Аннотация к рабочей программе дисциплины «Оценка защищённости информационных систем»

Цель преподавания дисциплины

Цель дисциплины – обучение 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 для решения задач профессиональной деятельности научно-исследовательского и контрольно-аналитического типов.

Задачи изучения дисциплины

Задачами дисциплины являются:

1. Формирование профессиональных навыков для проведения оценки состояния защищенности информационных систем (ИБ) в ИС.
2. Ознакомление с уязвимостями, угрозами ИБ и видами деструктивного воздействия, характерными для современных ИС, а также принципами построения защищенных ИС.
3. Изучение подходов и методов обеспечения ИБ ИС, а также анализа рисков ИБ.
4. Обеспечить совместно с другими дисциплинами семестра теоретическую подготовку обучающихся к производственной эксплуатационной практике на предприятии-заказчике.

Индикаторы компетенций, формируемые в результате освоения дисциплины

ПК-3.2 Формулирует целевые критерии для оценивания эффективности исследуемых систем

ПК-3.3 Определяет в результате натурных или математических экспериментов характеристики защищённых информационных систем

ПК-6.1 Формирует перечень угроз для защищаемой информационной системы

ПК-6.2 Формирует критерии оценки каждого вида угроз в защищаемой системе

ПК-6.3 Формирует перечень нарушителей информационной безопасности в защищаемой системе

ПК-7.1 Подбирает инструментальные средства тестирования систем защиты информации

ПК-7.2 Разрабатывает систему мероприятий по оценке уровня защищённости информационной системы

ПК-7.3 Определяет уязвимости информационной системы

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 ФиПИ
_____ Таныгин М.О.
(подпись, инициалы, фамилия)
«30» мая 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Оценка защищённости информационных систем
(наименование дисциплины)

ОПОП ВО 10.04.01 Информационная безопасность,
(шифр и наименование направления подготовки)

направленность (профиль) «Защищенные информационные системы»
(наименование направленности (профиля))

форма обучения очная

ОПОП ВО реализуется по модели дуального обучения

Курск – 2023

Рабочая программа дисциплины составлена:

– в соответствии с ФГОС ВО – магистратура по направлению подготовки 10.04.01 Информационная безопасность, утвержденным приказом Минобрнауки России от 26.11.2020 г. № 1455;

– на основании учебного плана ОПОП ВО 10.04.01 Информационная безопасность, направленность (профиль) «Защищенные информационные системы», одобренного Ученым советом университета (протокол №12 от 29.05.2023).

– с учетом заказа-требования от 28.04.2023 на результаты освоения ОПОП ВО – программы магистратуры 10.04.01 Информационная безопасность, направленность (профиль) «Защищенные информационные системы», реализуемой по модели дуального обучения в ФГБОУ ВО «Юго-Западный государственный университет», от ООО ЦСБ «ЩИТ-ИНФОРМ»
(наименование предприятия (организации))
(приложение к общей характеристике ОПОП ВО).

Рабочая программа дисциплины обсуждена и рекомендована к реализации в образовательном процессе для дуального обучения студентов по ОПОП ВО 10.04.01 Информационная безопасность, направленность (профиль) «Защищенные информационные системы» на совместном заседании кафедры информационной безопасности
(наименование кафедры)
с представителями ООО ЦСБ «ЩИТ-ИНФОРМ»
(наименование предприятия (организации))
(протокол № 8 от 29.05.2023).

Зав. кафедрой _____ А.Л. Марухленко

Разработчик программы
к.т.н., доцент _____ А.Л. Марухленко

Директор научной библиотеки _____ В.Г. Макаровская

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО дуального обучения 10.04.01 Информационная безопасность, направленность (профиль) «Защищенные информационные системы», одобренного Ученым советом университета (протокол № __ от __. __. 20__), на совместном заседании кафедры информационной безопасности
(наименование кафедры)
с представителями ООО ЦСБ «ЩИТ-ИНФОРМ»
(наименование предприятия (организации))
(протокол № __ от __. __. 20__).

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 дисциплины

Цель дисциплины – обучение 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 для решения задач профессиональной деятельности научно-исследовательского и контрольно-аналитического типов.

1.2 Задачи дисциплины

Задачами дисциплины являются:

1. Формирование профессиональных навыков для проведения оценки состояния защищенности информационных систем (ИБ) в ИС.
2. Ознакомление с уязвимостями, угрозами ИБ и видами деструктивного воздействия, характерными для современных ИС, а также принципами построения защищенных ИС.
3. Изучение подходов и методов обеспечения ИБ ИС, а также анализа рисков ИБ.
4. Обеспечить совместно с другими дисциплинами семестра теоретическую подготовку обучающихся к производственной эксплуатационной практике на предприятии-заказчике.

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-3.2 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 эф-

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*		
			фективности 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-3.3 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; - навыками разработки технического облика средств обработки и передачи данных в информационных системах; - навыками разработки методик теоретических и экспериментальных исследований защищённости информационных систем.
ПК-6	Способен управлять рисками информационной безопасности	ПК-6.1 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

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*		
			ИС; - навыками проведения анализа рисков.
		ПК-6.2 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-6.3 Формирует перечень нарушителей информационной безопасности в защищаемой системе	***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-7	Способен контролировать защищённость информационных систем	ПК-7.1 Подбирает инструментальные средства тестирования систем защиты информации	***Знать:*** - организационные основы защиты информации от несанкционированного доступа и утечки по техническим каналам на объектах информатизации; - нормативные правовые акты в области защиты информации; ***Уметь:*** - контролировать функционирование технических средств защиты информации; - применять действующую нормативную базу в области обеспечения безопасности информации; ***Владеть (****или* ***Иметь опыт деятельности):*** подбора инструментальных средств тестирования систем защиты информации в автоматизированных системах.

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-7.2 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-7.3 Определяет уязвимости информационной системы	***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 часть, формируемую участниками образовательных отношений, блока 1 «Дисциплины (модули)» основной профессиональной образовательной программы – программы магистратуры 10.04.01 Информационная безопасность, направленность (профиль) «Защищённые информационные системы», реализуемой по модели дуального обучения.

Дисциплина изучается на 2 курсе в 3 семестре.

Дисциплина имеет практико-ориентированный характер и изучается до прохождения обучающимися производственной эксплуатационной практики, завершающей данный семестр.

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 трудоемкость (объем) дисциплины составляет 3 зачетные единицы (з.е.), 108 академических 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
в том числе:	
лекции	18
лабораторные занятия	36, из них практическая подготовка обучающихся – 4.
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 предусмотрен

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 постро-	Регулирование ответственности нарушений информационной без-

	ения системы информационной безопасности	опасности. Программа информационной безопасности. Контроль деятельности в области безопасности на примере ООО ЦСБ «ЩИТ-ИНФОРМ». Модели представления информационной защиты на примере ООО ЦСБ «ЩИТ-ИНФОРМ». Формирование требований к системе информационной безопасности. Этапы обеспечения информационной безопасности на примере ООО ЦСБ «ЩИТ-ИНФОРМ».
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 на примере ООО ЦСБ «ЩИТ-ИНФОРМ». 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 ООО ЦСБ «ЩИТ-ИНФОРМ».
5.	Внутренний аудит ИБ	Цели и задачи, организационные принципы, принципы обеспечения эффективности. Подразделение внутреннего аудита, контролирующее вопросы ОИБ в организации ООО ЦСБ «ЩИТ-ИНФОРМ».
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 на примере ООО ЦСБ «ЩИТ-ИНФОРМ».
8.	Системы обнаружения и предотвращения вторжений	Виды систем, решаемые задачи, использование в целях оценки защищенности ИТ на примере ООО ЦСБ «ЩИТ-ИНФОРМ».

Таблица 4.1.2 – Содержание дисциплины и его методическое обеспечение

№ п/п	Раздел (тема) дисциплины	Виды деятельности			Учебно-методические материалы	Формы текущего контроля успеваемости[1] *(по неделям семестра)*	Компетенции
		лек., час	№ лаб.	№ пр.			
1	2	3	4	5	6	7	8
1	Нормативная база оценки защищенности ИТ	2			У-1-5 МУ-1	УО 1	ПК-3 ПК-6 ПК-7
2	Основные аспекты построения системы информационной безопасности	2	1		У-1-5 МУ-1	УО, ЗЛР 2-3	ПК-3 ПК-6 ПК-7
3	Базовые вопросы проверки защищенности ИТ	4	2		У-1-5 МУ-1	УО, ЗЛР, ПЗ 4-5	ПК-3 ПК-6 ПК-7
4	Виды проверок	2	3		У-1-5 МУ-1	УО, ЗЛР 6-7	ПК-3 ПК-6 ПК-7
5	Внутренний аудит ИБ	2			У-1-5 МУ-1	УО 8-9	ПК-3 ПК-6 ПК-7
6	Внешний аудит ИБ	2			У-1-5 МУ-1	УО 9-10	ПК-3

7	Системы анализа защищенности	2	4		У-1-5 МУ-1	УО, ЗЛР 11-12	ПК-6 ПК-7
8	Системы обнаружения и предотвращения вторжений	2	5		У-1-5 МУ-1	13-14	ПК-3 ПК-6 ПК-7

УО – устный опрос, ЗЛР – защита лабораторной работы, ПЗ – решение производственной задачи

4.2 Лабораторные работы и (или) практические занятия

4.2.1 Лабораторные работы

Таблица 4.2.1 – Лабораторные работы

№	Наименование лабораторной работы	Объем, час.
1	2	3
1	Разработка регламента защищенности к проектируемым информационным системам	4
2	Контроль защищенности информационных систем	6, из них практическая подготовка обучающихся – 4
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, из них практическая подготовка обучающихся – 4

4.3 Самостоятельная работа студентов (СРС)

Таблица 4.3 – Самостоятельная работа студентов

№	Наименование раздела учебной дисциплины	Срок	Время на выполнение СРС, час.
1.	Нормативная база оценки защищенности ИТ	1 неделя	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	6-7 недели	6
5.	Внутренний аудит ИБ	8-9 недели	6
6.	Внешний аудит ИБ	9-10 недели	5.9

7.	Системы анализа защищенности	11-12 недели	10
8.	Системы обнаружения и предотвращения вторжений	13-14 недели	10
Итого			53.9

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

При самостоятельном изучении отдельных тем и вопросов дисциплины студенты могут пользоваться учебно-наглядными пособиями, учебным оборудованием и методическими разработками кафедры *информационной безопасности* в рабочее время, установленное Правилами внутреннего распорядка работников университета.

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

библиотекой университета:

- библиотечный фонд укомплектован учебной, методической, научной, периодической, справочной и художественной литературой в соответствии с учебным планом и 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:

– методических рекомендаций, пособий по организации самостоятельной работы студентов;

– методических указаний к выполнению лабораторных работ и т.д.

типографией университета:

– посредством оказания помощи авторам в подготовке и издании научной, учебной и методической литературы;

– посредством удовлетворения потребности в тиражировании научной, учебной и методической литературы.

6 Образовательные технологии. Практическая подготовка обучающихся

Практическая подготовка обучающихся при реализации дисциплины осуществляется путем проведения лабораторных занятий, предусматривающих участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью и направленных на

формирование, закрепление, развитие практических навыков и компетенций по направленности (профилю) программы магистратуры.

Практическая подготовка обучающихся при реализации дисциплины организуется в модельных условиях.

Практическая подготовка обучающихся проводится в соответствии с положением П 02.181.

7 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

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

Таблица 7.1 – Этапы формирования компетенций

Код и наименование компетенции	Этапы формирования компетенций и дисциплины (модули), практики, при изучении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
ПК-3 Способен проводить теоретические и экспериментальные исследования защищённости информационных систем	Прикладные математические задачи информационной безопасности	Моделирование технических объектов и систем управления Производственная практика по получению умений и навыков управленческой деятельности	Оценка защищённости информационных систем Теоретические основы компьютерной безопасности Управление разработкой систем безопасности Производственная преддипломная практика
ПК-6 Способен управлять рисками информационной безопасности	Информационно-аналитические системы безопасности Экспертные системы комплексной оценки безопасности информационных и телекоммуникационных систем Теоретические основы компьютерной безопасности Оценка защищённости информационных систем Производственная эксплуатационная практика Производственная преддипломная практика		
ПК-7 Способен контролировать защищённость информационных систем	Методы и средства защиты информации в системах электронного документооборота Технологии обеспечения информационной безопасности объектов Оценка защищённости информационных систем Производственная эксплуатационная практика Производственная преддипломная практика		

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 *(наименование этапа по таблице 6.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за практикой)*	Критерии и шкала оценивания компетенций			
		Недостаточный уровень («неудовл.»)	Пороговый уровень («удовл.»)	Продвинутый уровень («хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5	6
ПК-3/ завершающий	ПК-3.1 Разрабатывает формальные модели обработки и передачи данных в информационных системах ПК-3.2 Формулирует целевые критерии для оценивания эффективности исследуемых систем ПК-3.3 Определяет в результате натурных или математических экс-	**Знать:** демонстрирует менее 60% знаний, указанных в таблице 1.3 для ПК-3. Обучающийся нуждается в постоянных подсказках; допускает грубые ошибки, которые не может исправить самостоятельно.	**Знать:** демонстрирует 60-74% знаний, указанных в таблице 1.3 для ПК-3. Знания обучающегося имеют поверхностный характер, имеют место неточности и ошибки.	**Знать:** демонстрирует 75-89% знаний, указанных в таблице 1.3 для ПК-3. Обучающийся имеет хорошие, но не исчерпывающие знания; допускает неточности.	**Знать:** демонстрирует 90-100% знаний, указанных в таблице 1.3 для ПК-3. Знания обучающегося являются прочными и глубокими, имеют системный характер. Обучающийся свободно оперирует знаниями.
		Уметь: демонстрирует менее 60% умений, установленных в таблице 1.3 для ПК-3.	**Уметь:** в целом сформированные, но вызывающие затруднения при самостоятельном применении умения, указанные в таблице 1.3 для ПК-3.	**Уметь:** сформированные и самостоятельно применяемые умения, указанные в таблице 1.3 для ПК-3.	**Уметь:** хорошо развитые, уверенно и успешно применяемые умения, указанные в таблице 1.3 для ПК-3.

	периментов характеристики защищённых информационных систем	***Владеть (или Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для ПК-3, не развиты.	***Владеть (или Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для ПК-3, развиты на элементарном уровне.	***Владеть (или Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для ПК-3, хорошо развиты.	***Владеть (или Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для ПК-3, доведены до автоматизма.
ПК-6/ завершающий	ПК-6.1 Формирует перечень угроз для защищаемой информационной системы ПК-6.2 Формирует критерии оценки каждого вида угроз в защищаемой системе ПК-6.3 Формирует перечень нарушителей информационной безопасности в защищаемой системе	**Знать:** демонстрирует менее 60% знаний, указанных в таблице 1.3 для ПК-6. Обучающийся нуждается в постоянных подсказках; допускает грубые ошибки, которые не может исправить самостоятельно.	**Знать:** демонстрирует 60-74% знаний, указанных в таблице 1.3 для ПК-6. Знания обучающегося имеют поверхностный характер, имеют место неточности и ошибки.	**Знать:** демонстрирует 75-89% знаний, указанных в таблице 1.3 для ПК-6. Обучающийся имеет хорошие, но не исчерпывающие знания; допускает неточности.	**Знать:** демонстрирует 90-100% знаний, указанных в таблице 1.3 для ПК-6. Знания обучающегося являются прочными и глубокими, имеют системный характер. Обучающийся свободно оперирует знаниями.
		Уметь: демонстрирует менее 60% умений, установленных в таблице 1.3 для ПК-6.	**Уметь:** в целом сформированные, но вызывающие затруднения при самостоятельном применении умения, указанные в таблице 1.3 для ПК-6.	**Уметь:** сформированные и самостоятельно применяемые умения, указанные в таблице 1.3 для ПК-6.	**Уметь:** хорошо развитые, уверенно и успешно применяемые умения, указанные в таблице 1.3 для ПК-6.

		Владеть (*или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для ПК-6, не развиты.	***Владеть (****или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для ПК-6, развиты на элементарном уровне.	***Владеть (****или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для ПК-6, хорошо развиты.	***Владеть (****или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для ПК-6, доведены до автоматизма.
ПК-7/ завершающий	ПК-7.1 Подбирает инструментальные средства тестирования систем защиты информации ПК-7.2 Разрабатывает систему мероприятий по оценке уровня защищённости информационной системы ПК-7.3 Определяет уязвимости информационной системы	**Знать:** демонстрирует менее 60% знаний, указанных в таблице 1.3 для ПК-7. Обучающийся нуждается в постоянных подсказках; допускает грубые ошибки, которые не может исправить самостоятельно.	**Знать:** демонстрирует 60-74% знаний, указанных в таблице 1.3 для ПК-7. Знания обучающегося имеют поверхностный характер, имеют место неточности и ошибки.	**Знать:** демонстрирует 75-89% знаний, указанных в таблице 1.3 для ПК-7. Обучающийся имеет хорошие, но не исчерпывающие знания; допускает неточности.	**Знать:** демонстрирует 90-100% знаний, указанных в таблице 1.3 для ПК-7. Знания обучающегося являются прочными и глубокими, имеют системный характер. Обучающийся свободно оперирует знаниями.
		Уметь: демонстрирует менее 60% умений, установленных в таблице 1.3 для ПК-7.	**Уметь:** в целом сформированные, но вызывающие затруднения при самостоятельном применении умения, указанные в таблице 1.3 для ПК-7.	**Уметь:** сформированные и самостоятельно применяемые умения, указанные в таблице 1.3 для ПК-7.	**Уметь:** хорошо развитые, уверенно и успешно применяемые умения, указанные в таблице 1.3 для ПК-7.

		Владеть (*или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для ПК-7, не развиты.	***Владеть (****или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для ПК-7, развиты на элементарном уровне.	***Владеть (****или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для ПК-7, хорошо развиты.	***Владеть (****или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для ПК-7, доведены до автоматизма.

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/п	Раздел (тема) дисциплины	Код контролируемой компетенции (или ее части)	Технология формирования	Оценочные средства		Описание шкал оценивания
				наименование	№ заданий	
1	2	3	4	5	6	7
1.	Нормативная база оценки защищенности ИТ	ПК-3 ПК-6 ПК-7	Лекция, СРС	Устный вопрос	1-10	Согласно табл. 7.2
2.	Основные аспекты построения системы информационной безопасности	ПК-3 ПК-6 ПК-7	Лекция, СРС, лабораторная работа	Устный вопрос КВЗЛР	1-10 1-10	Согласно табл. 7.2
3.	Базовые вопросы проверки защищенности ИТ	ПК-3 ПК-6 ПК-7	Лекция, СРС, лабораторная работа	Устный вопрос КВЗЛР Производственные задачи	1-10 1-10 1-10	Согласно табл. 7.2
4.	Виды проверок	ПК-3 ПК-6 ПК-7	Лекция, СРС, лабораторная работа	Устный вопрос КВЗЛР	1-10 1-10	Согласно табл. 7.2
5.	Внутренний аудит ИБ	ПК-3 ПК-6	Лекция, СРС	Устный вопрос	1-10	Согласно табл. 7.2

		ПК-7				
6.	Внешний аудит ИБ	ПК-3 ПК-6 ПК-7	Лекция, СРС,	Устный вопрос	1-10	Согласно табл. 7.2
7.	Системы анализа защищенности	ПК-3 ПК-6 ПК-7	Лекция, СРС, лабораторная работа	Устный вопрос КВЗЛР	1-10 1-10	Согласно табл. 7.2
8.	Системы обнаружения и предотвращения вторжений	ПК-3 ПК-6 ПК-7	Лекция, СРС, лабораторная работа	Устный вопрос КВЗЛР	1-10 1-10	Согласно табл. 7.2

КВЗЛР – контрольные вопросы для защиты лабораторных работ

7.3.1 Примеры типовых контрольных заданий для проведения текущего контроля успеваемости

Вопросы для устного опроса по разделу (теме) № 1 ««Нормативная база оценки защищенности ИТ»

1. Существующие стандарты и методологии проверки и оценки защищенности ИТ и СУИБ.
2. История развития. ISO/IEC 27004:2009 и ГОСТ Р ИСО/МЭК 27004-2011 – оценка функционирования СУИБ
3. ISO/IEC 27006:2011 и ГОСТ Р ИСО/МЭК 27006-2008 – требования к органам, осуществляющим аудит и сертификацию СУИБ.
4. ISO/IEC 27007:2011 и ISO/IEC 27008:2011 – руководства по аудиту СУИБ и средств управления ИБ, реализованных в СУИБ.
5. Существующие стандарты и методологии проверки и оценки защищенности ИТ и СУИБ: их отличия, сильные и слабые стороны.

Контрольные вопросы для защиты лабораторной работы № 2 «Контроль защищенности информационных систем»

1. Система обнаружения компьютерных атак, дайте определение.
2. Виды программ технического обслуживания (стандартные программы).
3. Значение технического обслуживания.
4. Причины отказа в гарантийном обслуживании.
5. Программы технического обслуживания.

Производственная задача

Необходимо провести оценку защищенности информационной системы компании перед ее внедрением. Разработайте план оценки защищенности информационной системы, определите основные этапы и методы оценки, а также критерии успешной оценки.

Полностью оценочные материалы и оценочные средства для проведения текущего контроля успеваемости представлены в УММ по дисциплине.

7.3.2 Типовые задания для проведения промежуточной аттестации обучающихся

Промежуточная аттестация по дисциплине проводится в форме зачета. На промежуточной аттестации по дисциплине применяется механизм квалификационного экзамена. Зачет имеет структуру квалификационного экзамена и состоит из 2 частей:

– теоретической (компьютерное тестирование);

– практической (решение компетентностно-ориентированной задачи).

На теоретической части зачета (тестировании) проверяются знания и частично – умения и навыки обучающихся. 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.

На практической части зачета проверяются результаты практической подготовки: *компетенции, включая умения, навыки (или опыт деятельности)*). Результаты практической подготовки *(компетенции, включая умения, навыки (или опыт деятельности))* проверяются с помощью компетентностно-ориентированных задач (ситуационных, производственных, кейс-задач или кейсов) 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.

а) Примеры типовых заданий для теоретической части зачета (тестирования)

Задание в закрытой 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 в открытой форме:

При разработке регламента оценки защищенности ИС необходимо учитывать _____.

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

б) Примеры типовых заданий для практической части зачета

Компетентностно-ориентированная задача:

Разработайте программу тестирования безопасности информационной системы организации, проведите тестирование и анализ результатов, определите уязвимые места и способы их защиты, выберите меры для повышения безопасности и оцените эффективность этих мер.

Полностью оценочные материалы и оценочные средства для проведения промежуточной аттестации обучающихся представлены в УММ по дисциплине.

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»;

– положение П 02.207 «Проектирование и реализация основных профессиональных программ высшего образования – программ магистратуры по модели дуального обучения»;

– 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
1	2	3	4	5
Лабораторная работа № 1	2	Выполнил, но не ответил или неполно ответил на какой-либо вопрос по лабораторной работе	4	Выполнил, правильно и полно ответил на все вопросы по лабораторной работе
Лабораторная работа № 2	2	Выполнил, но не ответил или неполно ответил на какой-либо вопрос	4	Выполнил, правильно и полно ответил на все вопросы по лаборатор-

Форма контроля	Минимальный балл		Максимальный балл	
	балл	примечание	балл	примечание
1	2	3	4	5
		по лабораторной работе		ной работе
Лабораторная работа № 3	2	Выполнил, но не ответил или неполно ответил на какой-либо вопрос по лабораторной работе	4	Выполнил, правильно и полно ответил на все вопросы по лабораторной работе
Лабораторная работа № 4	2	Выполнил, но не ответил или неполно ответил на какой-либо вопрос по лабораторной работе	4	Выполнил, правильно и полно ответил на все вопросы по лабораторной работе
Лабораторная работа № 5	2	Выполнил, но не ответил или неполно ответил на какой-либо вопрос по лабораторной работе	4	Выполнил, правильно и полно ответил на все вопросы по лабораторной работе
Устный опрос	10	Ответил или неполно ответил на какой-либо вопрос по лабораторной работе	20	Правильно и полно ответил на все вопросы по лабораторной работе
Производственная задача	4	Выполнил, но не ответил или неполно ответил на какой-либо вопрос по лабораторной работе	8	Выполнил, правильно и полно ответил на все вопросы по лабораторной работе
Итого	24		48	
Посещаемость	0		16	
Зачет	0		36	
Итого	24		100	

Для проведения промежуточной аттестации обучающихся (теоретической части и практической части) используется следующая методика оценивания знаний, умений, навыков и (или) опыта деятельности. В каждом варианте КИМ –16 заданий (15 вопросов для тестирования и одна компетентностно-ориентированная 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 по промежуточной аттестации – 36.

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

8.1 Основная литература

1) Мартынов, А. П. Информационная безопасность и защита информации : учебное пособие / А. П. Мартынов, И. А. Мартынова, А. А. Русаков. — Москва : Ай Пи Ар Медиа, 2023. — 122 с. — ISBN 978-5-4497-2247-8. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/131797.html (дата обращения: 09.10.2023). — Режим доступа: для авторизир. пользователей. - DOI: https://doi.org/10.23682/131797

2) Мирошников, А. И. Основы информационной безопасности и защита информации : учебное пособие / А. И. Мирошников, А. С. Сысоев. — Липецк : Липецкий государственный технический университет, ЭБС АСВ, 2022. — 107 с. — ISBN 978-5-00175-160-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/128718.html (дата обращения: 09.10.2023). — Режим доступа: для авторизир. пользователей

8.2 Дополнительная литература

3) Абденов, А. Ж. Методика оценки риска для информационных систем на основе экспертных оценок : учебное пособие / А. Ж. Абденов, С. А. Белкин, Р. Н. Заркумова-Райхель. — Новосибирск : Новосибирский государственный технический университет, 2014. — 71 с. — ISBN 978-5-7782-2588-6. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/44957.html (дата обращения: 09.10.2023). — Режим доступа: для авторизир. пользователей

4) Бескид, П. П. Проектирование защищенных информационных систем. Часть 1. Конструкторское проектирование. Защита от физических полей : учебное пособие / П. П. Бескид, В. Ю. Суходольский, Ю. М. Шапаренко. — Санкт-Петербург : Российский государственный гидрометеорологический университет, 2008. — 196 с. — ISBN 978-5-86813-235-3. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/17960.html (дата обращения: 09.10.2023). — Режим доступа: для авторизир. пользователей

5) Международная информационная безопасность: теория и практика: в трех томах. Т.1 : учебник для студентов вузов / А. В. Крутских, А. В. Бирюков, С. М. Бойко [и др.] ; под редакцией А. В. Крутских. — 2-е изд. — Москва : Аспект Пресс, 2021. — 384 с. — ISBN 978-5-7567-1098-4 (т.1), 978-5-7567-1097-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/104464.html (дата обращения: 17.08.2023). — Режим доступа: для авторизир. пользователей

8.3 Перечень методических указаний

1) Моделирование доступа к разделяемому ресурсу : методические указания по выполнению лабораторных и практических работ для студентов укрупненной группы специальностей и направлений подготовки 10.00.00 / Юго-Зап. гос. ун-т ; сост.: М. О. Таныгин, А. В. Митрофанов. - Курск : ЮЗГУ, 2023. - 16 с. - Загл. с титул. экрана. - Б. ц. - Текст : электронный.

9 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. Федеральная служба безопасности [официальный сайт]. Режим доступа: http://www.fsb.ru/
2. Федеральная служба по техническому и экспортному контролю [официальный сайт]. Режим доступа: http://fstec.ru/
3. Электронно-библиотечная система «Лань» - http://e.lanbook.com/
4. Электронно-библиотечная система IQLib – http://www.iqlib.ru
5. Электронная библиотека «Единое окно доступа к образовательным ресурсам» - http://window.edu.ru/

10 Методические указания для обучающихся по освоению дисциплины

Основными видами аудиторной работы студента при изучении дисциплины являются лекции и лабораторные занятия.

На лекциях излагаются и разъясняются основные понятия и положения каждой новой темы; важные положения аргументируются и иллюстрируются примерами из практики; объясняется практическая значимость изучаемой темы; делаются выводы; даются рекомендации для самостоятельной работы по данной теме. На лекциях необходимо задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных вопросов. В ходе лекции студент должен конспектировать учебный материал. Конспектирование лекций – сложный вид работы, предполагающий интенсивную умственную деятельность студента. Конспект является полезным тогда, когда записано самое существенное и сделано это лично студентом в режиме реального времени в течение лекции. Не следует стремиться записать лекцию дословно. Целесообразно вначале понять основную мысль, излагаемую лектором, а затем кратко записать ее. Желательно заранее оставлять в тетради пробелы, куда позднее, при самостоятельной работе с конспектом, можно внести дополнительные записи. Конспект лекции лучше подразделять на пункты, соблюдая красную строку. Этому в большой степени будут способствовать вопросы плана лекции, который преподаватель дает в начале лекционного занятия. Следует обращать внимание на акценты, выводы, которые делает лектор, отмечая наиболее важные моменты в лекционном материале.

Необходимым является глубокое освоение содержания лекции и свободное владение им, в том числе использованной в ней терминологией. Работу с конспектом лекции целесообразно проводить непосредственно после ее прослушивания, что способствует лучшему усвоению материала, позволяет своевременно выявить и устранить «пробелы» в знаниях. Работа с конспектом лекции предполагает перечитывание конспекта, внесение в него, по необходимости, уточнений, дополнений, разъяснений и изменений. Некоторые вопросы выносятся за рамки лекций. Изучение вопросов, выносимых за рамки лекционных занятий, предполагает самостоятельное изучение студентами дополнительной литературы, указанной в п.8.2.

Изучение наиболее важных тем или разделов дисциплины продолжается на лабораторных занятиях, 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. Самостоятельная работа с учебниками, учебными пособиями, научной, справочной литературой, материалами периодических изданий и Интернета является наиболее эффективным методом получения дополнительных знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала. При работе с источниками и литературой необходимо:

– сопоставлять, сравнивать, классифицировать, группировать, систематизировать информацию в соответствии с определенной учебной задачей;

– обобщать полученную информацию, оценивать прочитанное;

– фиксировать основное содержание прочитанного текста; формулировать устно и письменно основную идею текста; составлять план, формулировать тезисы.

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 освоению учебного материала. В случае необходимости студенты обращаются за консультацией к преподавателю. Обязательным элементом самостоятельной работы по дисциплине является самоконтроль. Одной из важных задач обучения студентов способам и приемам самообразования является формирование у них умения самостоятельно контролировать и адекватно оценивать результаты своей учебной деятельности и на этой основе управлять процессом овладения знаниями. Овладение умениями самоконтроля приучает студентов к планированию учебного труда, способ-

ствует углублению их внимания, памяти и выступает как важный фактор развития познавательных способностей. Самоконтроль включает:

– оперативный анализ глубины и прочности собственных знаний и умений;

– критическую оценку результатов своей познавательной деятельности.

Самоконтроль учит ценить свое время, позволяет вовремя заметить и исправить свои ошибки. Формы самоконтроля могут быть следующими:

– устный пересказ текста лекции и сравнение его с содержанием конспекта лекции;

– составление плана, тезисов, формулировок ключевых положений текста по памяти;

– пересказ с опорой на иллюстрации, чертежи, схемы, таблицы, опорные положения.

Самоконтроль учебной деятельности позволяет студенту оценивать эффективность и рациональность применяемых методов и форм умственного труда, находить допускаемые недочеты и на этой основе проводить необходимую коррекцию своей познавательной деятельности.

При подготовке к промежуточной аттестации по дисциплине необходимо повторить основные теоретические положения каждой изученной темы и основные термины, самостоятельно решить несколько типовых компетентностно-ориентированных задач.

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

Информационные технологии:

1. Средства для просмотра презентаций;
2. Средства для проведения онлайн-конференций.
3. Электронно-образовательная среда ЮЗГУ

Программное обеспечение:

1. OpenOffice: режим доступа: свободный.
2. Яндекс.Телемост: режим доступа: свободный.

Информационные справочные системы:

1. Научно-информационный портал ВИНИТИ РАН. Режим доступа: свободный.
2. База данных "Патенты России". Режим доступа: свободный.
3. Электронно-библиотечная система «Университетская библиотека онлайн» Режим доступа: по подписке.

4. Электронная библиотека диссертаций и авторефератов РГБ. Режим доступа: свободный.

5. Электронный каталог Научной библиотеки ЮЗГУ. Режим доступа: свободный.

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

Аудиторные занятия по дисциплине проводятся в учебной аудитории для проведения занятий лекционного типа и лаборатории кафедры информационной безопасности, оснащенных стандартной учебной мебелью (столы и стулья для обучающихся; стол и стул для преподавателя; доска).

Для организации образовательного процесса применяются технические средства обучения: Проекционный экран на штативе; Мультимедиа центр: ноутбук ASUS X50VL PMD-T2330/1471024Mb/160Gb/ сумка/ проектор inFocus IN24.

Для осуществления практической подготовки обучающихся при реализации дисциплины используются оборудование и технические средства обучения кафедры информационной безопасности:

1. Класс ПЭВМ - Asus-P7P55LX-/DDR34096Mb/Coree i3-540/SATA-11 500 Gb Hitachi/PCI-E 512Mb, Монитор TFT Wide 23.

2. Мультимедиацентр: ноутбук ASUS X50VL PMD - T2330/14"/1024Mb/ 160Gb/ сумка/проектор inFocus IN24+ .

3. Экран мобильный Draper Diplomat 60x60.

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. 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 звукозаписы-

вающих 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).

14 Лист дополнений и изменений, внесенных в рабочую программу дисциплины

Номер изменения	Номера страниц				Всего страниц	Дата	Основание для изменения и подпись лица, проводившего изменения
	измененных	замененных	аннулированных	новых			