиональной культуры.

Реализация воспитательного потенциала дисциплины на учебных занятиях направлена на поддержание в университете единой развивающей образовательной и воспитательной среды. Реализация воспитательного потенциала дисциплины в ходе самостоятельной работы обучающихся способствует развитию в них целеустремленности, инициативности, креативности, ответственности за результаты своей работы – качеств, необходимых для успешной социализации и профессионального становления.

7. Фонд оценочных средств для проведения промежуточной аттестации

7.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Таблица 7.1 – Этапы формирования компетенций

Код и содержание компетенции	Этапы формирования компетенций и дисциплины (модули), при изучении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
ПК-3 Способен проводить теоретические и экспериментальные исследования защищённости информационных систем	Математические проблемы обеспечения информационной безопасности Теоретические основы компьютерной безопасности		Производственная преддипломная практика Подготовка к процедуре защиты и защита выпускной квалификационной работы
ПК-8 Способен управлять рисками информационной безопасности	Информационно-аналитические системы безопасности Экспертные системы комплексной оценки безопасности информационных и телекоммуникационных систем		Подготовка к процедуре защиты и защита выпускной квалификационной работы
ПК-9 Способен контролировать защищённость информационных систем	Методы и средства защиты информации в системах электронного документооборота		Подготовка к процедуре защиты и защита выпускной квалификационной работы

7.2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Таблица 7.2 – Показатели и критерии оценивания компетенций, шкала оценивания

Код компетенции/ этап *(указывается название этапа из п.7.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
ПК-3 / осн	ПК-3.3 Формулирует целевые	***Знать:*** - основные целевые критерии для оценки эффективности	***Знать:*** - определение информации и её типы с точки зрения	***Знать:*** - принципы создания экспертной комиссии для проведения оценки

	критерии для оценивания эффективности исследуемых систем	исследуемых систем; ***Уметь:*** - определять целевые критерии для оценки эффективности исследуемых систем; - определять тип информации; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками анализа целевых критериев для оценивания эффективности исследуемых систем; - навыками определения типа информации, подлежащей защите;	защищённости ИС; - принципы создания экспертной комиссии для проведения оценки эффективности исследуемых систем с учётом основных типов угроз нарушения: конфиденциальности, целостности, ***Уметь:*** - определять тип информации; - самостоятельно организовывать экспертную комиссию для оценивания эффективности исследуемых систем ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками определения типа информации, подлежащей защите; - навыками организации экспертной оценки эффективности исследуемых систем.	эффективности исследуемых систем с учётом основных типов угроз нарушения: конфиденциальности, целостности, доступности информации. ***Уметь:*** - определять целевые критерии для оценки эффективности исследуемых систем; - определять тип информации; - самостоятельно организовывать экспертную комиссию для оценивания эффективности исследуемых систем ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками анализа целевых критериев для оценивания эффективности исследуемых систем; - навыками определения типа информации, подлежащей защите; - навыками организации экспертной оценки эффективности исследуемых систем.
	ПК-3.4 Определяет в результате натурных или математических экспериментов характеристики защищённых информационных систем	***Знать:*** - основные подходы к оценке качества защищённых ИС; ***Уметь:*** - определять функциональные характеристики отдельных структурных компонентов ИС ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками анализа защищённых ИС и выявления характеристик, как всех систем в целом, так и их отдельных функциональных блоков; - навыками разработки технического облика средств обработки и передачи данных в	***Знать:*** - методики проведения натурных и математических экспериментов характеристики защищённых ИС; - методологические аспекты для выявления соответствия характеристик защищённых ИС требованиям, к ним предъявляемым. ***Уметь:*** - определять на основе функционала компонентов защищённых ИС уровень защищённости системы в целом; - самостоятельно разрабатывать программы и методики проведения	***Знать:*** - методики проведения натурных и математических экспериментов характеристики защищённых ИС; - методологические аспекты для выявления соответствия характеристик защищённых ИС требованиям, к ним предъявляемым. ***Уметь:*** - определять на основе функционала компонентов защищённых ИС уровень защищённости системы в целом; - самостоятельно разрабатывать программы и методики проведения натурных и математических исследований средств и

		информационных системах; - навыками разработки методик теоретических и экспериментальных исследований защищённости информационных систем.	натурных и математических исследований средств и систем обеспечения информационной безопасности. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками разработки технического облика средств обработки и передачи данных в информационных системах; - навыками разработки методик теоретических и экспериментальных исследований защищённости информационных систем.	систем обеспечения информационной безопасности. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками анализа защищённых ИС и выявления характеристик, как всех систем в целом, так и их отдельных функциональных блоков; - навыками разработки технического облика средств обработки и передачи данных в информационных системах; - навыками разработки методик теоретических и экспериментальных исследований защищённости информационных систем.
ПК-8 / осн	ПК-8.1 Формирует перечень угроз для защищаемой информационной системы	***Знать*** -определение угрозы защищённой ИС; -классификацию и общий анализ угроз; - стек технологий обеспечения информационной безопасности. ***Уметь:*** - проводить анализ возможных угроз и каналов утечки информации; - проводить анализ, используя ГОСТ и международные стандарты; ***Владеть (или Иметь опыт деятельности):*** - навыками определения угроз для защищаемой ИС;	***Знать*** -классификацию и общий анализ угроз; -отличие случайных и преднамеренных угроз; - стек технологий обеспечения информационной безопасности. ***Уметь:*** - проводить анализ рисков; - проводить анализ, используя ГОСТ и международные стандарты; ***Владеть (или Иметь опыт деятельности):*** - навыками определения угроз для защищаемой ИС; - навыками проведения анализа рисков.	***Знать*** -определение угрозы защищённой ИС; -классификацию и общий анализ угроз; -отличие случайных и преднамеренных угроз; - стек технологий обеспечения информационной безопасности. ***Уметь:*** - проводить анализ возможных угроз и каналов утечки информации; - проводить анализ рисков; - проводить анализ, используя ГОСТ и международные стандарты; ***Владеть (или Иметь опыт деятельности):*** - навыками определения угроз для защищаемой ИС; - навыками проведения анализа рисков.
	ПК-8.2 Формирует критерии оценки каждого вида угроз в	***Знать:*** - основные характеристики ИС; - виды уязвимостей в ИС. ***Уметь:*** - собирать данные о	***Знать:*** - классификацию угроз и критерии оценки каждого вида; - виды уязвимостей в ИС. ***Уметь:***	***Знать:*** - основные характеристики ИС; - классификацию угроз и критерии оценки каждого вида; - виды уязвимостей в

	защищаемой системе	самой ИС; - найти потенциальные уязвимости в ИС. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками сбора данных о самой ИС; - навыками определения потенциальных угроз;	- собирать данные о самой ИС; - формировать критерии каждого вида угрозы в защищаемой системе; - найти потенциальные уязвимости в ИС. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками определения потенциальных угроз;	ИС. ***Уметь:*** - собирать данные о самой ИС; - формировать критерии каждого вида угрозы в защищаемой системе; - найти потенциальные уязвимости в ИС. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками сбора данных о самой ИС; - навыками определения потенциальных угроз; - навыками выявления потенциальных уязвимостей в ИС.
	ПК-8.3 Классифицирует угрозы информационной безопасности исходя из существующих и оригинальных методик	***Знать:*** - классификацию угроз информационной безопасности; - качественные и количественные методики оценки риска ИБ. ***Уметь:*** - выделять и ранжировать угрозы информационной безопасности; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками правильного применения выбранной методики.	***Знать:*** - методики формирования модели угроз для информационной системы; - качественные и количественные методики оценки риска ИБ. ***Уметь:*** - определять наиболее подходящую методику для определения угрозы ИБ исходя из существующих и оригинальных методик; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками формирования списка угроз, актуальных для конкретной информационной системы -	***Знать:*** - классификацию угроз информационной безопасности; - методики формирования модели угроз для информационной системы; - качественные и количественные методики оценки риска ИБ. ***Уметь:*** - выделять и ранжировать угрозы информационной безопасности; - определять наиболее подходящую методику для определения угрозы ИБ исходя из существующих и оригинальных методик; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками формирования списка угроз, актуальных для конкретной информационной системы - навыками правильного применения выбранной методики.
	ПК-8.4 Формирует перечень нарушителей информационной безопасности и	***Знать:*** - определение нарушителя информационной безопасности; - перечень нарушителей информационной	***Знать:*** - модель нарушителя информационной безопасности; - перечень нарушителей информационной безопасности.	***Знать:*** - определение нарушителя информационной безопасности; - модель нарушителя информационной безопасности;

	их возможностей	безопасности. ***Уметь:*** - определять нарушителя информационной безопасности; - оценить уровень информированности потенциального нарушителя о защищаемой системе (ЗС) и возможность влияния на ЗС; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками определения нарушителя информационной безопасности; - навыками оценки уровня информированности потенциального нарушителя.	***Уметь:*** -спрогнозировать вероятных нарушителей информационной безопасности; - оценить уровень информированности потенциального нарушителя о защищаемой системе (ЗС) и возможность влияния на ЗС; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками прогнозирования вероятных нарушителей информационной безопасности; - навыками оценки уровня информированности потенциального нарушителя.	- перечень нарушителей информационной безопасности. ***Уметь:*** - определять нарушителя информационной безопасности; -спрогнозировать вероятных нарушителей информационной безопасности; - оценить уровень информированности потенциального нарушителя о защищаемой системе (ЗС) и возможность влияния на ЗС; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками определения нарушителя информационной безопасности; - навыками прогнозирования вероятных нарушителей информационной безопасности; - навыками оценки уровня информированности потенциального нарушителя.
ПК-9 / осн	ПК-9.1 Разрабатывает методику оценки уровня защищённости информационной системы	***Знать:*** - исходные данные в БД предполагаемой информационной системе; - комплексные показатели оценки состояния ИС их интерпретацию; ***Уметь:*** - проводить контроль реализации требований; - рассчитывать комплексные показатели оценки состояния ИС и их интерпретировать; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками оценки данных БД; - навыками разработки рекомендаций.	***Знать:*** - требования к уровню защищённости информационной безопасности; - комплексные показатели оценки состояния ИС их интерпретацию; ***Уметь:*** - подготовить исходные данные в БД - проводить контроль реализации требований; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками оценки данных БД; - навыками расчета комплексных показателей; - навыками разработки	***Знать:*** - исходные данные в БД предполагаемой информационной системе; - требования к уровню защищённости информационной безопасности; - комплексные показатели оценки состояния ИС их интерпретацию; ***Уметь:*** - проводить контроль реализации требований; - рассчитывать комплексные показатели оценки состояния ИС и их интерпретировать; - разрабатывать рекомендации на базе оценки уровня защищённости информационной системы; ***Владеть (****или* ***Иметь опыт деятельности):***

			рекомендаций.	- навыками оценки данных БД; - навыками расчета комплексных показателей; - навыками разработки рекомендаций.
	ПК-9.2 Проводит оценку соответствия уровня защищённости требованиям политики безопасности и нормативным документам	***Знать:*** - характеристики систем стандартизации в области защиты информации; - виды тестирования систем информационной безопасности; ***Уметь:*** - составить перечень понятий и определений, используемых в стандартах и спецификациях; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками составления перечня понятий и определений, используемых в стандартах и спецификациях;	***Знать:*** - оценочные стандарты и технические спецификации: «Оранжевая книга», российские и международные стандарты оценки уровня защищённости; - виды тестирования систем информационной безопасности; ***Уметь:*** - протестировать систему защиты с целью проверки эффективности используемых в ней механизмов защиты, их устойчивости к атакам, а также с целью поиска уязвимостей. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками тестирования системы защиты с целью проверки эффективности.	***Знать:*** - характеристики систем стандартизации в области защиты информации; - оценочные стандарты и технические спецификации: «Оранжевая книга», российские и международные стандарты оценки уровня защищённости; - виды тестирования систем информационной безопасности; ***Уметь:*** - составить перечень понятий и определений, используемых в стандартах и спецификациях; - протестировать систему защиты с целью проверки эффективности используемых в ней механизмов защиты, их устойчивости к атакам, а также с целью поиска уязвимостей. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками составления перечня понятий и определений, используемых в стандартах и спецификациях; - навыками тестирования системы защиты с целью проверки эффективности.
	ПК-9.3 Разрабатывает систему мероприятий по оценке уровня защищённости информационной системы	***Знать:*** -требования по защите данных; - методы инструментального мониторинга - способы и средства выявления каналов утечки информации. ***Уметь:*** - разрабатывать	***Знать:*** - методы инструментального мониторинга защищенности информации; - способы и средства выявления каналов утечки информации. ***Уметь:*** - проводить	***Знать:*** -требования по защите данных; - методы инструментального мониторинга защищенности информации; - способы и средства выявления каналов утечки информации.

		технический проект в части защиты информации; - разрабатывать эксплуатационную документацию и средства защиты информации, а также организационно-распорядительные документы. ***Владеть (****или* ***Иметь опыт деятельности):*** -навыками управления проектом; -навыками оценки на основе инструментального мониторинга защищенности информации;	инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации - разрабатывать эксплуатационную документацию и средства защиты информации, а также организационно-распорядительные документы. ***Владеть (****или* ***Иметь опыт деятельности):*** -навыками оценки на основе инструментального мониторинга защищенности информации; - навыками оформления необходимой документации.	***Уметь:*** - разрабатывать технический проект в части защиты информации; - проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации - разрабатывать эксплуатационную документацию и средства защиты информации, а также организационно-распорядительные документы. ***Владеть (****или* ***Иметь опыт деятельности):*** -навыками управления проектом; -навыками оценки на основе инструментального мониторинга защищенности информации; - навыками оформления необходимой документации.
	ПК-9.4 Определяет уязвимости защищённости телекоммуникационных систем и сетей	***Знать:*** - определение уязвимости информационных объектов и их классификацию; - понятие риска. Способы оценки рисков; ***Уметь:*** - выявлять потенциальные уязвимости защищённости телекоммуникационных систем; - проводить оценку рисков; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками определения уязвимости защищённости телекоммуникационн	***Знать:*** - понятие риска. Способы оценки рисков; - модель нарушителя информационной безопасности телекоммуникационных систем и сетей. ***Уметь:*** - проводить оценку рисков; - определять потенциальных нарушителей информационной безопасности телекоммуникационных систем и сетей. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками определения уязвимости защищённости	***Знать:*** - определение уязвимости информационных объектов и их классификацию; - понятие риска. Способы оценки рисков; - модель нарушителя информационной безопасности телекоммуникационных систем и сетей. ***Уметь:*** - выявлять потенциальные уязвимости защищённости телекоммуникационных систем; - проводить оценку рисков; - определять потенциальных нарушителей информационной

		ых систем и сетей; - навыками проведения оценки рисков;	телекоммуникационных систем и сетей; - навыками проведения оценки рисков; - навыками определения потенциальных нарушителей.	безопасности телекоммуникационных систем и сетей. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками определения уязвимости защищённости телекоммуникационных систем и сетей; - навыками проведения оценки рисков; - навыками определения потенциальных нарушителей.

7.3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения основной профессиональной образовательной программы

Таблица 7.3 – Паспорт комплекта оценочных средств для текущего контроля успеваемости

/п	Раздел (тема) дисциплины	Код контролируемой компетенции (или ее части)	Технология формирования	Оценочные средства		Описание шкал оценивания
				наименование	№ заданий	
	2	3	4	5	6	7
1.	Нормативная база оценки защищенности ИТ	ПК-3 ПК-8 ПК-9	Лекция, СРС	Собеседование, тест	1-8, 1-20	Согласно табл. 7.2
2.	Основные аспекты построения системы информационной безопасности	ПК-3 ПК-8 ПК-9	Лекция, СРС, лабораторная работа	Собеседование, тест	9-18, 21-40, 1-4	Согласно табл. 7.2
3.	Базовые вопросы проверки защищенности ИТ	ПК-3 ПК-8 ПК-9	Лекция, СРС, лабораторная работа	Собеседование, тест	2 1-26 1-4	Согласно табл. 7.2

4.	Виды проверок	ПК-3 ПК-8 ПК-9	Лекция, СРС, лабораторная работа	Собеседование, тест	2 7-34 1 -4	Согласно табл. 7.2
5.	Внутренний аудит ИБ	ПК-3 ПК-8 ПК-9	Лекция, СРС	Собеседование, тест	3 5-41 1 -4	Согласно табл. 7.2
6.	Внешний аудит ИБ	ПК-3 ПК-8 ПК-9	Лекция, СРС,	Собеседование, тест	4 1-48 4 1-50	Согласно табл. 7.2
7.	Системы анализа защищенности	ПК-3 ПК-8 ПК-9	Лекция, СРС, лабораторная работа	Собеседование, тест	4 9-55 5 1-60 1 -4	Согласно табл. 7.2
8.	Системы обнаружения и предотвращения вторжений	ПК-3 ПК-8 ПК-9	Лекция, СРС, лабораторная работа	Собеседование, тест	5 6-68 1 -4	Согласно табл. 7.2

Примеры типовых контрольных заданий для проведения текущего контроля успеваемости

Вопросы для собеседования

Базовые вопросы проверки защищенности ИТ.

1. Дайте определение процессу в контексте ИТ.
2. Опишите методы формализации процессов.
3. Сформулируйте цели и задачи формализации процессов.
4. В чем заключается важность процесса с точки зрения управления ИБ.

Типовые задания для проведения промежуточной аттестации обучающихся

Промежуточная аттестация по дисциплине проводится в форме зачета. Зачет проводится в виде компьютерного тестирования.

Для тестирования используются контрольно-измерительные материалы (КИМ) – вопросы и задания в тестовой форме, составляющие банк тестовых

заданий (БТЗ) по дисциплине, утвержденный в установленном в университете порядке.

Проверяемыми на промежуточной аттестации элементами содержания являются темы дисциплины, указанные в разделе 4 настоящей программы. Все темы дисциплины отражены в КИМ в равных долях (%). БТЗ включает в себя не менее 100 заданий и постоянно пополняется. БТЗ хранится на бумажном носителе в составе УММ и электронном виде в ЭИОС университета.

Для проверки *знаний* используются вопросы и задания в различных формах:

- закрытой (с выбором одного или нескольких правильных ответов),
- открытой (необходимо вписать правильный ответ),
- на установление правильной последовательности,
- на установление соответствия.

Умения, навыки (или опыт деятельности) и компетенции проверяются с помощью компетентностно-ориентированных задач (ситуационных, производственных или кейсового характера) и различного вида конструкторов.

Все задачи являются многоходовыми. Некоторые задачи, проверяющие уровень сформированности компетенций, являются многовариантными. Часть умений, навыков и компетенций прямо не отражена в формулировках задач, но они могут быть проявлены обучающимися при их решении.

В каждый вариант КИМ включаются задания по каждому проверяемому элементу содержания во всех перечисленных выше формах и разного уровня сложности. Такой формат КИМ позволяет объективно определить качество освоения обучающимися основных элементов содержания дисциплины и уровень сформированности компетенций.

Примеры типовых заданий для проведения
промежуточной аттестации обучающихся

Задание в закрытой форме:

При разработке регламента оценки защищенности ИС необходимо учитывать _____.

.

Задание в открытой форме:

Из перечисленного: 1) идентификация и аутентификация; 2) регистрация и учет; 3) непрерывность защиты; 4) политика безопасности -- согласно «Оранжевой книге» требованиями в области аудита являются

a. 3, 4
b. 1, 2
c. 2, 4
d. 1, 3

Задание на установление правильной последовательности,

Расположите этапы в порядке их выполнения при разработки модели угроз

Оценка возможностей нарушителя, выбор угроз из банка угроз ФСТЭК, создание уточнённой модели нарушителя, формирование перечня актуальных угроз .

Задание на установление соответствия:

Для информационной системы в составе нескольких защищаемых помещений с числом субъектов ПДн более 100 установите соответствие:

a. Угроза скрытной регистрации вредоносной программой учетных записей администраторов внешний нарушитель с потенциалом не ниже усиленного базового.

b. Угроза хищения аутентификационной информации из временных файлов cookie внешний нарушитель с потенциалом не ниже усиленного базового;

c. Угроза изменения системных и глобальных переменных внутренний нарушитель с потенциалом не ниже усиленного базового;

1 Опасность угрозы низкая

2 Опасность угрозы средняя

3 Опасность угрозы высокая

Компетентностно-ориентированная задача:

Для некоторой системы характерно наличие беспроводного канала связи (Wi-fi), соединяющей компьютеры, находящиеся в аттестованных помещениях. Распространение сети проходит через неаттестованное помещение. Предложите перечень мероприятий, направленных на сохранение класса защиты данной информационной системы.

7.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, регулируются следующими нормативными актами университета:

− положение П 02.016 «О балльно-рейтинговой системе оценивания результатов обучения по дисциплинам (модулям) и практикам при освоении обучающимися образовательных программ»;

− методические указания, используемые в образовательном процессе, указанные в списке литературы.

Для *текущего контроля успеваемости* по дисциплине в рамках действующей в университете балльно-рейтинговой системы применяется следующий порядок начисления баллов:

Таблица 7.4 – Порядок начисления баллов в рамках БРС

Форма контроля	Минимальный балл		Максимальный балл	
	балл	примечание	балл	примечание
Выполнение лабораторной работы Разработка регламента защищенности к проектируемым информационным системам	4	Выполнил, но «не защитил»	5	Выполнил и «защитил»
Контроль защищенности информационных систем	4	Выполнил, но «не защитил»	5	Выполнил и «защитил»
Выполнение лабораторной работы Анализ типовых уязвимостей распределенных информационных систем	4	Выполнил, но «не защитил»	6	Выполнил и «защитил»
Выполнение лабораторной работы Сетевые и узловые системы анализа защищенности;	6	Выполнил, но «не защитил»	8	Выполнил и «защитил»
Выполнение лабораторной работы Сетевые и узловые системы обнаружения и предотвращений вторжений.	6	Выполнил, но «не защитил»	8	Выполнил и «защитил»
СРС	0		6	
Компетентностные задачи	0		6	
ИТОГО	24		48	
Посещаемость	0		16	
Зачет	0		36	
ИТОГО	24		100	

Для промежуточной аттестации обучающихся, проводимой в виде тестирования, используется следующая методика оценивания знаний, умений, навыков и (или) опыта деятельности. В каждом варианте КИМ –16 заданий (15 вопросов и одна задача).

Каждый верный ответ оценивается следующим образом:

- задание в закрытой форме –2 балла,
- задание в открытой форме – 2 балла,
- задание на установление правильной последовательности – 2 балла,
- задание на установление соответствия – 2 балла,
- решение компетентностно-ориентированной задачи – 6 баллов.

Максимальное количество баллов за тестирование –36 баллов.

8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Основная литература

1) Технологии обеспечения безопасности информационных систем : учебное пособие : [16+] / А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов и др. – Москва ; Берлин : Директ-Медиа, 2021. – 210 с. : ил., схем., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=598988 (дата обращения: 07.09.2021). – Библиогр.: с. 196-205. – ISBN 978-5-4499-1671-6. – DOI 10.23681/598988. – Текст : электронный.

2) Основы администрирования информационных систем : учебное пособие / Д. О. Бобынцев, А. Л. Марухленко, Л. О. Марухленко [и др.]. - Москва ; Берлин : Директ-Медиа, 2021. - 201 с. : ил., табл. - URL: http://biblioclub.ru/index.php?page=book&id=598955 (дата обращения: 28.08.2021) . - Режим доступа: по подписке. - ISBN 978-5-4499-1674-7. - Текст : электронный.

Дополнительная литература

3) Кобылянский, В. Г. Операционные системы, среды и оболочки : учебное пособие / В. Г. Кобылянский ; Новосибирский государственный технический университет. - Новосибирск : Новосибирский государственный технический университет, 2018. - 80 с.: ил., табл. - URL: http://biblioclub.ru/index.php?page=book&id=576354 (дата обращения: 26.08.2021) . - Режим доступа: по подписке. - Текст: электронный

Перечень методических указаний

1) Виды информации и основные методы ее защиты : методические указания по выполнению лабораторной работы по дисциплине «Основы информационной безопасности» для студентов специальности 10.05.02 / Юго-Зап. гос. ун-т ; сост. А. Л. Марухленко. - Курск : ЮЗГУ, 2017. - 8 с. - Текст : электронный.

2) Моделирование доступа к разделяемому ресурсу : методические указания по выполнению практической работы по дисциплине «Безопасность операционных систем» для студентов укрупненной группы специальностей 10.00.00 / Юго-Зап. гос. ун-т ; сост. М. О. Таныгин. - Курск : ЮЗГУ, 2017. - 16 с. : ил., табл. - Библиогр.: с. 16. - Текст : электронный.

3) Виды угроз информационной безопасности Российской Федерации : методические указания по выполнению лабораторной работы по дисциплине «Основы информационной безопасности» для студентов специальности 10.05.02 / Юго-Зап. гос. ун-т ; сост. А. Л. Марухленко. - Курск : ЮЗГУ, 2017. - 7 с. - Текст : электронный.

4) Источники угроз информационной безопасности Российской Федерации : методические указания / Юго-Зап. гос. ун-т ; сост. А. Л. Марухленко. - Курск : ЮЗГУ, 2017. - 8 с. - Текст : электронный.

5) Исследование атаки переполнения буфера как примера безопасности нарушения конфиденциальности, целостности и доступности информации : методические указания по выполнению лабораторной работы / Юго-Зап. гос. ун-т ; сост. А. Л. Марухленко. - Курск : ЮЗГУ, 2017. - 10 с. - Текст : электронный.

6) Причины, виды, каналы утечки и искажения информации : методические указания по выполнению лабораторной работы / Юго-Зап. гос. ун-т ; сост. А. Л. Марухленко. - Курск : ЮЗГУ, 2017. - 11 с. - Текст : электронный.

7) Сетевое сканирование: методические указания по выполнению лабораторной работы / Юго-Зап. гос. ун-т ; сост. А. Л. Марухленко. - Курск : ЮЗГУ, 2017. - 7 с. - Текст : электронный.

8) Анализ трафика и сбор критичной информации программами пассивного анализа: методические указания по выполнению лабораторной работы / Юго-Зап. гос. ун-т ; сост. А. Л. Марухленко. - Курск : ЮЗГУ, 2017. - 6 с. - Текст : электронный.

9) Аудит комплексной защиты информации предприятия : методические указания по выполнению лабораторной работы / Юго-Зап. гос. ун-т ; сост. А. Л. Марухленко. - Курск : ЮЗГУ, 2017. - 8 с. - Текст : электронный.

9. Перечень ресурсов информационно-телекоммуникационной сети Интернет

1) Облачный сервис математических вычислений SMath Studio in the Cloud [официальный сайт]. Режим доступа: https://ru.smath.com/cloud/
2) Электронно-библиотечная система «Университетская библиотека онлайн» Режим доступа: http://biblioclub.ru
3) Научно-информационный портал ВИНИТИ РАН [официальный сайт]. Режим доступа: http://www.consultant.ru/
4) Общероссийский портал Math-Net.Ru [официальный сайт]. Режим доступа: http://www.mathnet.ru/
5) База данных "Патенты России"

10. Методические указания для обучающихся по освоению дисциплины

Основными видами аудиторной работы студента при изучении дисциплины являются лекции и лабораторные занятия. Студент не имеет права пропускать занятия без уважительных причин.

На лекциях излагаются и разъясняются основные понятия темы,

связанные с ней теоретические и практические проблемы, даются рекомендации для самостоятельной работы. В ходе лекции студент должен внимательно слушать и конспектировать материал.

Изучение наиболее важных тем или разделов дисциплины завершают лабораторные и практические занятия, которые обеспечивают: контроль подготовленности студента; закрепление учебного материала; приобретение опыта устных публичных выступлений, ведения дискуссии, в том числе аргументации и защиты выдвигаемых положений и тезисов.

Лабораторному занятию предшествует самостоятельная работа студента, связанная с освоением материала, полученного на лекциях, и материалов, изложенных в учебниках и учебных пособиях, а также литературе, рекомендованной преподавателем.

Качество учебной работы студентов преподаватель оценивает по результатам тестирования, собеседования, защиты отчетов по лабораторным и практическим работам.

Преподаватель уже на первых занятиях объясняет студентам, какие формы обучения следует использовать при самостоятельном изучении дисциплины: конспектирование учебной литературы и лекции, составление словарей понятий и терминов и т. п.

В процессе обучения преподаватели используют активные формы работы со студентами: чтение лекций, привлечение студентов к творческому процессу на лекциях, промежуточный контроль путем отработки студентами пропущенных лекции, участие в групповых и индивидуальных консультациях (собеседовании). Эти формы способствуют выработке у студентов умения работать с учебником и литературой. Изучение литературы и справочной документации составляет значительную часть самостоятельной работы студента. Это большой труд, требующий усилий и желания студента. В самом начале работы над книгой важно определить цель и направление этой работы. Прочитанное следует закрепить в памяти. Одним из приемов закрепление освоенного материала является конспектирование, без которого немыслима серьезная работа над литературой. Систематическое конспектирование помогает научиться правильно, кратко и четко излагать своими словами прочитанный материал.

Самостоятельную работу следует начинать с первых занятий. От занятия к занятию нужно регулярно прочитывать конспект лекций, знакомиться с соответствующими разделами учебника, читать и конспектировать литературу по каждой теме дисциплины. Самостоятельная работа дает студентам возможность равномерно распределить нагрузку, способствует более глубокому и качественному усвоению учебного материала. В случае необходимости студенты обращаются за консультацией к преподавателю по вопросам дисциплины с целью усвоения и закрепления компетенций.

Основная цель самостоятельной работы студента при изучении дисциплины - закрепить теоретические знания, полученные в процессе

лекционных занятий, а также сформировать практические навыки самостоятельного анализа особенностей дисциплины.

11. **Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)**

Microsoft Office 2016.Лицензионный договор №S0000000722 от 21.12.2015 г. с ООО «АйТи46», лицензионный договор №K0000000117 от 21.12.2015 г. с ООО «СМСКанал», Kaspersky Endpoint Security Russian Edition, лицензия 156A-140624-192234,Windows 7, договор IT000012385, открытая среда разработки программного обеспечения Lazarus (Свободное ПО http://www.lazarus.freepascal.org/)

12. **Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине**

Учебная аудитория для проведения занятий лекционного типа и лаборатории кафедры информационной безопасности, оснащенные учебной мебелью: столы, стулья для обучающихся; стол, стул для преподавателя; доска. Компьютеры (10 шт) CPU AMD-Phenom, ОЗУ 16 GB, HDD 2 Tb, монитор Aok 21”. Проекционный экран на штативе; Мультимедиацентр: ноут- букASUSX50VLPMD-T2330/14"/1024Mb/160Gb/сумка/ проектор inFocusIN24+

13. **Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья**

При обучении лиц с ограниченными возможностями здоровья учитываются их индивидуальные психофизические особенности. Обучение инвалидов осуществляется также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).

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

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

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

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