Аннотация к рабочей программе дисциплины «Организация работ по обеспечению безопасности в информационных системах»

Цель преподавания дисциплины

Формирование у студентов знаний в области работ по обеспечению безопасности в информационных системах, организации мероприятий по защите информации, формирования у коллектива представления о важности защиты персональных данных и конфиденциальной информации.

Задачи изучения дисциплины

1 Получение углублённых знаний в теме кадровой политики в области информационной безопасности.

2 Получение навыков планирования работ по обеспечению информационной безопасности .

3 Изучение методов решения проблемных ситуаций в коллективе, развитие организаторских навыков в роли руководителя.

4. Совершенствование знаний в сфере нормативно-правовых актов при организации работ по защите информации .

5. Получение опыта деятельности в управлении разработкой информационных систем.

6. Изучение способов создания комплекса мер по обеспечению информационной безопасности.

7. Изучение порядка разработки модели угроз при построении информационных систем.

Компетенции, формируемые в результате освоения дисциплины

Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий (УК-1)

Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия (УК-5)

Способен организовать работы по выполнению требований защиты информации ограниченного доступа в защищённых информационных системах (ПК-2)

Способен обеспечивать документальное сопровождения процесса обеспечения информационной безопасности(ПК-5)

Разделы дисциплины

Кадровая политика в области информационной безопасности. Методы планирования работ по обеспечению информационной безопасности. Методы решения проблемных ситуаций в коллективе. Применение нормативно-правовых актов при организации работ по защите информации. Управление разработкой информационных систем. Формирование комплекса мер по обеспечению информационной безопасности. Порядок разработки модели угроз при построении информационных систем. Кадровая политика в области информационной безопасности.

МИНОБРНАУКИ РОССИИ

Юго-Западный государственный университет

УТВЕРЖДАЮ:
И. о. декана факультета
фундаментальной и прикладной информатики
(наименование ф-та полностью)

_____ М.О. Таныгин
(подпись, инициалы, фамилия)

«31» 08 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Организация работ по обеспечению безопасности в информационных системах
(наименование дисциплины)

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

«Защищённые информационные системы»
наименование направленности (профиля, специализации)

форма обучения очная
(очная, очно-заочная, заочная)

Курск – 2022

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 №11 от 30.06.2022г.

(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)

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

1.1 Цель дисциплины

Формирование у студентов знаний в области работ по обеспечению безопасности в информационных системах, организации мероприятий по защите информации, формирования у коллектива представления о важности защиты персональных данных и конфиденциальной информации.

1.2 Задачи дисциплины

1 Получение углублённых знаний в теме кадровой политики в области информационной безопасности.

2 Получение навыков планирования работ по обеспечению информационной безопасности

3 Изучение методов решения проблемных ситуаций в коллективе, развитие организаторских навыков в роли руководителя.

4. Совершенствование знаний в сфере нормативно-правовых актов при организации работ по защите информации

5. Получение опыта деятельности в управлении разработкой информационных систем

6. Изучение способов создания комплекса мер по обеспечению информационной безопасности.

7. Изучение порядка разработки модели угроз при построении информационных систем

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 компетенции	*наименование компетенции*		
УК-1	Способен осуществлять критический анализ проблемных	УК-1.2 Определяет пробелы в информации, необходимой для	***Знать:*** ряд проблемных ситуаций, которые могут возникать на предприятии ***Уметь:*** находить выход из

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 компетенции	*наименование компетенции*		
	ситуаций на основе системного подхода, вырабатывать стратегию действий	решения проблемной ситуации, и проектирует процессы по их устранению	сложившейся ситуации путём анализа опыта предыдущих проблем и конкурирующих организаций ***Владеть (или Иметь опыт деятельности):*** проектирования процессов исправления возникающего ряда трудностей в управлении
		УК-1.4 Разрабатывает и содержательно аргументирует стратегию решения проблемной ситуации на основе системного и междисциплинарных подходов	***Знать:*** принципы построения защищённых систем, методы и средства защиты операционных систем, сетевого оборудования, управления доступом, идентификации и аутентификации, настройки межсетевых экранов, защиты от компьютерных вирусов, вопросы организации системы защиты информации в информационных системах (ИС), этапы построения системы защиты информации, политики безопасности, виды угроз и возможные каналы утечки информации, основы проектирования и построения архитектур систем безопасности, методы, модели и технологии проектирования систем безопасности, требования стандартов и руководящих документов, стадии и этапы создания систем безопасности. ***Уметь:*** правильно эксплуатировать антивирусные программные комплексы, снижать

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 компетенции	*наименование компетенции*		
			вероятность отрицательных последствий сетевых атак путем правильной настройки операционной системы, применять средства защиты информации для решения практических задач в области информационной безопасности. ***Владеть (****или* ***Иметь опыт деятельности):*** навыками применения программных средств защиты информации, разработки защищенных сайтов, разработки архитектуры инфокоммутационных систем и сетевой защиты, поиска и обнаружения уязвимых узлов инфокоммуникационных систем и сетей.
УК-5	Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия	УК – 5.1 Анализирует важнейшие идеологические и ценностные системы, сформировавшиеся в ходе исторического развития; обосновывает актуальность их использования при социальном и профессиональном взаимодействии	***Знать:*** историческое наследие и социокультурные традиции различных социальных групп, этносов и конфессий, включая мировые религии, философские и этические учения ***Уметь:*** ориентироваться в историческом наследии и социокультурных традициях различных социальных групп, этносов и конфессий, включая мировые религии, философские и этические учения ***Владеть (****или* ***Иметь опыт деятельности):*** навыками социального и профессионального общения, учитывая историческое

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 компетенции	*наименование компетенции*		
			наследие и социокультурные традиции различных социальных групп, этносов и конфессий, включая мировые религии, философские и этические учения
		УК – 5.2 Выстраивает социальное профессиональное взаимодействие с учетом особенностей основных форм научного и религиозного сознания, деловой и общей культуры представителей других этносов и конфессий, различных социальных групп	***Знать:*** основные формы научного и религиозного сознания, общую культуру представителей других этносов и конфессий, различных социальных групп ***Уметь:*** выстраивать отношения с каждым представителем области профессиональных интересов, уметь наладить работу в коллективе из людей разных этносов и пр. ***Владеть (****или* ***Иметь опыт деятельности):*** навыками социального профессионального взаимодействия с учетом особенностей основных форм научного и религиозного сознания, дело-вой и общей культуры представителей других этносов и конфессий, различных социальных групп
		УК – 5.3 Обеспечивает создание недискриминационной среды взаимодействия при выполнении профессиональных задач	***Знать:*** принципы недискриминационного взаимодействия при личном и массовом общении ***Уметь:*** определять принципы недискриминационного взаимодействия при личном и массовом общении ***Владеть:*** навыками недискриминационного взаимодействия в целях выполнения

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 компетенции	*наименование компетенции*		
			профессиональных задач
ПК-2	Способен организовать работы по выполнению требований защиты информации ограниченного доступа в защищённых информационных системах	ПК – 2.1 Управляет работой специалистов по созданию и эксплуатации средств защиты информации в защищённых информационных системах	***Знать:*** правила работы персонала со средствами защиты информации; ***Уметь:*** формулировать правил работы персонала со средствами защиты информации; **Владеть (или Иметь опыт деятельности):** -навыками разработки правил обращения и эксплуатации средств защиты информации.
		ПК – 2.2 Формирует комплекс мер (принципов, правил, процедур, практических приемов, методов, средств) для защиты в защищённых информационных системах	***Знать:*** правила применения мер защиты информации, направленные на устранение причин возникновения инцидентов информационной безопасности в защищённых ин-формационных системах ***Уметь:*** - формулировать правила применения мер защиты информации, направленные на устранение причин возникновения инцидентов информационной безопасности в защищённых информационных системах ***Владеть (или Иметь опыт деятельности):*** -навыками разработки мер защиты информации, правил применения мер защиты информации, направленных на устранение причин возникновения инцидентов информационной безопасности в защищённых информационных системах
		ПК – 2.3 Управляет процессом разработки моделей	***Знать:*** модели угроза и модели нарушителей безопасности в

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 компетенции	*наименование компетенции*		
		угроз и моделей нарушителя безопасности информационных систем	компьютерных системах ***Уметь:*** определять классы нарушителей и ряд угроз, реализуемых в определённых условиях состояния системы безопасности ***Владеть (****или* ***Иметь опыт деятельности):*** разработкой моделей угроз и нарушителей безопасности компьютерных систем
		ПК – 2.4 Разрабатывает организационно-распорядительные документы, регламентирующие порядок эксплуатации защищённых информационных системах	***Знать:*** основные стандарты, регламентирующие управление информационной безопасности; ***Уметь:*** актуализировать версии организационно-распорядительной документации для эксплуатации телекоммуникационных систем и сетей согласно изменениям, в системе безопасности ***Владеть (****или* ***Иметь опыт деятельности):*** разрабатывать документацию, регламентирующую порядок эксплуатации телекоммуникационных систем и сетей
ПК-7	Способен обеспечивать документальное сопровождения процесса обеспечения информационной безопасности	ПК – 7.1 Определяет перечень объектов информатизации и информации (сведений) ограниченного доступа, подлежащих защите в организации	***Знать:*** Принципы организации телекоммуникационных систем и их уязвимости. ***Уметь:*** Формулировать технические требования к телекоммуникационным системам и мерам по предотвращению уязвимостей. ***Владеть (****или* ***Иметь опыт деятельности):*** навыками

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 компетенции	*наименование компетенции*		
			создания моделей угроз и моделей злоумышленника для телекоммуникационных систем и устройств.
		ПК – 7.2 Разрабатывает обоснование необходимости создания системы защиты информации в организации	***Знать:*** правила выполнения работ по обеспечению информационной безопасности ***Уметь:*** документально описывать применяемые для обеспечения безопасности ТКС технологии ***Владеть (или Иметь опыт деятельности):*** разработки и модернизации систем защиты информации
		ПК – 7.3 Разрабатывает эксплуатационную и техническую документацию на объект информатизации и средства защиты информации	***Знать:*** порядок внедрения, отладки и развития процессов и этапов разработки требований, задач, критериев качества и методов обеспечения информационной безопасности защищённых ТКС в процессе их эксплуатации и модернизации. ***Уметь:*** организовать и управлять внедрением, отладкой и развитием процессов и этапов работ, методов обеспечения информационной безопасности защищённых ТКС в процессе их эксплуатации и модернизации. ***Владеть (****или* ***Иметь опыт деятельности):*** : навыками организации и управления внедрением, отладкой и развитием процессами и

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 компетенции	*наименование компетенции*		
			этапами разработки системобеспечения информационной безопасности ТКС в процессе их эксплуатации и модернизации.

2 Указание места дисциплины в структуре основной профессиональной образовательной программы

Дисциплина «Организация работ по обеспечению безопасности в информационных системах» 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 1 курсе в 1 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 трудоемкость (объем) дисциплины составляет 5 зачетных единиц (з.е.), 180 академических часов.

Таблица 3 – Объем дисциплины

Виды учебной работы	Всего, часов
Общая трудоемкость дисциплины	180
Контактная работа обучающихся с преподавателем по видам учебных занятий (всего)	91.15
в том числе:	
лекции	36
лабораторные занятия	0
практические занятия	54
Самостоятельная работа обучающихся (всего)	52.85
Контроль (подготовка к экзамену)	1.15
Контактная работа по промежуточной аттестации (всего АттКР)	1.15
в том числе:	

Виды учебной работы	Всего, часов
Зачет	не предусмотрен
зачет с оценкой	не предусмотрен
курсовая работа (проект)	не предусмотрена
экзамен (включая консультацию перед экзаменом)	1.15

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	2	3
1	Кадровая политика в области информационной безопасности	Цель и задачи кадрового обеспечения. Основные принципы подготовки кадров. Виды преступлений и правонарушений так или иначе связаны с конкретными действиями сотрудников коммерческих структур. Программа работы с персоналом.
2	Методы планирования работ по обеспечению информационной безопасности	Организационные методы, инженерно-технические методы, технические методы, программно-аппаратные методы обеспечения информационной безопасности. Комплексный подход: использование нескольких способов защиты информации.
3	Методы решения проблемных ситуаций в коллективе	Типы конфликтов в коллективе. Причины, порождающие конфликты. Меры по предотвращению и разрешению конфликтных ситуаций.
4	Применение нормативно-правовых актов при организации работ по защите информации	Виды юридических документов, посвященных защите информации. Содержание законов, касающихся охраны секретных материалов. Федеральные законы, касающиеся защиты информации и информационной безопасности.
5	Управление разработкой информационных систем	Принципы создания информационной системы. Структура среды информационной системы. Модель создания информационной системы. Реинжиниринг бизнес-процессов. Внедрение информационных систем.
6	Формирование комплекса мер по обеспечению информационной безопасности	Концепция безопасности. Объекты защиты. Меры по обеспечению информационной безопасности. Организационные и технические меры обеспечения информационной безопасности предприятия.
7	Порядок разработки модели угроз при построении информационных систем	Принципы разработки модели угроз безопасности информации. Методы выявления и анализа угроз безопасности информации и уязвимостей программного обеспечения. Характеристика степени ущерба. Вероятность реализации угроз.

Таблица 4.1.2 – Содержание дисциплины и его методическое обеспечение

№ п/п	Раздел (тема) дисциплины	Виды деятельности			Учебно-методические материалы	Формы текущего контроля успеваемости *(по неделям семестра)*	Компетенции
		лек., час	№ лаб.	№ пр.			
1	2	3	4	5	6	7	8
1	Кадровая политика в области информационной безопасности	4		1	У-1-5, МУ-1	Т2, ПРР1	УК – 1.2, УК – 1.4
2	Методы планирования работ по обеспечению информационной безопасности	4		2	У-1,2 МУ-2	К2, ПРР2	УК – 5.1, УК – 5.2, УК – 5.3
3	Методы решения проблемных ситуаций в коллективе	4		3	У-1, 5 МУ-3	К 4, ПРР3	УК – 1.2, УК – 1.4
4	Применение нормативно-правовых актов при организации работ по защите информации	6		4	У-4,5 МУ 4	К 8, ПРР4	ПК – 2
5	Управление разработкой информационных систем	6		5	У-3 МУ-5	К 10, ПРР5	ПК – 7
6	Формирование комплекса мер по обеспечению информационной безопасности	6		6	У-1, 5, МУ - 6	Р12, ПРР6	УК – 5
7	Порядок разработки модели угроз при построении информационных систем	6		7	У-2, 3, МУ-7	Р16, ПРР7	ПК – 7

К – коллоквиум, Т – тестирование, Р – защита (проверка) рефератов , ПРР- практическая работа

4.2 Лабораторные работы и (или) практические занятия

4.2.1 Практические работы

Таблица 4.2.1 – Практические занятия

№	Наименование практической работы	Объем, час.
1	2	3
1	Система анализа рисков и проверки политики информационной безопасности предприятия	8
2	Моделирование объектов защиты	8
3	Организационная культура и управление конфликтами	6
4	Работа с нормативно-правовыми документами	8
5	Разработка организационных и технических мер по инженерно-технической защите информации	8
6	Оценка показателей качества функционирования комплексной системы защиты информации на предприятии: физическое проникновение	8
7	Разработка модели угроз информационной безопасности	8
Итого		54

4.3 Самостоятельная работа студентов (СРС)

Таблица 4.3 – Самостоятельная работа студентов

№ раздела (темы)	Наименование раздела (темы) дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час
1	2	3	4
1.	Кадровая политика в области информационной безопасности	2 неделя	6
2.	Методы планирования работ по обеспечению информационной безопасности	6 неделя	6
3.	Методы решения проблемных ситуаций в коллективе	8 неделя	8
4.	Применение нормативно-правовых актов при организации работ по защите информации	12 неделя	8
5.	Управление разработкой информационных систем	14 неделя	8
6.	Формирование комплекса мер по обеспечению информационной безопасности	16 неделя	8
7.	Порядок разработки модели угроз при построении информационных систем	17 неделя	8,85
Итого			52,85

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 УП 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;

– тем рефератов;

– вопросов к зачету;

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

типографией университета:

– помощь авторам в подготовке и издании научной, учебной и методической литературы;

–удовлетворение потребности в тиражировании научной, учебной и методической литературы.

6 Образовательные технологии

Реализация компетентностного подхода предусматривает широкое использование в образовательном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования универсальных, общепрофессиональных и профессиональных компетенций обучающихся. В рамках дисциплины предусмотрены выполнение в ходе практикоориентированных заданий.

Таблица 6.1 – Интерактивные образовательные технологии, используемые при проведении аудиторных занятий

№	Наименование раздела (темы лекции, практического или лабораторного	Используемые интерактивные образовательные технологии	Объем, час.

	занятия)		
1	2	3	4
1	Разработка организационных и технических мер по инженерно-технической защите информации	Выполнение студентом интерактивных заданий по применению мер ИТЗИ	4
2	Оценка показателей качества функционирования комплексной системы защиты информации на предприятии: физическое проникновение	Выполнение студентом интерактивных заданий по показателям качества функционирования системы защиты информации	4
Итого:			8

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)и практики, при изучении/ прохождении которых формируется данная компетенция		
	Начальный	Основной	Завершающий
1	2	3	4
УК-1.2 Определяет пробелы в информации, необходимой для решения проблемной ситуации, и проектирует процессы по их устранению	Организация работ по обеспечению безопасности в информационных системах Современная философия и методология науки		Подготовка к процедуре защиты и защита выпускной квалификационной работы
УК-1.4 Разрабатывает и содержательно аргументирует стратегию решения проблемной ситуации на основе системного и междисциплинарных подходов	Организация работ по обеспечению безопасности в информационных системах Современная философия и методология науки		Управление разработкой систем безопасности Подготовка к процедуре защиты и защита выпускной квалификационной работы
УК – 5.1 Анализирует важнейшие идеологические и ценностные системы, сформировавшиеся в ходе исторического развития; обосновывает актуальность их использования при	Организация работ по обеспечению безопасности в информационных системах Современная философия и методология науки		Подготовка к процедуре защиты и защита выпускной квалификационной работы

социальном и профессиональном взаимодействии			
УК – 5.2 Выстраивает социальное профессиональное взаимодействие с учетом особенностей основных форм научного и религиозного сознания, деловой и общей культуры представителей других этносов и конфессий, различных социальных групп			
УК – 5.3 Обеспечивает создание недискриминационной среды взаимодействия при выполнении профессиональных задач			
ПК – 2.1 Управляет работой специалистов по созданию и эксплуатации средств защиты информации в защищённых информационных системах	Организация работ по обеспечению безопасности в информационных системах	Технологии распределенных реестров Безопасность распределённых систем Производственная проектно-технологическая практика	Методы и средства защиты информации в системах электронного документооборота Подготовка к процедуре защиты и защита выпускной квалификационной работы
ПК – 2.2 Формирует комплекс мер (принципов, правил, процедур, практических приемов, методов, средств) для защиты в защищённых информационных системах			
ПК – 2.3 Управляет процессом разработки моделей угроз и моделей нарушителя безопасности информационных систем			
ПК – 2.4 Разрабатывает организационно-распорядительные документы, регламентирующие порядок эксплуатации защищённых информационных системах			
ПК – 7.1 Определяет перечень объектов информатизации и информации (сведений)	Организация работ по обеспечению безопасности в информационных системах		Производственная проектно-технологическая практика

ограниченного доступа, подлежащих защите в организации		Подготовка к процедуре защиты и защита выпускной квалификационной работы
ПК – 7.2 Разрабатывает обоснование необходимости создания системы защиты информации в организации		
ПК – 7.3 Разрабатывает эксплуатационную и техническую документацию на объект информатизации и средства защиты информации		

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	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
УК-1 основной	УК-1.2 Определяет пробелы в информации, необходимой для решения проблемной ситуации, и проектирует процессы по их устранению УК-1.4 Разрабатывает и содержательно аргументирует стратегию решения проблемной ситуации на основе	**Знать:** виды угроз и возможные каналы утечки конфиденциальной информации по техническим каналам. **Уметь:** выполнять требования нормативных и эксплуатационных документов (документации) по обеспечению защиты информации на объектах информатизации и вскрытия	**Знать:** основные тактико-технические характеристики, принципы построения технических средств передачи и защиты информации, виды сигналов и способы распространения радиоволн, принципы и способы организации системы защиты информации на объектах информатизации.	**Знать:** порядок и алгоритм проведения организационных мероприятий на объектах информатизации. Функциональные обязанности по организации мероприятий по защите информации. **Уметь:** осуществлять выбор технических средств защиты информации в

Код компетенции/ этап	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
	системного и междисциплинарных подходов	каналов утечки информации, по организации мероприятий, направленных на защиту информации. **Владеть (или Иметь опыт деятельности):** навыками разработки нормативных и технических документов по организации защиты объекта информатизации.	**Уметь:** разрабатывать нормативную документацию по выполнению требований защиты информации на объектах информатизации. **Владеть (или Иметь опыт деятельности):** навыками применения технических средств защиты информации.	зависимости от условий эксплуатации объектов информатизации. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями инструкций, эксплуатационной документации. **Владеть (или Иметь опыт деятельности):** навыками проведения организационных мероприятий по вскрытию уязвимых мест систем обеспечения защиты информации объекта информатизации.
УК-5	УК – 5.1 Анализирует важнейшие идеологические и ценностные системы, сформировавшиеся в ходе исторического развития; обосновывает актуальность их использования при социальном и профессионально	**Знать:** отдельные традиции различных социальных групп, этносов и конфессий, включая мировые религии, философские и этические учения ***Уметь:*** ориентироваться	**Знать:** основы социокультурных традиции различных социальных групп, этносов и конфессий, включая мировые религии, философские и этические учения; принципы недискриминационного взаимодействия	Знать: систему социокультурные традиции различных социальных групп, этносов и конфессий, включая мировые религии, философские и этические учения; принципы недискриминационного взаимодействия

Код компетенции/ этап	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
	м взаимодействии УК – 5.2 Выстраивает социальное профессиональное взаимодействие с учетом особенностей основных форм научного и религиозного сознания, деловой и общей культуры представителей других этносов и конфессий, различных социальных групп УК – 5.3 Обеспечивает создание недискриминационной среды взаимодействия при выполнении профессиональных задач	в основных социокультурных традициях различных социальных групп, этносов и конфессий, включая мировые религии, философские и этические учения **Владеть (или Иметь опыт деятельности):** отдельными навыками социального и профессионального общения	при личном и массовом общении ***Уметь:*** ориентироваться в основных социокультурных традициях различных социальных групп, этносов и конфессий, включая мировые религии, философские и этические учения **Владеть (или Иметь опыт деятельности):** Основными навыками социального и профессионального общения, учитывая историческое наследие и социокультурные традиции различных социальных групп, этносов и конфессий, включая мировые религии, философские и этические учения; навыками недискриминационного взаимодействия в целях выполнения профессиональных задач	при личном и массовом общении ***Уметь:*** использовать систему социокультурных традиций различных социальных групп, этносов и конфессий, включая мировые религии, философские и этические учения; определять принципы недискриминационного взаимодействия при личном и массовом общении **Владеть (или Иметь опыт деятельности):** навыками социального и профессионального общения, учитывая историческое наследие и социокультурные традиции различных социальных групп, этносов и конфессий, включая мировые религии, философские и этические учения; навыками

Код компетенции/ этап	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
				недискриминационного взаимодействия в целях выполнения профессиональных задач
ПК-2 начальный	ПК – 2.1 Управляет работой специалистов по созданию и эксплуатации средств защиты информации в защищённых информационных системах ПК – 2.2 Формирует комплекс мер (принципов, правил, процедур, практических приемов, методов, средств) для защиты в защищённых информационных системах ПК – 2.3 Управляет процессом разработки моделей угроз и моделей нарушителя безопасности информационных систем ПК – 2.4 Разрабатывает организационно-распорядительные документы,	***Знать:*** основные правила работы со средствами защиты информации в защищённых информационных системах ***Уметь:*** применять базовые правила работы с штатными средствами защиты информации. ***Владеть (или Иметь опыт деятельности):*** навыками формулирования основных правил работы со средствами защиты информации.	***Знать:*** правила работы со средствами защиты информации. ***Уметь:*** применять правила работы со средствами защиты информации различных производителей. ***Владеть (или Иметь опыт деятельности):*** навыками формулирования перечня правил обращения и работы со средствами защиты информации.	***Знать:*** в полной мере правила работы со средствами защиты информации. ***Уметь:*** в полной мере применять правила работы со средствами защиты информации различных производителей. ***Владеть (или Иметь опыт деятельности):*** навыками формулирования расширенного перечня правил обращения и работы со средствами защиты информации.

Код компетенции/ этап	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
	регламентирующие порядок эксплуатации защищённых информационных системах			
ПК-7 основной	ПК – 7.1 Определяет перечень объектов информатизации и информации (сведений) ограниченного доступа, подлежащих защите в организации ПК – 7.2 Разрабатывает обоснование необходимости создания системы защиты информации в организации ПК – 7.3 Разрабатывает эксплуатационную и техническую документацию на объект информатизации и средства защиты информации	**Знать:** порядок внедрения, отладки и развития процессов и этапов разработки требований, задач. ***Уметь:*** отлаживать этапы работ обеспечения информационной безопасности защищённых систем в процессе их эксплуатации и модернизации. **Владеть (или Иметь опыт деятельности):** навыками отладки систем обеспечения информационной безопасности в процессе их эксплуатации и модернизации.	***Знать:*** порядок внедрения, отладки и развития процессов и этапов разработки требований, задач, критериев качества информационной безопасности защищённых систем в процессе их эксплуатации и модернизации. **Уметь:** управлять внедрением, отладкой и развитием процессов и этапов работ, методов обеспечения информационной безопасности защищённых систем в процессе их эксплуатации и модернизации. **Владеть (или Иметь опыт деятельности):** навыками управления внедрением, отладкой и развитием процессами и этапами	**Знать:** порядок внедрения, отладки и развития процессов и этапов разработки требований, задач, критериев качества и методов обеспечения информационной безопасности защищённых систем в процессе их эксплуатации и модернизации. **Уметь:** организовать и управлять внедрением, отладкой и развитием процессов и этапов работ, методов обеспечения информационной безопасности защищённых систем в процессе их эксплуатации и модернизации. **Владеть (или Иметь опыт деятельности):** навыками организации и управления

Код компетенции/ этап	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
			разработки системобеспечения информационной безопасности систем в процессе их эксплуатации и модернизации.	внедрением, отладкой и развитием процессами и этапами разработки систем обеспечения информационной безопасности систем в процессе их эксплуатации и модернизации.

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	Кадровая политика в области информационной безопасности	УК – 1.2, УК – 1.4	Лекция, СРС, практическая работа №1	Собеседование	1-7	Согласно табл.7.2
				Задания и контрольные вопросы к лаб. № 1	1-6	
2	Методы планирования работ по обеспечению информационной безопасности	УК – 5.1, УК – 5.2, УК – 5.3	Лекция, СРС, практическая работа №2	Собеседование	1-9	Согласно табл.7.2
				Задания и контрольные вопросы к лаб. № 2	1-7	

№ 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
3	Методы решения проблемных ситуаций в коллективе	УК – 1.2, УК – 1.4	Лекция, СРС, практическая работа №3	Собеседование	1-4	Согласно табл.7.2
				Задания и контрольные вопросы к лаб. № 3	1-5	
4	Применение нормативно-правовых актов при организации работ по защите информации	ПК – 2	Лекция, СРС, практическая работа №4	Собеседование	1-6	Согласно табл.7.2
				Задания и контрольные вопросы к лаб. № 4	1-6	
5	Управление разработкой информационных систем	ПК – 7	Лекция, СРС, практическая работа №5	Собеседование	1-7	Согласно табл.7.2
				Задания и контрольные вопросы к лаб. № 5	1-6	
6	Формирование комплекса мер по обеспечению информационной безопасности	УК – 5	Лекция, СРС, практическая работа №6	Собеседование	1-9	Согласно табл.7.2
				Задания и контрольные вопросы к лаб. № 6	1-7	
7	Порядок разработки модели угроз при построении информационных систем	ПК – 7	Лекция, СРС, практическая работа №7	Собеседование	1-5	Согласно табл.7.2
				Задания и контрольные вопросы к лаб. № 6	1-6	

Примеры типовых контрольных заданий для проведения текущего контроля успеваемости

Вопросы для собеседования по разделу (теме) 1. «Кадровая политика в области информационной безопасности»:

1. Что такое «политика безопасности»?
2. От каких факторов зависит выбор персонала?

3. Какие существуют механизмы обеспечения безопасности в распределённых системах?

4. Что такое требования доверия безопасности и для чего они нужны?

5. Задачи, возникающие при выполнении информационно-аналитической работы

Контрольные вопросы для практической работы №1:

1. Что такое политика информационной безопасности?

2. Какие организационные меры защиты существуют?

3. Назначение организационных мер?

4. Какие из них наиболее эффективны? Почему?

5. Перечислите основные нормативные документы, регламентирующие ИБ в России

6. Какой состав и организационная структура системы обеспечения информационной безопасности?

7. В чем заключается стандарт ISO 17799?

8. Опишите методику анализа рисков.

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

Типовые задания для проведения промежуточной аттестации обучающихся

Промежуточная аттестация по дисциплине проводится в форме экзамена. Экзамен 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:

В обязанности какого сотрудника входит разработка и поддержка эффективных мер защиты по обработке информации для обеспечения сохранное данных

1) Сотрудник группы безопасности
2) Администратор безопасности системы
3) Администратор безопасности данных
4) Руководитель группы

Задание в открытой форме:

Все нарушения единого информационного процесса на предприятии связаны с ……. материальных ценностей: бумажных и электронных носителей информации, компьютеров и периферийного оборудования.

Задание на установление правильной последовательности:

Обследование состояния объекта и уровня организации защиты информации, разработка и обоснование задач по защите информации, выявление потенциально возможных угроз информации, внедрение системы защиты информации, анализ безопасности используемых для передачи конфиденциальной информации линий связи.

Задание на установление соответствия:

1. режимно-секретное подразделение;
2. бюро пропусков;
3. контрольно-пропускной пункт (КПП).

А) отвечает за выполнение комплекса мероприятий по пропускному режиму и осуществляют постоянный контроль над их выполнением

Б) служат для непрерывного осуществления пропускного режима на территорию и объекты предприятия, контролируют вход и выход лиц с территории предприятия

В) решает непосредственно задачи по учету, хранению, уничтожению и выдаче пропусков сотрудникам предприятия, а также другим лицам, имеющим на это право

Компетентностно-ориентированная задача:

Провести анализ потенциальных каналов утечки в аудитории проведения занятий. Составить перечень каналов утечки информации на защищаемом объекте с указанием места расположения и предлагаемые технические и организационные меры противодействия.

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»;

– 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
Система анализа рисков и проверки политики информационной безопасности предприятия	2	Выполнил, но «не защитил»	4	Выполнил и «защитил»

Форма контроля	Минимальный балл		Максимальный балл	
	балл	примечание	балл	Примечание
1	2	3	4	5
Моделирование объектов защиты	2	Выполнил, но «не защитил»	4	Выполнил и «защитил»
Организационная культура и управление конфликтами	2	Выполнил, но «не защитил»	4	Выполнил и «защитил»
Работа с нормативно-правовыми документами	2	Выполнил, но «не защитил»	4	Выполнил и «защитил»
Разработка организационных и технических мер по инженерно-технической защите информации	2	Выполнил, но «не защитил»	4	Выполнил и «защитил»
Оценка показателей качества функционирования комплексной системы защиты информации на предприятии: физическое проникновение	2	Выполнил, но «не защитил»	4	Выполнил и «защитил»
Разработка модели угроз информационной безопасности	2		4	
СРС	10		20	
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

8.1 Основная учебная литература

1. Аверченков, В. И. Служба защиты информации: организация и управление : учебное пособие для вузов / В. И. Аверченков, М. Ю. Рытов. - 3-е изд., стереотип. - Москва : Издательство «Флинта», 2016. - 186 с. - URL: http://biblioclub.ru/index.php?page=book&id=93356 (дата обращения: 03.03.2022) . - Режим доступа: по подписке. - Текст : электронный.

2. Аверченков, В. И. Аудит информационной безопасности : учебное пособие для вузов / В. И. Аверченков. - 4-е изд., стереотип. - Москва : Флинта, 2021. - 269 с. - URL: http://biblioclub.ru/index.php?page=book&id=93245 (дата обращения: 03.03.2022) . - Режим доступа: по подписке. - Текст : электронный.

3. Олифер, Виктор Григорьевич. Компьютерные сети. Принципы, технологии, протоколы : учебник для вузов / В. Г. Олифер, Н. А. Олифер. - 4-е изд. - Санкт-Петербург : Питер, 2015. - 943 с. - Текст : непосредственный.

4. Романов, О. А. Организационное обеспечение информационной безопасности : учебник / О. А. Романов, С. А. Бабин, С. Г. Жданов. - М. : Академия, 2008. - 192 с. - Текст : непосредственный.

8.2 Дополнительная учебная литература

1. Абрамов, Г. В. Проектирование информационных систем : учебное пособие / Г. В. Абрамов, И. Е. Медведкова, Л. А. Коробова. - Воронеж : Воронежский государственный университет инженерных технологий, 2012. - 172 с. - URL: http://biblioclub.ru/index.php?page=book&id=141626 (дата обращения: 03.03.2022) . - Режим доступа: по подписке. - Текст : электронный.

2. Лопин, В. Н. Защита информации в компьютерных системах : учебное пособие / В. Н. Лопин, И. С. Захаров, А. В. Николаев ; Министерство образования и науки Российской Федерации, Курский государственный технический университет. - Курск : КГТУ, 2006. - 159 с. : ил. - Текст : непосредственный.

3. Петренко, В .И. Теоретические основы защиты информации : учебное пособие / В. И. Петренко. - Ставрополь : СКФУ, 2015. - 222 с. - URL: http://biblioclub.ru/index.php?page=book&id=458204 (дата обращения: 03.03.2022) . - Режим доступа: по подписке. - Текст : электронный.

5. Технологии обеспечения безопасности информационных систем : учебное пособие / А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов [и др.]. - Москва ; Берлин : Директ-Медиа, 2021. - 210 с. : табл., ил. - URL: https://biblioclub.ru/index.php?page=book&id=598988 (дата обращения: 03.03.2022) . - Режим доступа: по подписке. - Текст : электронный.

6. Шапиро, С. А. Теоретические основы управления персоналом : учебное пособие / С. А. Шапиро, Е. К. Самраилова, Н. Л. Хусаинова. - 2-е изд., доп. и перераб. - Москва ; Берлин : Директ-Медиа, 2015. - 322 с. - URL: http://biblioclub.ru/index.php?page=book&id=272161 (дата обращения: 03.03.2022) . - Режим доступа: по подписке. - Текст : электронный.

7. Галай, А. Г. Экономика и управление предприятием : учебное пособие / А. Г. Галай, В. И. Дудаков. - Москва : Альтаир-МГАВТ, 2013. - 179 с. : табл. - URL: http://biblioclub.ru/index.php?page=book&id=429739 (дата обращения: 03.03.2022) . - Режим доступа: по подписке. - Текст : электронный.

8.3 Перечень методических указаний

1. Система анализа рисков и проверки политики информационной безопасности предприятия : методические указания по выполнению лабораторной работы : [для студентов укрупненной группы специальностей 10.00.00 дневной формы обучения] / Юго-Зап. гос. ун-т ; сост.: В. В. Карасовский, О. А. Демченко. - Курск : ЮЗГУ, 2017. - 9 с. - Текст : электронный.

2. Комплексное обеспечение информационной безопасности инфокоммуникационных систем : методические указания к практическим занятиям для студентов укрупненной группы специальностей 10.00.00 / Юго-Зап. гос. ун-т ; сост.: М. О. Таныгин, И. В. Калуцкий, А. А. Чеснокова. - Курск : ЮЗГУ, 2017. - 48 с. - Текст : электронный.

3. Система анализа рисков и проверки политики информационной безопасности предприятия : методические указания по выполнению лабораторной работы : [для студентов укрупненной группы специальностей 10.00.00 дневной формы обучения] / Юго-Зап. гос. ун-т ; сост.: В. В. Карасовский, О. А. Демченко. - Курск : ЮЗГУ, 2017. - 9 с. - Текст : электронный.

4. Определение показателей защищенности информации при несанкционированном доступе : методические указания по выполнению лабораторной работы : [для студентов укрупненной группы специальностей 10.00.00 дневной формы обучения] / Юго-Зап. гос. ун-т ; сост.: В. В. Карасовский, О. А. Демченко. - Курск : ЮЗГУ, 2017. - 7 с. - Текст : электронный.

5. Оценка показателей качества функционирования комплексной системы защиты информации на предприятии: физическое проникновение : методические указания по выполнению лабораторной работы : [для студентов укрупненной группы специальностей 10.00.00 дневной формы обучения] / Юго-Зап. гос. ун-т ; сост.: В. В. Карасовский, О. А. Демченко. - Курск : ЮЗГУ, 2017. - 16 с. - Текст : электронный.

6. Организационно-правовые механизмы обеспечения информационной безопасности : методические рекомендации по подготовке к практическим занятиям для направления подготовки магистратуры 10.04.01 «Информационная безопасность» для студентов всех форм обучения / Юго-Зап. гос. ун-т ; сост.: А. А. Гребеньков, А. Г. Спеваков. - Курск : ЮЗГУ, 2017. - 28 с. - 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 «Университетская библиотека онлайн» Режим доступа: http://biblioclub.ru

4. Компания «Консультант Плюс» [официальный сайт]. Режим доступа: http://www.consultant.ru

5. Научно-информационный портал ВИНИТИ РАН [официальный сайт]. Режим доступа: http://www.consultant.ru/

6. База данных "Патенты России"

7. Аналитический раздел компании «Код Безопасности» https://www.securitycode.ru/documents/analytics/

10 Методические указания для обучающихся по освоению дисциплины

Основными видами аудиторной работы студента при изучении дисциплины «Организация работ по обеспечению безопасности в информационных системах» являются лекции и практические 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 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.

Практическому 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.

По согласованию с преподавателем или по его заданию студенты готовят рефераты по отдельным темам дисциплины, выступают на занятиях с докладами. Основу докладов составляет, как правило, содержание подготовленных студентами рефератов.

Качество учебной работы студентов преподаватель оценивает по результатам тестирования, собеседования, защиты отчетов по лабораторным работам, а также по результатам докладов.

Преподаватель уже на первых занятиях объясняет студентам, какие формы обучения следует использовать при самостоятельном изучении дисциплины «Организация работ по обеспечению безопасности в информационных системах»: 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, отработку студентами пропущенных лекций, участие в групповых и индивидуальных консультациях (собеседовании). Эти формы способствуют выработке у студентов умения работать с учебником и литературой. Изучение литературы 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 закрепления 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 освоению учебного материала. В случае необходимости студенты обращаются за консультацией к преподавателю по вопросам дисциплины «Организация работ по обеспечению безопасности в информационных системах» с целью освоения и закрепления компетенций.

Основная цель самостоятельной работы студента при изучении дисциплины «Организация работ по обеспечению безопасности в информационных системах» - 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 №К0000000117 от 21.12.2015 г. с

ООО «СМСКанал», Kaspersky Endpoint Security Russian Edition, лицензия 156A-140624-192234, Windows 7, договор IT000012385

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

Учебная аудитория для проведения занятий лекционного и практического типа или лаборатории кафедры «информационная безопасность», оснащенные мебелью: столы, стулья для обучающихся; стол, стул для преподавателя; доска, проектор для демонстрации презентаций. Помещение для самостоятельной работы Компьютер PDC2160/iC33/2*512Mb/HDD 160Gb/DVD-ROM/FDD/ATX350W/ K/m/ OFF/l7"TFT E700 (6 шт)

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).

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
	изме-ненных	замененных	аннулированных	новых			