Аннотация к рабочей программе дисциплины «Теоретические основы компьютерной безопасности»

Цель преподавания дисциплины

Дисциплина «Теоретические основы компьютерной безопасности» преподается с целью обучения студентов основам обеспечения информационной безопасности на как уровне отдельного терминала, так и в масштабе распределенной системы с применением актуальных инструментальных средств с учетом требований нормативно-правовой базы Российской Федерации.

Задачи изучения дисциплины

1. Ознакомление с принципами, базовыми определениями и вариантами организации защиты информации;
2. Ознакомление с актуальной нормативно-правовой базой РФ по части информационной безопасности.
3. Изучение угроз информационной безопасности, моделей поведения злоумышленника, основ работы с конфиденциальными данными;
4. Ознакомление с основами защиты авторских прав, работы с персональными данными;
5. Изучения способов выявления контрафактной продукции;
6. Изучение, в том числе на практическом уровне, основ криптографических преобразований в части потоковых шифров, ассиметричных систем и перспективных методов защиты.
7. Ознакомление с технологиями защиты программного обеспечения.

Индикаторы компетенций, формируемые в результате освоения дисциплины

ПК-1.1 Разрабатывает проектные документы на средства защиты информации создаваемых телекоммуникационных систем и сетей.

ПК-1.2 Готовит техническую и проектную документацию по вопросам создания защищённых информационных систем.

ПК-1.3 Сопоставляет характеристики проектируемых решений с требованиями защиты информации.

ПК-1.4 Формирует конфигурацию и состав защищённых информационных систем

ПК-3.2 Разрабатывает формальные модели обработки и передачи данных в информационных системах.

ПК-3.3 Формулирует целевые критерии для оценивания эффективности исследуемых систем.

ПК-3.4 Определяет в результате натурных или математических экспериментов характеристики защищённых информационных систем.

ПК-8.1 Формирует перечень угроз для защищаемой информационной системы.

ПК-8.2 Формирует критерии оценки каждого вида угроз в защищаемой системе.

ПК-8.3 Классифицирует угрозы информационной безопасности исходя из существующих и оригинальных методик.

ПК-8.4 Формирует перечень нарушителей информационной безопасности и их возможностей.

Разделы дисциплины

Основные аспекты построения системы информационной безопасности. Угрозы информационной безопасности, оценка риска их возникновения. Персональные данные, защита авторских прав. Выявление контрафактной продукции. Криптографические методы защиты. Методы выбора системы защиты информации.

МИНОБРНАУКИ РОССИИ
Юго-Западный государственный университет

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

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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Теоретические основы компьютерной безопасности
(наименование дисциплины)

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

Защищённые информационные системы
наименование направленности (профиля, специализации)

форма обучения очная
очная, очно-заочная, заочная

Курск – 2021

Рабочая программа дисциплины «Теоретические основы компьютерной безопасности» 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 № __ «__» _____ 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» 08 2021 г.

Зав. кафедрой _____ Таныгин М.О.

Разработчик программы
к.т.н., доцент _____ Марухленко А.Л.
(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 30.06.2022 г.
(наименование кафедры, дата, номер протокола)

Зав. кафедрой Таныгин М.О.

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

Зав. кафедрой Марухленко А.Л.

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.04.01 Информационная безопасность, профиль «Защищённые информационные системы», одобренного Ученым советом университета протокол № ___ «__» _____ 20___ г., на заседании кафедры _____.
(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

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

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

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

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

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

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

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

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

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

1.1. Цель преподавания дисциплины

Дисциплина «Теоретические основы компьютерной безопасности» преподается с целью обучения студентов основам обеспечения информационной безопасности на как уровне отдельного терминала, так и в масштабе распределенной системы с применением актуальных инструментальных средств с учетом требований нормативно-правовой базы Российской Федерации.

1.2. Задачи изучения дисциплины

1. Ознакомление с принципами, базовыми определениями и вариантами организации защиты информации;
2. Ознакомление с актуальной нормативно-правовой базой РФ по части информационной безопасности.
3. Изучение угроз информационной безопасности, моделей поведения злоумышленника, основ работы с конфиденциальными данными;
4. Ознакомление с основами защиты авторских прав, работы с персональными данными;
5. Изучения способов выявления контрафактной продукции;
6. Изучение, в том числе на практическом уровне, основ криптографических преобразований в части потоковых шифров, ассиметричных систем и перспективных методов защиты.
7. Ознакомление с технологиями защиты программного обеспечения.

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

Таблица 1.3 – Результаты обучения по дисциплине

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код комп	*наименование компетенции*		
ПК-1	Способен формировать проектные решения по созданию и модернизации защищённых информационных систем	ПК-1.1 Разрабатывает проектные документы на средства защиты информации создаваемых телекоммуникационных систем и сетей	***Знать:*** - нормативная база, регламентирующая создание средств защиты информации создаваемых телекоммуникационных систем и сетей; - назначение и классификация средств защиты информации; - источники и классификация угроз; - методы проектирования средств защиты информации создаваемых телекоммуникационных систем и сетей. ***Уметь:*** - разрабатывать проекты технических заданий на проектирование средств защиты информации; - разрабатывать проекты нормативно-распорядительные документов; - классифицировать и оценивать угрозы ИБ для объекта информатизации; - составлять проектную документацию на систему защиты информации. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками разработки технических заданий; - навыками разработки проектов нормативно-распорядительных документов; - навыками оценки угроз ИБ.
		ПК-1.2 Готовит техническую и проектную документацию по вопросам создания защищённых информационных систем	***Знать:*** - основные методы организационного обеспечения процесса подготовки документов, регламентирующих создание защищённых информационных систем; - организационные меры по защите информации; - нормативные правовые акты в области защиты информации. ***Уметь:*** - готовить проектную и техническую документацию по вопросам создания защищённых информационных систем; - готовить проекты методических документов; - применять необходимые нормативные правовые акты; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками организации проекта; - навыками подготовки необходимой технической и проектной документации;
		ПК-1.3 Сопоставляет характеристики проектируемых	***Знать:*** - характеристики проектируемых решений; - нормативная база, регламентирующая создание средств защиты информации;

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код комп	*наименование компетенции*		
		решений с требованиями защиты информации	***Уметь:*** - анализировать характеристики проектируемых решений; - сопоставлять характеристики проектируемых решений с требованиями защиты информации; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками составления проектируемых решений; - навыками анализа характеристик проектируемых решений с требованиями защиты информации.
		ПК-1.4 Формирует конфигурацию и состав защищённых информационных систем	***Знать:*** - определение конфигурации; - состав защищённых информационных систем; - архитектура средств контроля конфигурации; - модули ***Уметь:*** - формировать эталон конфигурации ИС; - считывать текущую конфигурацию и сравнивать её с эталонной; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками анализа состава защищённых информационных систем; - навыками работы с конфигурационными файлами; - навыками работы с несколькими модулями проверки.
ПК-3	Способен проводить теоретические и экспериментальные исследования защищённости информационных систем	ПК-3.2 Разрабатывает формальные модели обработки и передачи данных в информационных системах	***Знать:*** - модели обработки и передачи данных в информационных системах; - виды обработки информации, классификация архитектур ЭВМ; - характеристики и назначение ИТ передачи информации; - классификация локальных вычислительных сетей; - модель OSI, протоколы ***Уметь:*** - определить вид обработки информации; - определить архитектуру ЭВМ; - определить тип ЛВС; - разработать формальную модель обработки и передачи данных в ИС ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками определения архитектуры ЭВМ; - навыками применения модели OSI; - навыками использования протоколов при передаче данных.
		ПК-3.3 Формулирует целевые критерии для оценивания эффективности исследуемых систем	***Знать:*** - основные целевые критерии для оценки эффективности исследуемых систем; - определение информации и её типы с точки зрения защищённости ИС; - принципы создания экспертной комиссии для проведения оценки эффективности исследуемых

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код комп	*наименование компетенции*		
			систем с учётом основных типов угроз нарушения: конфиденциальности, целостности, доступности информации. ***Уметь:*** - определять целевые критерии для оценки эффективности исследуемых систем; - определять тип информации; - самостоятельно организовывать экспертную комиссию для оценивания эффективности исследуемых систем ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками анализа целевых критериев для оценивания эффективности исследуемых систем; - навыками определения типа информации, подлежащей защите; - навыками организации экспертной оценки эффективности исследуемых систем.
		ПК-3.4 Определяет в результате натурных или математических экспериментов характеристики защищённых информационных систем	***Знать:*** - основные подходы к оценке качества защищённых ИС; - методики проведения натурных и математических экспериментов характеристики защищённых ИС; - методологические аспекты для выявления соответствия характеристик защищённых ИС требованиям, к ним предъявляемым. ***Уметь:*** - определять функциональные характеристики отдельных структурных компонентов ИС - определять на основе функционала компонентов защищённых ИС уровень защищённости системы в целом; - самостоятельно разрабатывать программы и методики проведения натурных и математических исследований средств и систем обеспечения информационной безопасности. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками анализа защищённых ИС и выявления характеристик, как всех систем в целом, так и их отдельных функциональных блоков; - навыками разработки технического облика средств обработки и передачи данных в информационных системах; - навыками разработки методик теоретических и экспериментальных исследований защищённости информационных систем.
ПК-8	Способен управлять рисками информационной безопасности	ПК-8.1 Формирует перечень угроз для защищаемой информационной системы	***Знать*** -определение угрозы защищённой ИС; -классификацию и общий анализ угроз; -отличие случайных и преднамеренных угроз; - стек технологий обеспечения информационной безопасности. ***Уметь:*** - проводить анализ возможных угроз и каналов

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код комп	*наименование компетенции*		
			утечки информации; - проводить анализ рисков; - проводить анализ, используя ГОСТ и международные стандарты; ***Владеть (или Иметь опыт деятельности):*** - навыками определения угроз для защищаемой ИС; - навыками проведения анализа рисков.
		ПК-8.2 Формирует критерии оценки каждого вида угроз в защищаемой системе	***Знать:*** - основные характеристики ИС; - классификацию угроз и критерии оценки каждого вида; - виды уязвимостей в ИС. ***Уметь:*** - собирать данные о самой ИС; - формировать критерии каждого вида угрозы в защищаемой системе; - найти потенциальные уязвимости в ИС. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками сбора данных о самой ИС; - навыками определения потенциальных угроз; - навыками выявления потенциальных уязвимостей в ИС.
		ПК-8.3 Классифицирует угрозы информационной безопасности исходя из существующих и оригинальных методик	***Знать:*** - классификацию угроз информационной безопасности; - методики формирования модели угроз для информационной системы; - качественные и количественные методики оценки риска ИБ. ***Уметь:*** - выделять и ранжировать угрозы информационной безопасности; - определять наиболее подходящую методику для определения угрозы ИБ исходя из существующих и оригинальных методик; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками формирования списка угроз, актуальных для конкретной информационной системы - навыками правильного применения выбранной методики.
		ПК-8.4 Формирует перечень нарушителей информационной безопасности и их возможностей	***Знать:*** - определение нарушителя информационной безопасности; - модель нарушителя информационной безопасности; - перечень нарушителей информационной безопасности. ***Уметь:*** - определять нарушителя информационной безопасности; -спрогнозировать вероятных нарушителей информационной безопасности;

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код комп	*наименование компетенции*		
			- оценить уровень информированности потенциального нарушителя о защищаемой системе (ЗС) и возможность влияния на ЗС; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками определения нарушителя информационной безопасности; - навыками прогнозирования вероятных нарушителей информационной безопасности; - навыками оценки уровня информированности потенциального нарушителя.

2. Указание места дисциплины в структуре основной профессиональной образовательной программы

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

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

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

Таблица 3 – Объем дисциплины

Виды учебной работы	Всего, часов
Общая трудоемкость дисциплины	108
Контактная работа обучающихся с преподавателем по видам учебных занятий (всего)	54.1
в том числе:	
лекции	18
лабораторные занятия	0
практические занятия	36
Самостоятельная работа обучающихся (всего)	53.9
Контроль (подготовка к экзамену)	

Контактная работа по промежуточной аттестации (всего АттКР)	0.1
в том числе:	
зачет	0.1
зачет с оценкой	не предусмотрен
курсовая работа (проект)	не предусмотрена
экзамен (включая консультацию перед экзаменом)	не предусмотрена

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

4.1. Содержание дисциплины

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

№ п/п	Раздел (тема) дисциплины	Содержание
1.	Основные аспекты построения системы информационной безопасности	Регулирование ответственности нарушений информационной безопасности. Программа информационной безопасности. Контроль деятельности в области безопасности. Модели представления информационной защиты. Формирование требований к системе информационной безопасности. Этапы обеспечения информационной безопасности.
2.	Угрозы информационной безопасности, оценка риска их возникновения	Угрозы утечки по техническим каналам, уязвимости каналов взаимодействия. Анализ сетевого трафика. Сканирование сети. Угрозы выявления пароля. Подмена доверенного объекта. Навязывание ложного маршрута. Внедрение ложного объекта. Отказ в обслуживании. Распространение вредоносных программ и удаленный запуск. Оценка угроз по классам нарушителей. Субъективная оценка вероятности реализации угроз
3.	Персональные данные, защита авторских прав	Обработка персональных данных. Защита интеллектуальной собственности. Авторское право. Гражданско-правовая ответственность. Административная ответственность. Уголовная ответственность
4.	Выявление контрафактной продукции	Выявление контрафактной продукции. Выбор оптимальных методов контроля и защиты информационной систем. Лицензирование

		программных продуктов. Интеграция механизмов защиты в программное обеспечение для борьбы с НСД.
5.	Криптографические методы защиты	Основы криптографии, методы защиты. Классификация криптографических методов. Потоковые шифры. Скремблирование. Ассиметричные шифры. Клеточные автоматы
6.	Методы выбора системы защиты информации	Классификация методов выбора систем защиты информации. Метод анализа иерархий. Метод парных сравнений альтернатив. Многокритериальный выбор в иерархических структурах с множеством различных альтернатив под критериями. Методы принятия решений, основанные на исследовании операций. Сопоставление угроз и методов и средств их устранения. Игровые стратегии выбора системы защиты информации

Таблица 4.1.2 – Содержание дисциплины и её методическое обеспечение

№ Пп/п	Раздел (тема) дисциплины	Виды деятельности			Учебно-методические материалы	Формы текущего контроля успеваемости *(по неделям семестра)*	Компетенции
		лек., час	№ лб.	№ пр.			
1	2	3	4	5	6	7	8
1.	Основные аспекты построения системы информационной безопасности	2			У-1, МО-1	С,Т	ПК-1 ПК-3
2.	Угрозы информационной безопасности, оценка риска их возникновения	2		1	У-2, 6, МО-1	С,Т	ПК-3 ПК-8
3.	Персональные данные, защита авторских прав	4			У-1,2 МО-2	С	ПК-1
4.	Выявление контрафактной продукции	4			У-1,2 МО-3	С	ПК-3 ПК-8
5.	Криптографические методы защиты	2		2-5	У-1,2 МО-4-9	С	ПК-1 ПК-3 ПК-8
6.	Методы выбора системы защиты информации	4		6		С,Т	ПК-8

С – собеседование, Т – тест

4.2. Лабораторные работы и практические занятия

4.2.1. Практические работы

Таблица 4.2.1 – Практические занятия

№	Наименование	Объем, час.
1.	Анализ защищенности вычислительной системы	4
2.	Шифры полиалфавитной замены	4
3.	Потоковые шифры. Скремблирование бинарного потока данных	8
4.	Ассиметричные клиптоалгоритмы. Метод RSA	8
5.	Обработка на базе клеточных автоматов	8
6.	Интеграция механизмов защиты в программное обеспечение	4
Итого		36

4.3. Самостоятельная работа студентов (СРС)

Таблица 4.5 – Самостоятельная работа студентов

№	Наименование раздела учебной дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час.
1.	Основные аспекты построения системы информационной безопасности	1-4 недели	4
2.	Угрозы информационной безопасности, оценка риска их возникновения	5-8 недели	8
3.	Персональные данные, защита авторских прав	9-11 недели	6
4.	Выявление контрафактной продукции	12-14 нед	5
5.	Криптографические методы защиты	3-18 недели	26.9
6.	Методы выбора системы защиты информации	8-11 недели	4
Итого			53,9

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

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

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

библиотекой университета:

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

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

кафедрой:

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

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

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

типографией университета:

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

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

6. Образовательные технологии.

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 профессиональных компетенций обучающихся. В рамках дисциплины предусмотрены выполнение в ходе лабораторных работ практикоориентированных заданий.

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

№	Наименование раздела	Используемые интерактивные образовательные технологии	Объём, час.
1.	Выполнение практической работы №1	Выполнение студентом интерактивных заданий по определению этапов проектирования информационной системы	4
2.	Выполнение лабораторной работы №3	Выполнение студентом интерактивных заданий по определению характеристик информационной системы	6
	Итого		10

Технологии использования воспитательного потенциала дисциплины

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

Реализация воспитательного потенциала дисциплины подразумевает:

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

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

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

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

7. Фонд оценочных средств для проведения промежуточной аттестации

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

Таблица 7.1 – Этапы формирования компетенций

Код и содержание компетенции	Этапы формирования компетенций и дисциплины (модули), при изучении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
ПК-1 Способен формировать проектные решения по созданию и модернизации защищённых информационных систем	Методы и средства защиты информации в системах электронного документооборота Управление разработкой систем безопасности Безопасность распределённых систем		Производственная проектно-технологическая практика Подготовка к процедуре защиты и защита выпускной квалификационной работы
ПК-3 Способен проводить теоретические и экспериментальные исследования защищённости информационных систем	Методология научных исследований Организация научной деятельности Математические проблемы обеспечения информационной безопасности		Подготовка к процедуре защиты и защита выпускной квалификационной работы
ПК-8 Способен управлять рисками информационной безопасности	Экспертные системы комплексной оценки безопасности информационных и телекоммуникационных систем Информационно-аналитические системы безопасности		Производственная преддипломная практика Подготовка к процедуре защиты и защита выпускной квалификационной работы

7.2. Описание показателей и критериев оценивания компетенций на раз- личных этапах их формирования, описание шкал оценивания

Таблица 7.2 – Показатели и критерии оценивания компетенций, шкала оценивания

Код компетенции/ этап *(указывается название этапа из п.7.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
ПК-1 / осн	ПК-1.1 Разрабатывает проектные	***Знать:*** - нормативная база, регламентирующая	***Знать:*** - назначение и классификация	***Знать:*** - нормативная база, регламентирующая

	документы на средства защиты информации создаваемых телекоммуникационных систем и сетей	создание средств защиты информации создаваемых телекоммуникационных систем и сетей; - источники и классификация угроз; ***Уметь:*** - разрабатывать проекты технических заданий на проектирование средств защиты информации; - классифицировать и оценивать угрозы ИБ для объекта информатизации; - составлять проектную документацию на систему защиты информации. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками разработки технических заданий;	средств защиты информации; - источники и классификация угроз; - методы проектирования средств защиты информации создаваемых телекоммуникационных систем и сетей. ***Уметь:*** - разрабатывать проекты нормативно-распорядительные документов; - классифицировать и оценивать угрозы ИБ для объекта информатизации; - составлять проектную документацию на систему защиты информации. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками разработки технических заданий; - навыками разработки проектов нормативно-распорядительных документов;	создание средств защиты информации создаваемых телекоммуникационных систем и сетей; - назначение и классификация средств защиты информации; - источники и классификация угроз; - методы проектирования средств защиты информации создаваемых телекоммуникационных систем и сетей. ***Уметь:*** - разрабатывать проекты технических заданий на проектирование средств защиты информации; - разрабатывать проекты нормативно-распорядительные документов; - классифицировать и оценивать угрозы ИБ для объекта информатизации; - составлять проектную документацию на систему защиты информации. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками разработки технических заданий; - навыками разработки проектов нормативно-распорядительных документов; - навыками оценки угроз ИБ.
	ПК-1.2 Готовит техническую и проектную документацию по вопросам создания защищённых информационных систем	***Знать:*** - основные методы организационного обеспечения процесса подготовки документов, регламентирующих создание защищённых информационных систем; ***Уметь:*** - готовить проектную и техническую документацию по вопросам создания защищённых информационных систем;	***Знать:*** - организационные меры по защите информации; - нормативные правовые акты в области защиты информации. ***Уметь:*** - готовить проекты методических документов; - применять необходимые нормативные правовые акты; ***Владеть (****или* ***Иметь опыт деятельности):***	***Знать:*** - организационные меры по защите информации; - нормативные правовые акты в области защиты информации. ***Уметь:*** - готовить проектную и техническую документацию по вопросам создания защищённых информационных систем; - готовить проекты методических документов; - применять необходимые

		Владеть (*или* ***Иметь опыт деятельности):*** - навыками организации проекта;	- навыками организации проекта; - навыками подготовки необходимой технической и проектной документации;	нормативные правовые акты; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками организации проекта; - навыками подготовки необходимой технической и проектной документации;
	ПК-1.3 Сопоставляет характеристики проектируемых решений с требованиями защиты информации	***Знать:*** - характеристики проектируемых решений; ***Уметь:*** - анализировать характеристики проектируемых решений; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками составления проектируемых решений;	***Знать:*** - нормативная база, регламентирующая создание средств защиты информации; ***Уметь:*** - сопоставлять характеристики проектируемых решений с требованиями защиты информации; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками составления проектируемых решений; - навыками анализа характеристик проектируемых решений с требованиями защиты информации.	***Знать:*** - характеристики проектируемых решений; - нормативная база, регламентирующая создание средств защиты информации; ***Уметь:*** - анализировать характеристики проектируемых решений; - сопоставлять характеристики проектируемых решений с требованиями защиты информации; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками составления проектируемых решений; - навыками анализа характеристик проектируемых решений с требованиями защиты информации.
	ПК-1.4 Формирует конфигурацию и состав защищённых информационных систем	***Знать:*** - определение конфигурации; - архитектура средств контроля конфигурации; - модули ***Уметь:*** - формировать эталон конфигурации ИС; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками анализа состава защищённых информационных систем;	***Знать:*** - состав защищённых информационных систем; - архитектура средств контроля конфигурации; - модули ***Уметь:*** - считывать текущую конфигурацию и сравнивать её с эталонной; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками работы с конфигурационными файлами; - навыками работы с несколькими модулями проверки.	***Знать:*** - определение конфигурации; - состав защищённых информационных систем; - архитектура средств контроля конфигурации; - модули ***Уметь:*** - формировать эталон конфигурации ИС; - считывать текущую конфигурацию и сравнивать её с эталонной; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками анализа состава защищённых информационных систем; - навыками работы с

				конфигурационными файлами; - навыками работы с несколькими модулями проверки.
ПК-3 / осн	ПК-3.2 Разрабатывает формальные модели обработки и передачи данных в информационных системах	***Знать:*** - модели обработки и передачи данных в информационных системах; - классификация локальных вычислительных сетей; - модель OSI, протоколы ***Уметь:*** - определить вид обработки информации; - определить тип ЛВС; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками определения архитектуры ЭВМ; - навыками применения модели OSI;	***Знать:*** - виды обработки информации, классификация архитектур ЭВМ; - характеристики и назначение ИТ передачи информации; - классификация локальных вычислительных сетей; - модель OSI, протоколы ***Уметь:*** - определить архитектуру ЭВМ; - определить тип ЛВС; - разработать формальную модель обработки и передачи данных в ИС ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками применения модели OSI; - навыками использования протоколов при передаче данных.	***Знать:*** - модели обработки и передачи данных в информационных системах; - виды обработки информации, классификация архитектур ЭВМ; - характеристики и назначение ИТ передачи информации; - классификация локальных вычислительных сетей; - модель OSI, протоколы ***Уметь:*** - определить вид обработки информации; - определить архитектуру ЭВМ; - определить тип ЛВС; - разработать формальную модель обработки и передачи данных в ИС ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками определения архитектуры ЭВМ; - навыками применения модели OSI; - навыками использования протоколов при передаче данных.
	ПК-3.3 Формулирует целевые критерии для оценивания эффективности исследуемых систем	***Знать:*** - основные целевые критерии для оценки эффективности исследуемых систем; - принципы создания экспертной комиссии для проведения оценки эффективности исследуемых систем с учётом основных типов угроз нарушения: конфиденциальности, целостности, доступности информации. ***Уметь:*** - определять целевые	***Знать:*** - определение информации и её типы с точки зрения защищённости ИС; - принципы создания экспертной комиссии для проведения оценки эффективности исследуемых систем с учётом основных типов угроз нарушения: конфиденциальности, целостности, доступности информации. ***Уметь:*** - определять тип	***Знать:*** - определение информации и её типы с точки зрения защищённости ИС; - принципы создания экспертной комиссии для проведения оценки эффективности исследуемых систем с учётом основных типов угроз нарушения: конфиденциальности, целостности, доступности информации. ***Уметь:*** - определять целевые критерии для оценки эффективности

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

			средств обработки и передачи данных в информационных системах; - навыками разработки методик теоретических и экспериментальных исследований защищённости информационных систем.	методик теоретических и экспериментальных исследований защищённости информационных систем.
ПК-8 / осн	ПК-8.1 Формирует перечень угроз для защищаемой информационной системы	***Знать*** -определение угрозы защищённой ИС; -классификацию и общий анализ угроз; -отличие случайных и преднамеренных угроз; ***Уметь:*** - проводить анализ возможных угроз и каналов утечки информации; ***Владеть (или Иметь опыт деятельности):*** - навыками определения угроз для защищаемой ИС;	***Знать*** -классификацию и общий анализ угроз; -отличие случайных и преднамеренных угроз; - стек технологий обеспечения информационной безопасности. ***Уметь:*** - проводить анализ рисков; - проводить анализ, используя ГОСТ и международные стандарты; ***Владеть (или Иметь опыт деятельности):*** - навыками определения угроз для защищаемой ИС; - навыками проведения анализа рисков.	***Знать*** -определение угрозы защищённой ИС; -классификацию и общий анализ угроз; -отличие случайных и преднамеренных угроз; - стек технологий обеспечения информационной безопасности. ***Уметь:*** - проводить анализ возможных угроз и каналов утечки информации; - проводить анализ рисков; - проводить анализ, используя ГОСТ и международные стандарты; ***Владеть (или Иметь опыт деятельности):*** - навыками определения угроз для защищаемой ИС; - навыками проведения анализа рисков.
	ПК-8.2 Формирует критерии оценки каждого вида угроз в защищаемой системе	***Знать:*** - основные характеристики ИС; - классификацию угроз и критерии оценки каждого вида; ***Уметь:*** - собирать данные о самой ИС; - найти потенциальные уязвимости в ИС. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками сбора данных о самой ИС; - навыками определения потенциальных угроз;	***Знать:*** - классификацию угроз и критерии оценки каждого вида; - виды уязвимостей в ИС. ***Уметь:*** - формировать критерии каждого вида угрозы в защищаемой системе; - найти потенциальные уязвимости в ИС. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками определения потенциальных угроз;	***Знать:*** - основные характеристики ИС; - классификацию угроз и критерии оценки каждого вида; - виды уязвимостей в ИС. ***Уметь:*** - собирать данные о самой ИС; - формировать критерии каждого вида угрозы в защищаемой системе; - найти потенциальные уязвимости в ИС. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками сбора данных о самой ИС;

			- навыками выявления потенциальных уязвимостей в ИС.	- навыками определения потенциальных угроз; - навыками выявления потенциальных уязвимостей в ИС.
	ПК-8.3 Классифицирует угрозы информационной безопасности исходя из существующих и оригинальных методик	***Знать:*** - классификацию угроз информационной безопасности; - качественные и количественные методики оценки риска ИБ. ***Уметь:*** - выделять и ранжировать угрозы информационной безопасности; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками формирования списка угроз, актуальных для конкретной информационной системы	***Знать:*** - методики формирования модели угроз для информационной системы; - качественные и количественные методики оценки риска ИБ. ***Уметь:*** - определять наиболее подходящую методику для определения угрозы ИБ исходя из существующих и оригинальных методик; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками формирования списка угроз, актуальных для конкретной информационной системы - навыками правильного применения выбранной методики.	***Знать:*** - классификацию угроз информационной безопасности; - методики формирования модели угроз для информационной системы; - качественные и количественные методики оценки риска ИБ. ***Уметь:*** - выделять и ранжировать угрозы информационной безопасности; - определять наиболее подходящую методику для определения угрозы ИБ исходя из существующих и оригинальных методик; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками формирования списка угроз, актуальных для конкретной информационной системы - навыками правильного применения выбранной методики.
	ПК-8.4 Формирует перечень нарушителей информационной безопасности и их возможностей	***Знать:*** - определение нарушителя информационной безопасности; - перечень нарушителей информационной безопасности. ***Уметь:*** - определять нарушителя информационной безопасности; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками определения нарушителя информационной	***Знать:*** - модель нарушителя информационной безопасности; - перечень нарушителей информационной безопасности. ***Уметь:*** -спрогнозировать вероятных нарушителей информационной безопасности; - оценить уровень информированности потенциального нарушителя о защищаемой системе (ЗС) и возможность влияния на ЗС;	***Знать:*** - модель нарушителя информационной безопасности; - перечень нарушителей информационной безопасности. ***Уметь:*** -спрогнозировать вероятных нарушителей информационной безопасности; - оценить уровень информированности потенциального нарушителя о защищаемой системе (ЗС) и возможность влияния на ЗС; ***Владеть (****или* ***Иметь опыт деятельности):***

		безопасности;	***Владеть (или Иметь опыт деятельности):*** - навыками определения нарушителя информационной безопасности; - навыками оценки уровня информированности потенциального нарушителя.	- навыками прогнозирования вероятных нарушителей информационной безопасности; - навыками оценки уровня информированности потенциального нарушителя.

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

Таблица 7.3 – Паспорт комплекта оценочных средств

/п	Раздел (тема) дисциплины	Код контролируемой компетенции (или ее части)	Технология формирования	Оценочные средства		Описание шкал оценивания
				наименование	№ заданий	
	2	3	4	5	6	7
1.	Основные аспекты построения системы информационной безопасности	ПК-1 ПК-3 ПК-8	Лекция, СРС, практическая работа	ВС, БТЗ	1-8, 1-20	Согласно табл. 7.2
2.	Угрозы информационной безопасности, оценка риска их возникновения	ПК-3 ПК-8	Лекция, СРС,	ВС, БТЗ, КВЗЛР	9-18, 2 1-40, 1-4	Согласно табл. 7.2
3.	Персональные данные, защита авторских прав	ПК-1 ПК-8	Лекция, СРС,	ВС КВЗЛР	2 1-26 1-4	Согласно табл. 7.2
4.	Выявление контрафактной	ПК-1	Лекция, СРС	ВС	2 7-34	Согласно табл. 7.2

	продукции	ПК-3		КВЗЛР	1-4	
5.	Криптографические методы защиты	ПК-1 ПК-3 ПК-8	Лекция, СРС, практическая работа	ВС КВЗПР	3 5-41 1-4	Согласно табл. 7.2
6.	Методы выбора системы защиты информации	ПК-1 ПК-3 ПК-8	Лекция, СРС, практическая работа	ВС БТЗ	4 1-48 4 1-50	Согласно табл. 7.2

ВС- вопросы для собеседования
БТЗ – банк тестовых заданий
КВЗПР- контрольные вопросы для защиты практической работы
КВЗЛР- контрольные вопросы для защиты лабораторной работы

Примеры типовых контрольных заданий для проведения текущего контроля успеваемости

Вопросы для собеседования

Критерии оценки безопасности информационных технологий.

1. Опишите иерархию сущностей в "Критериях оценки безопасности информационных технологий".
2. Назовите основные термины, описанные в "Критериях оценки безопасности информационных технологий".
3. Опишите структуру класса «приватность».
4. Опишите структуру класса «использование ресурсов».
5. Что такое требования доверия безопасности и для чего они нужны?
6. Что такое уровни доверия?
7. Какие существуют механизмы обеспечения безопасности в распределённых системах?

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.

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.

$$ci = (27i+n) \bmod 5 + 3i$$

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
Основные аспекты построения системы информационной безопасности	4	Выполнил, но «не защитил»	6	Выполнил и «защитил»
Угрозы информационной безопасности, оценка риска их возникновения	4	Выполнил, но «не защитил»	6	Выполнил и «защитил»
Персональные данные, защита авторских прав	4	Выполнил, но «не защитил»	6	Выполнил и «защитил»
Выявление контрафактной продукции	4	Выполнил, но «не защитил»	6	Выполнил и «защитил»
Криптографические методы защиты	4	Выполнил, но «не защитил»	6	Выполнил и «защитил»
Методы выбора системы защиты информации	4	Выполнил, но «не защитил»	6	Выполнил и «защитил»
СРС	0		6	
Компетентностные задачи	0		6	
ИТОГО	24		48	
Посещаемость	0		16	
Экзамен	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

Основная литература

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

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

Дополнительная литература

1) Марухленко, А. Л. Разработка защищённых интерфейсов Web-приложений : учебное пособие : [16+] / А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов. – Москва ; Берлин : Директ-Медиа, 2021. – 175 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=599050 (дата обращения: 07.09.2021). – Библиогр. в кн. – ISBN 978-5-4499-1676-1. – DOI 10.23681/599050. – Текст : электронный.

2) Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства. Москва: ДМК Пресс, 2010.- 544 с. (полнотекстовый доступ в базе Iqlib.ru)

3) Грибунин В.Г., Чудовский В.В. Комплексная система защиты информации на предприятии: учеб. пособие для студ. высш. учеб. заведений. – М.: Издательский дом «Академия», 2009. – 416 с.

4) Мельников В.П., Клейменов С.А., Петракова А.М. Информационная безопасность и защита информации: учеб. пособие для студ. учреждений высш. проф. образования. – 6-е изд., стер. – М.: Издательский центр «Академия», 2012. – 336 с.

Перечень методических указаний

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

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

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

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

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

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

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

8) Критерии оценки и выбора CASE-средств [Электронный ресурс] : методические указания для практических занятий и самостоятельной работы для студентов специальностей УГСНП 10.00.00 Информационная безпасность / Юго-Зап. гос. ун-т; сост.: А. Л. Марухленко Курск, 2017. 10 с. Библиогр.: с. 10

9) 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. - Электрон. текстовые дан. (324 КБ). - Курск : ЮЗГУ, 2017. - 7 с. : ил., табл. - Библиогр.: с. 7. - Б. ц.

9. Перечень ресурсов информационно-телекоммуникационной сети Интернет

1) Облачный сервис математических вычислений SMath Studio in the Cloud [официальный сайт]. Режим доступа: https://ru.smath.com/cloud/

2) Электронно-библиотечная система «Университетская библиотека онлайн» Режим доступа: http://biblioclub.ru
3) Научно-информационный портал ВИНИТИ РАН [официальный сайт]. Режим доступа: http://www.consultant.ru/
4) Общероссийский портал Math-Net.Ru [официальный сайт]. Режим доступа: http://www.mathnet.ru/
5) База данных "Патенты России"

10 Методические указания для обучающихся по освоению дисциплины

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