Аннотация к рабочей программе дисциплины «Основы информационной безопасности»

Цель преподавания дисциплины

Целью преподавания дисциплины «Основы информационной безопасности» изучается с целью ознакомления студентов с современным состоянием теории безопасности информационных систем, правовым регулированием в области защиты информации, принципами, алгоритмами и методами организации защиты информации в организациях и предприятиях различных направлений деятельности и различных форм собственности.

Задачи изучения дисциплины

– Ознакомление с принципами, базовыми определениями и вариантами организации защиты информации;

– Ознакомление с актуальной нормативно-правовой базой РФ по части информационной безопасности;

– Изучение угроз информационной безопасности, моделей поведения злоумышленника, основ работы с конфиденциальными данными;

– Ознакомление с основами защиты авторских прав, работы с персональными данными;

– Изучение способов выявления контрафактной продукции;

– Изучение, в том числе на практическом уровне, основ криптографических преобразований в части потоковых шифров, ассиметричных систем и перспективных методов защиты.

– Ознакомление с технологиями защиты программного обеспечения.

Индикаторы компетенций, формируемые в результате освоения дисциплины

ОПК-1.1 Классифицирует угрозы информационной безопасности в соответствии с нормативными документами

ОПК-1.2 Оценивает угрозы информационной безопасности с точки зрения основных концепций национальной безопасности Российской Федерации

ОПК-1.3 Определяет угрозы информационной безопасности для различных систем

Разделы дисциплины

Базовые понятия. Конфиденциальность. Классификация угроз. Угрозы ИБ. Классы нарушителей. Оценка риска. Персональные данные. Защита авторских прав. Выявление контрафактной продукции. Криптографические методы защиты.

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

Основы информационной безопасности
(наименование дисциплины)

ОПОП ВО 10.03.01 Информационная безопасность
шифр и наименование направление подготовки (специальности)

Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий
наименование направленности (профиля, специализации)

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

Курск – 2021

Рабочая программа дисциплины «Основы информационной безопасности» составлена в соответствии с ФГОС ВО – бакалавриат по направлению подготовки 10.03.01 Информационная безопасность на основании учебного плана ОПОП ВО 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий», 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 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий)» 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 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий», одобренного Ученым советом университета протокол № 4 «28» 02 2022 г., на заседании кафедры ИБ Протокол №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 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий», 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 «Основы информационной безопасности» изучается с целью ознакомления студентов с современным состоянием теории безопасности информационных систем, правовым регулированием в области защиты информации, принципами, алгоритмами и методами организации защиты информации в организациях и предприятиях различных направлений деятельности и различных форм собственности.

1.2. Задачи 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, закрепл. за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленной за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код	*наименование*		

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*		
ОПК-1	Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;;	ОПК-1.1 Классифицирует угрозы информационной безопасности в соответствии с нормативными документами	***Знать:*** - основные угрозы информационной безопасности; - возможные каналы утечки конфиденциальной информации; - нормативно-правовые аспекты обеспечения информационной безопасности РФ; ***Уметь:*** ***- выявлять угрозы информационной безопасности;*** - снижать вероятность отрицательных последствий сетевого взаимодействия; - классифицировать угрозы информационной безопасности; - ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками классификации угроз ; - навыками выявления уязвимостей технических каналов связи информационных систем.
		ОПК-1.2 Оценивает угрозы информационной безопасности с точки зрения основных концепций национальной безопасности Российской Федерации	***Знать:*** - концепцию национальной безопасности РФ; - технологии повышения защищенности распределенных информационных систем; - административную, уголовную, гражданско-правовую ответственность. - основы криптографии, методы защиты. ***Уметь:*** - выполнять определять характер угрозы и масштабы последствий; - минимизировать последствия ущерба за счет интеграции средств защиты. - выполнять шифрование криптографическими методами; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками оценки угроз ИБ с точки зрения нормативно-правового обеспечения; - навыками ранжирования угроз с учетом масштаба возможных последствий;
		ОПК-1.3	***Знать:***

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*		
		Определяет угрозы информационной безопасности для различных систем	- основы работы в режиме пошаговой отладки передачи конфиденциальных данных в информационной системе; - особенности вывода промежуточных значений в ходе работы отдельных модулей информационных систем; - основы использования средств защиты информации. ***Уметь:*** - выполнять выявление контрафактной продукции; - организовать безопасную работу в Интернет; - 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; - технологией ведения протокола работы системы с выводом промежуточных результатов обработки данных. - навыками оценки защищенности информационной системы с учетом возможных угроз. - выполнять шифрование криптографическими методами; - определять целесообразность применения тех или иных методов защиты;

2 Указание места дисциплины в структуре основной профессиональной образовательной программы

Дисциплина «Основы информационной безопасности» входит в обязательную часть блока 1 «Дисциплины (модули)») основной профессиональной образовательной программы – специалитет по

специальности 10.05.02 Информационная безопасность телекоммуникационных систем. Дисциплина изучается на 1 курсе во 2 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)	54.1
в том числе:	
лекции	36
лабораторные занятия	0
практические занятия	18
Самостоятельная работа обучающихся (всего)	53.9
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.	Базовые понятия	Термины и определения. Информация как предмет защиты. Субъекты информационных отношений. Организация системы защиты информации. Комплексная защита информационных систем
2.	Конфиденциальность. Классификация угроз	Работа с конфиденциальными данными. Угрозы информационной безопасности. Модель поведения

		нарушителя. Классификация угроз
3.	Угрозы ИБ. Классы нарушителей. Оценка риска	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
4.	Персональные данные. Защита авторских прав	Обработка персональных данных. Защита интеллектуальной собственности. Авторское право. Гражданско-правовая ответственность. Административная ответственность. Уголовная ответственность
5.	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.
6.	Криптографические методы защиты	Основы криптографии, методы защиты. Классификация криптографических методов. Потоковые шифры. Скремблирование. Ассиметричные шифры. Клеточные автоматы

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., час	№ лб.	№ пр.			
1	2	3	4	5	6	7	8
1.	Базовые понятия	4			У-1-3 Д-1-3	С,Т (1-2)	ОПК-1.1
2.	Конфиденциальность. Классификация угроз	4			У-1-3	С,Т (2-4)	ОПК-1.1
3.	Угрозы ИБ. Классы нарушителей. Оценка риска	4			У-1-3	С, Т (4-6)	ОПК-1.2
4.	Персональные данные. Защита авторских прав	4			У-1-4 МО 5	С, Т (6-8)	ОПК-1.2
5.	Выявление контрафактной продукции	4			У-1-4 МО	С, Т (9-13)	ОПК-1.2

					1,2,3		
6.	Криптографические методы защиты	16		18	У-1-4 МО 1-9	С ,Т (6-18)	ОПК-1.3
	Всего	36	0	18			

С – собеседование, Т – тест, Кейс-задача ЗКР – защита курсовой работы, Р- реферат, ККР – контроль выполнения этапов курсовой работы

4.2 Лабораторные работы и практические занятия

4.2.1 Практические работы

Таблица 4.2.1 – Практические работы

№	Наименование	Объем, час.
1.	Анализ защищенности вычислительной системы	2
2.	Шифры полиалфавитной замены	2
3.	Потоковые шифры. Скремблирование бинарного потока данных	4
4.	Ассиметричные клиптоалгоритмы. Метод RSA	4
5.	Обработка на базе клеточных автоматов	4
6.	Интеграция механизмов защиты в программное обеспечение	2
Итого		18

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.	Базовые понятия	1-2 недели	4
2.	Конфиденциальность. Классификация угроз	2-3 недели	6
3.	Угрозы ИБ. Классы нарушителей. Оценка риска	3-8 недели	8
4.	Персональные данные. Защита авторских прав	7-9 недели	4

5.	Выявление контрафактной продукции	9-12 недели	6
6.	Криптографические методы защиты	6-18 недели	25.9
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 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.	Угрозы ИБ. Классы нарушителей. Оценка риска (к выполнению работы №1 «Анализ защищенности вычислительной системы»)	Интерактивная лекция, выполнение студентами анализа защищенности информационных систем с использованием прикладных решений, в том числе через Интернет	2
2.	Криптографические методы защиты (к выполнению работы №3 «Потоковые шифры. Скремблирование бинарного потока данных»)	Интерактивная лекция, выполнение студентами интерактивных заданий по преобразованию потока данных с применением на битовом уровне	2
3.	Криптографические методы защиты (к выполнению работы №4 «Ассиметричные клиптоалгоритмы. Метод RSA»)	Интерактивная лекция, выполнение студентом интерактивной проверки результатов обработки на выделенном портале верификации.	2
4.	Криптографические методы защиты (к выполнению работы №5 «Обработка на базе клеточных автоматов»)	Интерактивная лекция, выполнение студентом интерактивной проверки результатов обработки на выделенном портале верификации.	2
	Итого		8

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
ОПК-1 Способен оценивать роль информации, информационных	Учебная ознакомительная практика		Подготовка к процедуре защиты и защита выпускной

технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;		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 комп/ 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»)
ОПК-1/ основной	ОПК-1.1 Классифицирует угрозы информационной безопасности в соответствии с нормативными документами	***Знать:*** - основные угрозы информационной безопасности; ***Уметь:*** - выявлять угрозы информационной безопасности; - классифицировать угрозы информационной безопасности; - ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками выявления уязвимостей технических каналов связи информационных систем.	***Знать:*** - основные угрозы информационной безопасности; - возможные каналы утечки конфиденциальной информации; ***Уметь:*** - выявлять угрозы информационной безопасности; - снижать вероятность отрицательных последствий сетевого взаимодействия; - классифицировать угрозы информационной безопасности; - ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками классификации угроз ;	***Знать:*** - возможные каналы утечки конфиденциальной информации; - нормативно-правовые аспекты обеспечения информационной безопасности РФ; ***Уметь:*** ***- выявлять угрозы информационной безопасности;*** - снижать вероятность отрицательных последствий сетевого взаимодействия; - классифицировать угрозы информационной безопасности; - ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками классификации угроз ; - навыками выявления уязвимостей технических каналов связи информационных систем.
	ОПК-1.2 Оценивает угрозы информационной безопасности с	***Знать:*** - концепцию национальной безопасности РФ; - административную,	***Знать:*** - технологии повышения защищенности распределенных информационных	**Знать:** - концепцию национальной безопасности РФ; - технологии повышения защищенности

Код комп/ 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»)
	точки зрения основных концепций национальной безопасности Российской Федерации	уголовную, гражданско-правовую ответственность. ***Уметь:*** - минимизировать последствия ущерба за счет интеграции средств защиты. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками ранжирования угроз с учетом масштаба возможных последствий;	систем; ***Уметь:*** - выполнять определять характер угрозы и масштабы последствий; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками ранжирования угроз с учетом масштаба возможных последствий;	распределенных информационных систем; - административную, уголовную, гражданско-правовую ответственность. - основы криптографии, методы защиты. **Уметь:** - выполнять определять характер угрозы и масштабы последствий; - минимизировать последствия ущерба за счет интеграции средств защиты. - выполнять шифрование криптографическими методами; **Владеть (или Иметь опыт деятельности):** - навыками оценки угроз ИБ с точки зрения нормативно-правового обеспечения; - навыками ранжирования угроз с учетом масштаба возможных последствий;
	ОПК-1.3 Определяет угрозы информационной безопасности для различных систем	***Знать:*** - основы работы в режиме пошаговой отладки передачи конфиденциальных данных в информационной системе; ***Уметь:*** - выполнять выявление контрафактной продукции; - выводить сообщения в случае возникновения нештатных ситуаций работы информационной системы; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками установки	***Знать:*** - особенности вывода промежуточных значений в ходе работы отдельных модулей информационных систем; - основы использования средств защиты информации. ***Уметь:*** - организовать безопасную работу в Интернет; - выводить сообщения в случае возникновения нештатных ситуаций работы информационной системы; - интегрировать средства защиты на программном уровне. ***Владеть (****или* ***Иметь***	***Знать:*** - основы работы в режиме пошаговой отладки передачи конфиденциальных данных в информационной системе; - особенности вывода промежуточных значений в ходе работы отдельных модулей информационных систем; - основы использования средств защиты информации. **Уметь**: - выполнять выявление контрафактной продукции; - организовать безопасную работу в Интернет; - выводить сообщения в случае возникновения нештатных ситуаций работы информационной

Код комп/ 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»)
		программных средств защиты; - навыками оценки защищенности информационной системы с учетом возможных угроз.	***опыт деятельности):*** - навыками установки программных средств защиты; - навыками оценки защищенности информационной системы с учетом возможных угроз.	системы; - интегрировать средства защиты на программном уровне. **Владеть (или Иметь опыт деятельности):** - навыками установки программных средств защиты; - технологией ведения протокола работы системы с выводом промежуточных результатов обработки данных. - навыками оценки защищенности информационной системы с учетом возможных угроз. - выполнять шифрование криптографическими методами; - определять целесообразность применения тех или иных методов защиты;

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

Таблица 7.3 – Паспорт комплекта оценочных средств для текущего контроля успеваемости

п/п	Раздел (тема) дисциплины	Код контролируемой компе-тенции (или её части)	Технология формирования	Оценочные средства		Описание шкал оценивания
				наим	№№ заданий	
1	2	3	4	5	6	7

1.	Базовые понятия	УК-1 ОПК-1	Лекция, СРС	Собеседование,	1-5	Согласно табл.7.2
				Тест	1-25	
2.	Конфиденциальность. Классификация угроз	УК-1 ОПК-1	Лекция, СРС	Собеседование,	1-5	Согласно табл.7.2
				Тест	1-24	
3.	Угрозы ИБ. Классы нарушителей. Оценка риска	ОПК-1	Лекция, СРС	Собеседование,	1-5	Согласно табл.7.2
				Тест	1-5	
4.	Персональные данные. Защита авторских прав	ОПК-1	Лекция, СРС	Собеседование,	1-5	Согласно табл.7.2
				Тест	1-5	
5.	Выявление контрафактной продукции	ОПК-1	Лекция, СРС, практические работы	Собеседование,	1-5	Согласно табл.7.2
				Тест	1-5	
6.	Криптографические методы защиты	ОПК-1	Лекция, СРС	Собеседование, тест	1-42	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 работы №1 Анализ защищенности вычислительной системы	2	Выполнил, но «не защитил»	1	Выполнил и «защитил»
Выполнение работы №2 Шифры полиалфавитной замены	2	Выполнил, но «не защитил»	2	Выполнил и «защитил»
Выполнение работы №3 Потоковые шифры. Скремблирование бинарного потока данных	2	Выполнил, но «не защитил»	5	Выполнил и «защитил»
Выполнение работы №4 Ассиметричные клиптоалгоритмы. Метод RSA	4	Выполнил, но «не защитил»	8	Выполнил и «защитил»
Выполнение работы №5 Обработка на базе клеточных автоматов	10	Выполнил, но «не защитил»	10	Выполнил и «защитил»
Выполнение работы №6 Интеграция механизмов защиты в программное обеспечение	4	Выполнил, но «не защитил»	4	Выполнил и «защитил»
СРС	0		12	
Кейс-задачи	0		6	
ИТОГО	24		48	
Посещаемость	0		16	
Зачет	0		36	
ИТОГО	24		100	

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

Каждый верный ответ оценивается следующим образом:

- задание в закрытой форме –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) 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

3) 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: электронный

4) Ищейнов, Вячеслав Яковлевич. Защита конфиденциальной информации [Текст] : учебное пособие / В. Я. Ищейнов, М. В. Мецатунян. - Москва : Форум, 2013. - 256 с.

8.2 Дополнительная литература

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

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

3) Спицын, В. Г. Информационная безопасность вычислительной техники : учебное пособие : [16+] / В. Г. Спицын ; Томский Государственный

университет систем управления и радиоэлектроники (ТУСУР). – Томск : Эль Контент, 2011. – 148 с. – URL: https://biblioclub.ru/index.php?page=book&id=208694 (дата обращения: 07.09.2021). – Режим доступа: по подписке. – Текст : электронный.

8.3 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 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.

4) Исследование атаки переполнения буфера как примера безопасности нарушения конфиденциальности, целостности и доступности информации : 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. - 10 с. - Текст : электронный.

5) Причины, виды, каналы утечки и искажения информации : 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. - 11 с. - Текст : электронный.

6) Защита от утечек по каналу ПЭМИН, по акустическому и виброакустическому каналам : 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.

7) Сетевое сканирование : 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.

8) Анализ трафика и сбор критичной информации программами пассивного анализа : 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. - 6 с. - Текст : электронный.

9) Аудит комплексной защиты информации предприятия : 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.

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).