Аннотация к рабочей программе дисциплины «Порядок проведения аттестации объектов информатизации»

Цель преподавания дисциплины

Целью преподавания дисциплины «Порядок проведения аттестации объектов информатизации» является освоение студентами основных принципов и порядка проведения процедур сертификации и лицензирования в области обеспечения информационной безопасности телекоммуникационных систем.

Задачи изучения дисциплины

– Ознакомить студентов с основными положениями проведения процедур сертификации и лицензирования в области обеспечения информационной безопасности;

– Изучение нормативно-правовой базы процедур сертификации и лицензирования;

– Формирование у обучаемых понимания требований регуляторов к деятельности в области информационной безопасности;

– Ознакомление обучаемых с порядком проведения сертификационных и лицензирующих процедур.

Компетенции, формируемые в результате освоения дисциплины

Способен документально обеспечивать процесса защиты информации в телекоммуникационных системах и сетях (ПК-7);

Способен организовать работы по выполнению требований защиты информации ограниченного доступа в телекоммуникационных системах и сетях (ПК-8).

Разделы дисциплины

Основные понятия в области технической защиты информации. Концептуальные основы защиты информации. Система документов по технической

защите информации. Органы по технической защите информации в РФ. Лицензирование деятельности в области ТЗИ. Объект информатизации. Классификация объектов защиты. Общий порядок сертификации средств защиты информации. Порядок сертификации во ФСТЭК России. Аттестация объекта информатизации по требованиям безопасности информации. Требования и рекомендации по защите информации, обрабатываемой средствами вычислительной техники.

МИНОБРНАУКИ РОССИИ
Юго-Западный государственный университет

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

М.О. Таныгин
(подпись, инициалы, фамилия)
«31» 05 2021 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Порядок проведения аттестации объектов информатизации
(наименование дисциплины)

ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем
шифр и наименование направление подготовки (специальности)

Управление безопасностью телекоммуникационных систем и сетей
наименование направленности (профиля, специализации)

форма обучения *очная*
очная, очно-заочная, заочная

Курск – 2021

Рабочая программа дисциплины «Порядок проведения аттестации объектов информатизации» составлена в соответствии с ФГОС ВО – специалитет по специальности 10.05.02 Информационная безопасность телекоммуникационных систем на основании учебного плана ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем, специализация «Управление безопасностью телекоммуникационных систем и сетей», 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 10.05.02 Информационная безопасность телекоммуникационных систем на основании учебного плана ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем, специализация «Управление безопасностью телекоммуникационных систем и сетей» на заседании кафедры информационной безопасности №1 «30» 08 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 «Порядок проведения аттестации объектов информатизации» пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем, специализация «Управление безопасностью телекоммуникационных систем и сетей», одобренного Ученым советом университета протокол № 6 «26» 02 2021 г., на заседании кафедры ИБ, протокол № 11 от 30.06.2022 г.
(наименование кафедры, дата, номер протокола)

Зав. кафедрой М.О. Таныгин

Рабочая программа дисциплины «Порядок проведения аттестации объектов информатизации» пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем, специализация «Управление безопасностью телекоммуникационных систем и сетей», одобренного Ученым советом университета протокол № ___ «__» _____ 20___ г., на заседании кафедры _____.
(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

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

1.1. Цель преподавания дисциплины

Целью преподавания дисциплины «Порядок проведения аттестации объектов информатизации» является освоение студентами основных принципов и порядка проведения процедур сертификации и лицензирования в области обеспечения информационной безопасности телекоммуникационных систем.

1.2. Задачи дисциплины

1. Ознакомить студентов с основными положениями проведения процедур сертификации и лицензирования в области обеспечения информационной безопасности;
2. Изучение нормативно-правовой базы процедур сертификации и лицензирования;
3. Формирование у обучаемых понимания требований регуляторов к деятельности в области информационной безопасности;
4. Ознакомление обучаемых с порядком проведения сертификационных и лицензирующих процедур.

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, закрепл. за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленной за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код	*наименование*		
ПК-7	Способен документально обеспечивать процесса защиты информации в телекоммуникационных системах и сетях	ПК-7.1 Разрабатывает технические задания на модернизацию систем защиты информации	***Знать:*** - основные требования, предъявляемые к информационным системам и объектам информатизации; - основные этапы разработки технического задания на модернизацию систем защиты информации. ***Уметь:*** - анализировать требования нормативно-правовых актов, предъявляемые к информационным системам; - оценивать выполнение требований нормативных правовых актов в области информационной безопасности для разработки технического задания

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепл. за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленной за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код	*наименование*		
			на модернизацию систем защиты информации. ***Владеть:*** - навыками определения порядка приведения в соответствие информационных систем требованиям регуляторов; - навыками разработки требований, предъявляемых к информационным системам и объектам информатизации; - навыками разработки технического задания на модернизацию систем защиты информации.
		ПК-7.2 Формирует документы для обоснования разработки и модернизации систем защиты информации	***Знать:*** - основные требования, предъявляемые к формированию документов для обоснования разработки и модернизации систем защиты информации; - основные этапы формирования документов на модернизацию систем защиты информации. ***Уметь:*** - сопоставлять текущую структуру предприятия требованиям регуляторов в области ИБ; - анализировать требования нормативно-правовых актов, предъявляемые к объектам информатизации. ***Владеть (****или* ***Иметь опыт деятельности):*** **-** общими приемами организации поиска нормативно-правовой информации для формирования документов на модернизацию систем защиты информации; - навыками работы с нормативно-правовой документацией ФСТЭК и ФСБ.
		ПК-7.3 Разрабатывает модели угроз и модели нарушителей	**Знать**: - основные характеристики программных и технических средств разработки телекоммуникационных систем; - основы формирования и преобразования сигналов в телекоммуникационных системах. **Уметь**: - строить модели формирования и преобразования сигналов - анализировать сигнал в условиях зашумленности ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками разработки модели формирования сигнала - навыками разработки модели преобразования сигнала

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепл. за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленной за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код	*наименование*		
		ПК-7.4 Готовит проекты нормативных и методических материалов, регламентирующих выполнение работ по защите информации	**Знать**: - основные характеристики программных и технических средств разработки телекоммуникационных систем; - основы формирования и преобразования сигналов в телекоммуникационных системах. **Уметь**: - строить модели формирования и преобразования сигналов - анализировать сигнал в условиях зашумленности ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками разработки модели формирования сигнала - навыками разработки модели преобразования сигнала
ПК-8	Способен организовать работы по выполнению требований защиты информации ограниченного доступа в телекоммуникационных системах и сетях	ПК-8.1 Управляет работой специалистов по созданию и эксплуатации средств защиты информации в телекоммуникационных системах и сетях	***Знать:*** - основы формирования исходных данных для телекоммуникационных задач; - основы экономического обоснования проекта. ***Уметь:*** - анализировать исходные данные для обоснования целесообразности разработки проекта; - анализировать предметную область и создавать декларативное описание задачи; - применять принципы выявления ключевых параметров работы информационной системы; ***Владеть (****или* ***Иметь опыт деятельности):*** - приемами анализа полноты и корректности ключевых параметров эксплуатации;
		ПК-8.2 Формирует комплекс мер (принципов, правил, процедур, практических приемов, методов, средств) для защиты в телекоммуникационных системах и сетях информации ограниченного доступа	***Знать:*** - технологии повышения защищенности распределенных информационных систем; ***Уметь:*** - выполнять определять характер угрозы и масштабы последствий; - проектировать регламент защищенного взаимодействия компонентов ТЛК системы; - минимизировать последствия ущерба за счет интеграции средств защиты. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками разработки компонентов ТЛК систем; - навыками обеспечения совместимого взаимодействия отдельных модулей;

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепл. за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленной за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код	*наименование*		
		ПК-8.3 Управляет процессом разработки моделей угроз и моделей нарушителя безопасности компьютерных систем	***Знать:*** - особенности вывода промежуточных значений в ходе работы модулей; - основы использования управляющих директив. ***Уметь:*** - выполнять отладку приложения в пошаговом режиме и с контрольными точками; - минимизировать количество потенциальных нештатных ситуаций работы программы. ***Владеть (****или* ***Иметь опыт деятельности):*** - установки директив, определяющих работу программных модулей; - технологией ведения протокола работы системы с выводом промежуточных результатов обработки данных.
		ПК-8.4 Разрабатывает организационно-распорядительные документы, регламентирующие порядок эксплуатации телекоммуникационных систем и сетей	***Знать:*** - основы работы в режиме пошаговой отладки передачи конфиденциальных данных в информационной системе; - основы шифрования потоков данных; - основы использования средств защиты информации. ***Уметь:*** - организовать безопасную работу в масштабе вычислительной сети; - выводить сообщения в случае возникновения нештатных ситуаций работы информационной системы; - интегрировать средства защиты на программном уровне. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками установки программных средств защиты; - навыками оценки защищенности информационной системы с учетом возможных угроз.
		ПК-8.5 Определяет действия сотрудников при проведении мероприятий по информационной безопасности	***Знать:*** - этапы разработки программного обеспечения; - модели жизненного цикла программного обеспечения; ***Уметь:*** **-** разрабатывать базовые компоненты ТЛК систем; - принимать обоснованные решения по выбору технологий разработки; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками разработки компонентов ТЛК систем на

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепл. за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленной за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код	*наименование*		
			программном уровне; - навыками интеграции отдельных компонентов в состав единой распределенной системы.

2 Указание места дисциплины в структуре основной профессиональной образовательной программы

Дисциплина «Порядок проведения аттестации объектов информатизации» входит в часть, формируемая участниками образовательных отношений основной профессиональной образовательной программы – специалитет по специальности 10.05.02 Информационная безопасность телекоммуникационных систем. Дисциплина изучается на 5 курсе в 9 семестре.

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

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

Таблица 3 – Объем дисциплины

Виды учебной работы	Всего, часов
Общая трудоемкость дисциплины	108
Контактная работа обучающихся с преподавателем по видам учебных занятий (всего)	72.1
в том числе:	
лекции	36
лабораторные занятия	36
практические занятия	0
Самостоятельная работа обучающихся (всего)	35.9
Контроль (подготовка к экзамену)	36
Контактная работа по промежуточной аттестации (всего АттКР)	0.1
в том числе:	
зачет	0.1
зачет с оценкой	не предусмотрен
курсовая работа (проект)	не предусмотрен
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.	Основные понятия в области технической защиты информации	Цель построения системы защиты информации. Основные понятия проблематики построения СЗИ. Виды защиты информации
2.	Концептуальные основы защиты информации. Система документов по технической защите информации.	Концептуальные основы защиты информации. Доктрина информационной безопасности РФ. Законодательные и иные правовые акты в области технической защиты информации.
3.	Органы по технической защите информации в РФ.	Государственные органы в области защиты информации. Фунции ФСТЭК России. Правовые основы деятельности ФСТЭК
4.	Лицензирование деятельности в области ТЗИ.	Общий порядок лицензирования. Порядок получения лицензии следующий. Документы при лицензировании. Прекращение лицензии. Виды деятельности на осуществление которых требуется получение лицензии. Контроль за соблюдением лицензионных требований и условий.
5.	Объект информатизации. Классификация объектов защиты.	Классификация информации. Классификация АС. Классификация СВТ. Политики разграничения доступа
6.	Общий порядок сертификации средств защиты информации.	Понятие сертификации. Органы сертификации, их функции. Порядок проведения процедуры сертификации. Схемы проведения сертификации средств защиты информации.
7.	Порядок сертификации во ФСТЭК России	Подача заявки на сертификацию во ФСТЭК России. Решение на проведение сертификационных испытаний. Заключение договора с испытательной лабораторией. Подготовка исходных данных. Сертификационные испытания.
8.	Аттестация объекта информатизации по требованиям безопасности информации	Необходимость аттестации. Органы, проводящие аттестацию. Ответственность при проведении аттестации. Документальное сопровождение процедуры аттестации. Структура аттестата соответствия.
9.	Требования и рекомендации по защите информации, обрабатываемой средствами	Структура и содержание СТР-К. Обязательные требования. Желательные требования к объектам информатизации. Порядок обеспечения защиты информации в АС. Требования и рекомендации в зависимости от типа АС. Основные рекомендации по защите информации,

	вычислительной техники	составляющей коммерческую тайну.

Таблица 4.1.2 – Содержание дисциплины и её методическое обеспечение

№ п/п	Раздел (тема) дисциплины	Виды деятельности			Учебно-методические материалы	Формы текущего контроля успеваемости *(по неделям семестра)*	Компетенции
		лек.	№ лаб.	№ пр.			
1	Основные понятия в области технической защиты информации	2			У-1	С, КО (2)	ПК-7, ПК-8
2	Концептуальные основы защиты информации. Система документов по технической защите информации.	2	1		У-1-3 МУ-1	С, КО (4)	ПК-7, ПК-8
3	Органы по технической защите информации в РФ.	2			У-4,5 МУ-3	С, КО (6)	ПК-7, ПК-8
4	Лицензирование деятельности в области ТЗИ.	2			У-1,6,7	С, КО (8)	ПК-7, ПК-8
5	Объект информатизации. Классификация объектов защиты.	2			У-1,2	С, КО (10)	ПК-7, ПК-8
6	Общий порядок сертификации средств защиты информации.	2	2		У-4,5 МУ-3	С, КО (12)	ПК-7, ПК-8
7	Порядок сертификации во ФСТЭК России	2			У-4,5	С, КО (14)	ПК-7, ПК-8
8	Аттестация объекта информатизации по требованиям безопасности информации	2	3		У-4,5 МУ-3	С, КО (16)	ПК-7, ПК-8
9	Требования и рекомендации по защите информации, обрабатываемой средствами вычислительной техники	2			У-4,5	С, КО (18)	ПК-7, ПК-8

С – собеседование, КО – контрольный опрос

4.2Лабораторные работы и практические занятия

4.2.1 Лабораторные работы

Таблица 4.2.1 – Лабораторные работы

№	Наименование лабораторной работы	Объем, час.
1	2	3
1	Анализ заданного нормативно-правового акта: методические указания по выполнению практической работы	6
2	Составление обзорного документа по сертифицированным продуктам в заданной области информационной безопасности: методические указания по выполнению практической работы	6
3	Определение класса государственной информационной системы: методические указания по выполнению практической работы	6
Итого		18

4.3 Самостоятельная работа студентов (СРС)

Таблица 4.3 – Самостоятельная работа студентов

№	Наименование раздела учебной дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час.
1	2	3	4
1.	Основные понятия в области технической защиты информации	2 неделя	3,9
2.	Концептуальные основы защиты информации. Система документов по технической защите информации.	4 неделя	4
3.	Органы по технической защите информации в РФ.	6 неделя	4
4.	Лицензирование деятельности в области ТЗИ.	8 неделя	4
5.	Объект информатизации. Классификация объектов защиты.	10 неделя	4
6.	Общий порядок сертификации средств защиты информации.	12 неделя	4
7.	Порядок сертификации во ФСТЭК России	14 неделя	4
8.	Аттестация объекта информатизации по требованиям безопасности информации	16 неделя	4
9.	Требования и рекомендации по защите информации, обрабатываемой средствами вычислительной техники	18 неделя	4
Итого			35,9

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

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

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

библиотекой университета:

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

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

кафедрой:

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

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

− путем разработки вопросов к зачету/экзамену, методических указаний к выполнению лабораторных и практических работ.

типографией университета:

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

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

6 Образовательные технологии. Технологии использования воспитательного потенциала дисциплины

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

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

№	Наименование раздела	Используемые интерактивные образовательные технологии	Объём, час.
1.	Выполнение практической №1	Выполнение студентом	4

	«Анализ заданного нормативно-правового акта: методические указания по выполнению практической работы»	интерактивных заданий по изучению системного подхода при создании структуры ГОСТ и ИСО.	
2.	Выполнение практической работы №2 «Составление обзорного документа по сертифицированным продуктам в заданной области информационной безопасности »	Выполнение студентом интерактивных заданий по анализу сертифицированных продуктов в заданной области информационной безопасности	4
	Итого		8

Технологии использования воспитательного потенциала дисциплины

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

Реализация воспитательного потенциала дисциплины подразумевает:

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

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

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

Реализация воспитательного потенциала дисциплины на учебных занятиях направлена на поддержание в университете единой развивающей образовательной и воспитательной среды. Реализация воспитательного потенциала дисциплины в ходе самостоятельной работы обучающихся способствует развитию в них целеустремленности, инициативности,

креативности, ответственности за результаты своей работы – качеств, необходимых для успешной социализации и профессионального становления.

7 Фонд оценочных средств для проведения промежуточной аттестации

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

Таблица 7.1 – Этапы формирования компетенций

Код и содержание компетенции	Этапы формирования компетенций и дисциплины (модули), при изучении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
ПК-7 Способен документально обеспечивать процесса защиты информации в телекоммуникационных системах и сетях	Порядок проведения аттестации объектов информатизации Производственная преддипломная практика		Подготовка к процедуре защиты и защита выпускной квалификационной работы
ПК-8 Способен организовать работы по выполнению требований защиты информации ограниченного доступа в телекоммуникационных системах и сетях	Порядок проведения аттестации объектов информатизации Организация и управление службой защиты информации Система сертификации и лицензирования деятельности по защите информации Производственная преддипломная практика		Подготовка к процедуре защиты и защита выпускной квалификационной работы

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

Таблица 7.2 – Показатели и критерии оценивания компетенций, шкала оценивания

Код	Показатели	Критерии и шкала оценивания компетенций

компетенции/ этап *(указывается название этапа из п.7.1)*	оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
ПК-7 / основная	ПК-7.1 Разрабатывает технические задания на модернизацию систем защиты информации	***Знать:*** - особенности построения ТЛК систем на базе микропроцессорной техники. ***Уметь:*** - применять аппаратную базу для реализации системы. ***Владеть:*** - навыками оценки быстродействия и защищенности работы логических устройств.	***Знать:*** - методы моделирования логических устройств ***Уметь:*** - использовать методы математического и компьютерного моделирования для анализа проектируемых устройств ***Владеть:*** - навыками использования инструментальных сред моделирования при разработке программного обеспечения - навыками оценки быстродействия и защищенности работы логических устройств.	***Знать:*** - особенности построения ТЛК систем на базе микропроцессорной техники. ***Уметь:*** - использовать методы математического и компьютерного моделирования для анализа проектируемых устройств - применять аппаратную базу для реализации системы. ***Владеть:*** - навыками использования инструментальных сред моделирования при разработке программного обеспечения - навыками оценки быстродействия и защищенности работы логических устройств.
	ПК-7.2 Формирует документы для обоснования разработки и модернизации систем защиты информации	***Знать:*** **-** стандарты, предназначенные для контроля функциональных характеристик работы системы - особенности передачи сообщений между компонентами ТЛК систем. ***Уметь:*** - формализовать выборки для формирования сообщений; - проводить	***Знать:*** - методы повышения уровня защищенности информационных систем; - особенности передачи сообщений между компонентами ТЛК систем. ***Уметь:*** - составлять простые и составные запросы к системам учета. - проводить анализ основных	***Знать:*** - методы повышения уровня защищенности информационных систем; **-** стандарты, предназначенные для контроля функциональных характеристик работы системы - особенности передачи сообщений между компонентами ТЛК систем. ***Уметь:*** - формализовать выборки для

		анализ основных характеристик системы. ***Владеть (****или* ***Иметь опыт деятельности): -*** общими приемами организации поиска; - навыками анализа ожидаемых и фактических результатов работы системы.	характеристик системы. ***Владеть (****или* ***Иметь опыт деятельности): -*** общими приемами организации поиска; - алгоритмическими схемами оценки характеристик;	формирования сообщений; - составлять простые и составные запросы к системам учета. - проводить анализ основных характеристик системы. ***Владеть (****или* ***Иметь опыт деятельности): -*** общими приемами организации поиска; - алгоритмическими схемами оценки характеристик; - навыками анализа ожидаемых и фактических результатов работы системы.
	ПК-7.3 Разрабатывает модели угроз и модели нарушителей	**Знать**: - основные характеристики программных и технических средств разработки телекоммуникационных систем; **Уметь**: - строить модели формирования и преобразования сигналов ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками разработки модели преобразования сигнала	**Знать**: - основы формирования и преобразования сигналов в телекоммуникационных системах. **Уметь**: - анализировать сигнал в условиях зашумленности ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками разработки модели формирования сигнала - навыками разработки модели преобразования сигнала	**Знать**: - основные характеристики программных и технических средств разработки телекоммуникационных систем; - основы формирования и преобразования сигналов в телекоммуникационных системах. **Уметь**: - строить модели формирования и преобразования сигналов - анализировать сигнал в условиях зашумленности ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками разработки модели формирования сигнала - навыками разработки модели преобразования сигнала
	ПК-7.4 Готовит проекты нормативных и методических			

	материалов, регламентирующих выполнение работ по защите информации			
ПК-8 / основная	ПК-8.1 Управляет работой специалистов по созданию и эксплуатации средств защиты информации в телекоммуникационных системах и сетях	***Знать:*** - основы экономического обоснования проекта. ***Уметь:*** - анализировать исходные данные для обоснования целесообразности разработки проекта; - применять принципы выявления ключевых параметров работы информационной системы; ***Владеть (****или* ***Иметь опыт деятельности):*** - приемами анализа полноты и корректности ключевых параметров эксплуатации;	***Знать:*** - основы формирования исходных данных для телекоммуникационных задач; ***Уметь:*** - анализировать исходные данные для обоснования целесообразности разработки проекта; - применять принципы выявления ключевых параметров работы информационной системы; ***Владеть (****или* ***Иметь опыт деятельности):*** - приемами анализа полноты и корректности ключевых параметров эксплуатации;	***Знать:*** - основы формирования исходных данных для телекоммуникационных задач; - основы экономического обоснования проекта. ***Уметь:*** - анализировать исходные данные для обоснования целесообразности разработки проекта; - анализировать предметную область и создавать декларативное описание задачи; - применять принципы выявления ключевых параметров работы информационной системы; ***Владеть (****или* ***Иметь опыт деятельности):*** - приемами анализа полноты и корректности ключевых параметров эксплуатации;
	ПК-8.2 Формирует комплекс мер (принципов, правил, процедур, практических приемов, методов, средств) для защиты в телекоммуникационных системах и сетях информации ограниченного доступа	***Знать:*** - технологии повышения защищенности распределенных информационных систем; ***Уметь:*** - проектировать регламент защищенного взаимодействия компонентов ТЛК системы; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками обеспечения	***Знать:*** - технологии повышения защищенности распределенных информационных систем; ***Уметь:*** - выполнять определять характер угрозы и масштабы последствий; - минимизировать последствия ущерба за счет интеграции средств защиты. ***Владеть (****или*	***Знать:*** - технологии повышения защищенности распределенных информационных систем; ***Уметь:*** - выполнять определять характер угрозы и масштабы последствий; - проектировать регламент защищенного взаимодействия компонентов ТЛК системы; - минимизировать последствия ущерба за счет интеграции средств

		совместимого взаимодействия отдельных модулей;	***Иметь опыт деятельности):*** - навыками разработки компонентов ТЛК систем; - навыками обеспечения совместимого взаимодействия отдельных модулей;	защиты. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками разработки компонентов ТЛК систем; - навыками обеспечения совместимого взаимодействия отдельных модулей;
	ПК-8.3 Управляет процессом разработки моделей угроз и моделей нарушителя безопасности компьютерных систем	***Знать:*** - основы использования управляющих директив. ***Уметь:*** - минимизировать количество потенциальных нештатных ситуаций работы программы. ***Владеть (****или* ***Иметь опыт деятельности):*** - технологией ведения протокола работы системы с выводом промежуточных результатов обработки данных.	***Знать:*** - особенности вывода промежуточных значений в ходе работы модулей; ***Уметь:*** - минимизировать количество потенциальных нештатных ситуаций работы программы. ***Владеть (****или* ***Иметь опыт деятельности):*** - установки директив, определяющих работу программных модулей;	***Знать:*** - особенности вывода промежуточных значений в ходе работы модулей; - основы использования управляющих директив. ***Уметь:*** - выполнять отладку приложения в пошаговом режиме и с контрольными точками; - минимизировать количество потенциальных нештатных ситуаций работы программы. ***Владеть (****или* ***Иметь опыт деятельности):*** - установки директив, определяющих работу программных модулей; - технологией ведения протокола работы системы с выводом промежуточных результатов обработки данных.
	ПК-8.4 Разрабатывает организационно-распорядительные документы, регламентирующие порядок эксплуатации телекоммуникационных	***Знать:*** - основы работы в режиме пошаговой отладки передачи конфиденциальных данных в информационной системе; - основы шифрования потоков данных; ***Уметь:*** - выводить	***Знать:*** - основы шифрования потоков данных; - основы использования средств защиты информации. ***Уметь:*** - организовать безопасную работу в масштабе вычислительной сети;	***Знать:*** - основы работы в режиме пошаговой отладки передачи конфиденциальных данных в информационной системе; - основы шифрования потоков данных; - основы использования средств защиты информации. ***Уметь:***

	систем и сетей	сообщения в случае возникновения нештатных ситуаций работы информационной системы; - интегрировать средства защиты на программном уровне. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками оценки защищенности информационной системы с учетом возможных угроз.	- выводить сообщения в случае возникновения нештатных ситуаций работы информационной системы; - интегрировать средства защиты на программном уровне. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками установки программных средств защиты;	- организовать безопасную работу в масштабе вычислительной сети; - выводить сообщения в случае возникновения нештатных ситуаций работы информационной системы; - интегрировать средства защиты на программном уровне. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками установки программных средств защиты; - навыками оценки защищенности информационной системы с учетом возможных угроз.
	ПК-8.5 Определяет действия сотрудников при проведении мероприятий по информационной безопасности	***Знать:*** - модели жизненного цикла программного обеспечения; ***Уметь:*** **-** разрабатывать базовые компоненты ТЛК систем; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками интеграции отдельных компонентов в состав единой распределенной системы.	***Знать:*** - этапы разработки программного обеспечения; - модели жизненного цикла программного обеспечения; ***Уметь:*** - принимать обоснованные решения по выбору технологий разработки; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками разработки компонентов ТЛК систем на программном уровне; - навыками интеграции отдельных компонентов в состав единой распределенной системы.	***Знать:*** - этапы разработки программного обеспечения; - модели жизненного цикла программного обеспечения; ***Уметь:*** **-** разрабатывать базовые компоненты ТЛК систем; - принимать обоснованные решения по выбору технологий разработки; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками разработки компонентов ТЛК систем на программном уровне; - навыками интеграции отдельных компонентов в состав единой распределенной системы.

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 контроли-руемой	Технология формирова-ния	Оценочные средства		Описание шкал оценивания
				наимено вание	№№ заданий	
1	2	3	4	5	6	7
1.	Основные понятия в области технической защиты информации	ПК-9, ПК-10	Лекция, СРС,	Собеседов ание	1-7	Согласно табл.7.2
2.	Концептуальные основы защиты информации. Система документов по технической защите информации.	ПК-9, ПК-10	Лекция, СРС, практическое занятие	Собеседов ание	1-7	Согласно табл.7.2
				контроль ные вопросы к ПР№1		
3.	Органы по технической защите информации в РФ.	ПК-9, ПК-10	Лекция, СРС	собеседо вание	1-6	Согласно табл.7.2
4.	Лицензирование деятельности в области ТЗИ.	ПК-9, ПК-10	Лекция, СРС	собеседо вание	1-10	Согласно табл.7.2
5.	Объект информатизации. Классификация объектов защиты.	ПК-9, ПК-10	Лекция, СРС	собеседо вание	1-9	Согласно табл.7.2
6.	Общий порядок сертификации средств защиты информации.	ПК-9, ПК-10	Лекция, СРС, практическое занятие	Собеседов ание	1-8	Согласно табл.7.2
				контроль ные вопросы к ПР№2		
7.	Порядок сертификации во ФСТЭК России	ПК-9, ПК-10	Лекция, СРС,	Собеседов ание,	1-7	Согласно табл.7.2
8.	Аттестация объекта информатизации по требованиям безопасности информации	ПК-9, ПК-10	Лекция, СРС, практическое занятие	Собеседов ание	1-10	Согласно табл.7.2
				контроль ные вопросы к ПР№3		

9.	Требования и рекомендации по защите информации, обрабатываемой средствами вычислительной техники	ПК-9, ПК-10	Лекция, СРС,	Собеседование,	1-10	Согласно табл.7.2

Примеры типовых контрольных заданий для проведения текущего контроля успеваемости

Вопросы в тестовой форме по теоретическим разделам (темы 1-5)

Из перечисленного базовыми услугами для обеспечения безопасности компьютерных систем и сетей являются
1) аутентификация;
2) идентификация;
3) целостность;
4) контроль доступа;
5) контроль трафика;
6) причастность.

Готовность устройства к использованию всякий раз, когда в этом возникает необходимость, характеризует свойство:
1) Целостность;
2) Доступность;
3) Детерминированность;
4) Восстанавливаемость.

Гарантия сохранности данными правильных значений, которая обеспечивается запретом для неавторизованных пользователей каким-либо образом модифицировать, разрушать или создавать данные - это
1) Доступность;
2) Детерминированность;
3) Целостность.
4) Восстанавливаемость

Информация - это
1) Только сведения, содержащиеся в электронных базах данных;
2) Только документированные сведения о лицах, предметах, фактах, событиях;
3) Сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.
4) Сведения, поступающие от СМИ

Защита информации это:

1) получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;
2) процесс сбора, накопления, обработки, хранения, распределения и поиска информации;
3) деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё.
4) совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям
5) преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа

Что такое политика безопасности?
1) Пошаговые инструкции по выполнению задач безопасности;
2) Детализированные документы по обработке инцидентов безопасности;
3) Общие руководящие требования по достижению определенного уровня безопасности.
4) Широкие, высокоуровневые заявления руководства

Информация
1) Становится доступной, если она содержится на материальном носителе;
2) Характеризуется всеми перечисленными свойствами;
3) Не исчезает при потреблении.
4) Подвергается только "моральному износу"

Перехват данных является угрозой
1) Целостности;
2) Доступности;
3) Конфеденциальности.

Естественные угрозы безопасности информации вызваны
1) Воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;
2) Ошибками при проектировании АСОИ, её элементов или разработке программного обеспечения;
3) Корыстными устремлениями злоумышленников.
4) Деятельностью человека
5) Ошибками при действиях персонала

Искусственные угрозы безопасности информации вызваны:
1) Ошибками при действиях персонала;
2) Корыстными устремлениями злоумышленников;
3) Ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения.

4) Деятельностью человека
5) Воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека

Вопросы для собеседования

Тема 3. Угрозы ИБ. Классы нарушителей. Оценка риска

1. Угрозы утечки по техническим каналам.
2. Уязвимости каналов взаимодействия.
3. Распространение вредоносных программ и удаленный запуск.
4. Оценка угроз по классам нарушителей.
5. Субъективная оценка вероятности реализации угроз

Кейс – задачи

Тема 6. Криптографические методы защиты

1. Выполните сохранение результатов скремблирования в файл с применением HEX-редактора.
2. Проконтролируйте обратимость преобразования при ассиметричном шифровании.
3. Подберите несколько вариантов закрытого ключа на основе открытого ключа в алгоритме RSA.

Типовые задания для проведения промежуточной аттестации обучающихся

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

Для тестирования используются контрольно-измерительные материалы (КИМ) – вопросы и задания в тестовой форме, составляющие банк тестовых заданий (БТЗ) по дисциплине, утвержденный в установленном в университете порядке.

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

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

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

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

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

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

Примеры типовых заданий для проведения
промежуточной аттестации обучающихся

Задание в закрытой форме:
Используя браузер выполняется запрос методом ___.

Задание в открытой форме:
Вредоносные вставки при обращении к базе данных называются:
- инъекциями
- синхронизацией
-транзакциями

Задание на установление правильной последовательности,
Пользователь зарегистрирован, авторизован, аутентифицирован.

Задание на установление соответствия:
1 Наиболее эффективный в системах обработки конфиденциальных данных алгоритм
2 Наиболее эффективный в системах реального времени алгоритм диспетчеризации
3 Наиболее просто реализуемый алгоритм
4 Алгоритм, позволяющий реализовывать динамические приоритеты
5 Алгоритм, при котором процесс может оставаться неограниченно долго в режиме ожидания
А "самый короткий - следующий"
Б алгоритм планирования согласно приоритетам
В "самый длинный - следующий"
Г выбор случайного процесса _____.

Компетентностно-ориентированная задача:

В качестве входной информации берется текстовый файл, состоящий из ФИО студента, названия кафедры и специальности. Исходный поток данных соответствует последовательности бит, расположение которых определяется формулой, учитывающей порядковый номер студента по списку.

$$ci = (7i+n) \bmod 13 + 13i$$

Ключ скремблера соответствует номеру зачетки студента «слева направо», генератор псевдослучайных чисел - аналогично «справа налево».

Порядок выполнения работы:

1. Сформировать блок исходных данных (не более 48 бит)
2. Рассчитать состояния скремблера для обработки входного блока
3. Рассчитать период зацикливания и период наибольшей длины скремблера.
4. Произвести скремблирование исходных данных.
5. Подобрать скремблер минимальной разрядности, который не зациклится при обработке всего исходного файла.

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

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

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

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

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

Таблица 7.4 – Порядок начисления баллов в рамках БРС

Форма контроля	Минимальный балл		Максимальный балл	
	балл	примечание	балл	примечание
Выполнение лабораторной работы №1 «Анализ заданного нормативно-правового акта: методические указания по выполнению практической работы»	8	Выполнил, но «не защитил»	12	Выполнил и «защитил»

Выполнение лабораторной работы №2 «Составление обзорного документа по сертифицированным продуктам в заданной области информационной безопасности»	8	Выполнил, но «не защитил»	12	Выполнил и «защитил»
Выполнение лабораторной работы №3 «Определение класса государственной информационной системы: методические указания по выполнению практической работы»	8	Выполнил, но «не защитил»	12	Выполнил и «защитил»
СРС	0		12	
ИТОГО	24		48	
Посещаемость	0		16	
Зачёт	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 –2балла,
– 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 литература

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

2 Крылова, Г. Д. Основы стандартизации, сертификации, метрологии : учебник / Г. Д. Крылова. - 3-е изд., перераб. и доп. - Москва : Юнити-Дана, 2015. - 671 с. - URL: http://biblioclub.ru/index.php?page=book&id=114433 (дата обращения: 09.09.2019) . - режим доступа: по подписке. - Текст : электронный.

3 Камардин, Н. Б. Метрология, стандартизация, подтверждение соответствия : учебное пособие / Н. Б. Камардин, И. Ю. Суркова. - Казань : Издательство КНИТУ, 2013. - 240 с. - URL: http://biblioclub.ru/index.php?page=book&id=258829 (дата обращения: 09.09.2019) . - режим доступа: по подписке. - Текст : электронный.

8.2 Дополнительная литература

1. Спеваков, А. Г. Основы правового обеспечения информационной безопасности : учебное пособие / А. Г. Спеваков, А. П. Фисун ; Юго-Зап. гос. ун-т. - Курск : ЮЗГУ, 2013 - .Ч. 1. - 150 с. : ил., табл. - ISBN 978-5-7681-08 57-1. – Текст: непосредственный.

2. Организационно-правовое обеспечение информационной безопасности [Текст] : учебное пособие / под ред. А. А. Стрельцова. - М. : Академия, 2008. - 256 с.

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

4. Титов, В. С. Метрология, стандартизация и сертификация : учебное пособие / В. С. Титов, В. Е. Эрастов ; Министерство образования и науки Российской Федерации, Курский государственный технический университет. - Курск : КГТУ, 2005. - 184 с. - ISBN 5-7681-0240-X : 85.00 р. - Текст : непосредственный.

5. Кретова, Валерия Михайловна. Метрология, стандартизация и сертификация : конспект лекций / В. М. Кретова ; МИНОБРНАУКИ РОССИИ, Юго-Западный государственный университет. - Курск : ЮЗГУ, 2011. - 168 с. - Имеется электрон.аналог. - 170 р. - Текст : непосредственный.

8.3 Перечень методических указаний

1) Определение класса государственной информационной системы (ГИС) [Электронный ресурс] : методические указания по выполнению практической работы : [для студентов укрупненной группы специальностей 10.00.00 дневной формы обучения] / Юго-Зап. гос. ун-т ; сост.: Е. С. Волокитина, М. О. Таныгин. - Курск : ЮЗГУ, 2017. - 12 с.

2) Разработка структуры государственных и международных стандартов в Российской Федерации в области информационной безопасности и защиты информации [Электронный ресурс] : методические указания по выполнению практической работы : [для студентов укрупненной группы специальностей 10.00.00 дневной формы обучения] / Юго-Зап. гос. ун-т ; сост.: Е. С. Волокитина, М. О. Таныгин. - Курск : ЮЗГУ, 2017. - 7 с.

3) Составление обзорного документа по сертифицированным продуктам в заданной области информационной безопасности [Электронный ресурс] : методические указания по выполнению практической работы : [для студентов укрупненной группы специальностей 10.00.00 дневной формы обучения] / Юго-Зап. гос. ун-т ; сост.: Е. С. Волокитина, М. О. Таныгин. - Курск : ЮЗГУ, 2017. - 7 с.

4) Анализ заданного нормативно-правового акта Российской Федерации [Электронный ресурс] : методические указания по выполнению практической работы : [для студентов укрупненной группы специальностей 10.00.00 дневной формы обучения] / Юго-Зап. гос. ун-т ; сост.: Е. С. Волокитина, М. О. Таныгин. - Курск : ЮЗГУ, 2017. - 7 с.

9 Перечень ресурсов информационно-телекоммуникационной сети Интернет

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) Сообщество Ubuntu [официальный сайт]. Режим доступа: http://ubuntu.com/
4) Корпорация Microsoft [официальный сайт]. Режим доступа: http://microsoft.com/
5) Электронно-библиотечная система «Университетская библиотека онлайн» Режим доступа: http://biblioclub.ru
6) Компания «Консультант Плюс» [официальный сайт]. Режим доступа: http://www.consultant.ru
7) Научно-информационный портал ВИНИТИ РАН [официальный сайт]. Режим доступа: http://www.consultant.ru/
8) База данных "Патенты России"

10 Методические указания для обучающихся по освоению дисциплины

Основными видами аудиторной работы студента при изучении дисциплины 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.

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

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

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

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

Основная цель самостоятельной работы студента при изучении дисциплины - закрепить теоретические знания, полученные в процессе лекционных занятий, а также сформировать практические навыки самостоятельного анализа особенностей дисциплины.

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

Microsoft Office 2016.Лицензионный договор №S0000000722 от 21.12.2015 г. с ООО «АйТи46», лицензионный договор №K0000000117 от

21.12.2015 г. с ООО «СМСКанал», Kaspersky Endpoint Security Russian Edition, лицензия 156A-140624-192234,Windows, договор IT000012385, Oracle Virtualbox (Бесплатная, GNU General Public License), редактор двоичных файлов Free Hex Editor Neo, (Свободное ПО http://www.hhdsoftware.com/free-hex-editor), ОС Ubuntu (Бесплатная, GNU GPLv3), IDE Visual studio code (https://code.visualstudio.com) (свободное ПО), NodeJS (https://nodejs.org/dist/) (свободное ПО), XAMPP (https://www.apachefriends.org/ru/index.html), Composer (https://getcomposer.org/download/) (свободное ПО), GIT (https://git-scm.com/downloads) (свободное ПО), PostgreSQL + PgAdmin (свободное ПО), портал верификации результатов шифрования (https://x46.herokuapp.com) (свободное ПО).

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

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

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

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

Для лиц с нарушением слуха возможно предоставление учебной информации в визуальной форме (краткий конспект лекций; тексты заданий, напечатанные увеличенным шрифтом), на аудиторных занятиях допускается присутствие ассистента, а также сурдопереводчиков и тифлосурдопереводчиков. Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменно отвечает на вопросы, письменно выполняет практические задания. Доклад (реферат) также может быть представлен в письменной форме, при этом требования к содержанию остаются теми же, а требования к качеству изложения материала (понятность, качество речи, взаимодействие с аудиторией и т. д.) заменяются на соответствующие требования, предъявляемые к письменным работам (качество оформления текста и списка литературы, грамотность, наличие иллюстрационных материалов и т.д.). Промежуточная аттестация для лиц с нарушениями слуха проводится в письменной форме, при этом используются общие критерии оценивания. При необходимости время подготовки к ответу может быть увеличено.

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

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