МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение высшего образования
«Национальный исследовательский технологический университет «МИСИС»

Рабочая программа дисциплины (модуля)

Современные технологии защиты информации

Закреплена за подразделением — Кафедра инфокоммуникационных технологий

Направление подготовки — 09.04.03 ПРИКЛАДНАЯ ИНФОРМАТИКА

Профиль — Прикладная информатика в цифровой экономике

Квалификация **Магистр**
Форма обучения **очная**
Общая трудоемкость **3 ЗЕТ**

Часов по учебному плану 108
в том числе:
аудиторные занятия 34
самостоятельная работа 74

Формы контроля в семестрах:
зачет 1

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	1 (1.1)		Итого	
Недель	18			
Вид занятий	УП	РП	УП	РП
Лекции	9	9	9	9
Практические	25	25	25	25
Итого ауд.	34	34	34	34
Контактная работа	34	34	34	34
Сам. работа	74	74	74	74
Итого	108	108	108	108

Программу составил(и):
Старший преподаватель, Бахаров Леонид Ефимович

Рабочая программа
Современные технологии защиты информации

Разработана в соответствии с ОС ВО:

Самостоятельно устанавливаемый образовательный стандарт высшего образования - магистратура Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский технологический университет «МИСиС» по направлению подготовки 09.04.03 ПРИКЛАДНАЯ ИНФОРМАТИКА (приказ от 05.03.2020 г. № 95 о.в.)

Составлена на основании учебного плана:

09.04.03 Прикладная информатика, 09.04.03-МПИ-23-2.plx Прикладная информатика в цифровой экономике, утвержденного Ученым советом НИТУ МИСИС в составе соответствующей ОПОП ВО 22.06.2023, протокол № 5-23

Утверждена в составе ОПОП ВО:

09.04.03 Прикладная информатика, Прикладная информатика в цифровой экономике, утвержденной Ученым советом НИТУ МИСИС 22.06.2023, протокол № 5-23

Рабочая программа одобрена на заседании
Кафедра инфокоммуникационных технологий

Протокол от 12.04.2023 г., №9

Руководитель подразделения Кузнецова Ксения Александровна

1. ЦЕЛИ ОСВОЕНИЯ	
1.1	Целью освоения дисциплины является обучение студентов методам обеспечения защиты информации в современных информационных системах (ИС), функционирующих в условиях внешних и внутренних угроз информационной безопасности. Это даст возможность будущему магистру глубоко понимать функционирование механизмов защиты информации в современных ИС, а также решать вопросы формирования политики безопасности, возникающие в ходе проектирования и эксплуатации перспективных ИС. Студенты будут уметь выбирать необходимые протоколы безопасности и предлагать современные методы защиты от новых угроз информационной безопасности; применять методы защиты цифрового контента от угроз модификации и несанкционированного использования при построении ИС; разрабатывать методики построения программной и аппаратной реализации защиты корпоративной сети с учетом применения облачных технологий; моделировать работу алгоритмов защиты информации на базе математического аппарата динамических дискретных систем; анализировать риски функционирования систем защиты информации.

2. МЕСТО В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Блок ОП:	Б1.О
2.1	**Требования к предварительной подготовке обучающегося:**
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Методология моделирования и совершенствования бизнес-процессов предприятия
2.2.2	Проектно-продуктовая трансформация в корпоративных информационных системах
2.2.3	Производственная практика по получению профессиональных умений и опыта профессиональной деятельности
2.2.4	Управление инновационными и инвестиционными проектами в сфере ИКТ
2.2.5	Экономика информационных систем
2.2.6	Подготовка к процедуре защиты и защита выпускной квалификационной работы
2.2.7	Роботизация бизнес-процессов (RPA)

3. РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫЕ С ФОРМИРУЕМЫМИ КОМПЕТЕНЦИЯМИ
ПК-3: Способен проводить анализ и реинжиниринг бизнес-процессов, осуществлять проектирование и поддержку архитектуры и прототив ИС
Знать:
ПК-3-З1 Основные методики анализа рисков информационной безопасности на предприятии
ПК-3-З3 Типовые программно-аппаратные средства и системы защиты информации от несанкционированного доступа в компьютерную среду; виды угроз информационных систем и методы обеспечения информационной безопасности; принципы обеспечения информационной безопасности управления предприятием; принципы защиты информации и обеспечения информационной безопасности, сведения об основных угрозах информационной безопасности и их источниках
ПК-3-З2 Методы моделирования поведения нарушителя информационной безопасности. Принципы построения и функционирования сетей Петри
ОПК-5: Способен разрабатывать и модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем
Знать:
ОПК-5-З2 Основные квантово-механические принципы, лежащие в основе построения квантовых систем защиты информации
ОПК-5-З1 Современные методы криптографической и стеганографической защиты информации
ОПК-5-З3 Методы защиты программного обеспечения от угроз информационной безопасности, методы защиты авторских прав на цифровой контент
ПК-3: Способен проводить анализ и реинжиниринг бизнес-процессов, осуществлять проектирование и поддержку архитектуры и прототив ИС
Уметь:
ПК-3-У2 Анализировать угрозы информационной безопасности и уязвимости систем защиты информации, строить модель информационной безопасности с полным перекрытием угроз
ПК-3-У1 Использовать концепцию управления рисками при анализе защищенности инфокоммуникационной структуры предприятия
ОПК-5: Способен разрабатывать и модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем
Уметь:

ОПК-5-У2 Производить расчет критической длины линии связи при PNS-атаке на квантовый канал
ОПК-5-У1 Применять простейшие методы шифрования и дешифрования текстовой информации, использовать протоколы разделения и разбиения секрета
ПК-3: Способен проводить анализ и реинжиниринг бизнес-процессов, осуществлять проектирование и поддержку архитектуры и прототив ИС
Уметь:
ПК-3-У3 Применять методы Парето-оптимизации в системе поддержки принятия решений в области проектирования системы защиты информации на предприятии
ОПК-5: Способен разрабатывать и модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем
Уметь:
ОПК-5-У3 Производить встраивание цифровых водяных знаков в мультимедийные и программные файлы
ПК-3: Способен проводить анализ и реинжиниринг бизнес-процессов, осуществлять проектирование и поддержку архитектуры и прототив ИС
Владеть:
ПК-3-В1 Методикой анализа рисков информационной безопасности при построении системы защиты информации
ОПК-5: Способен разрабатывать и модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем
Владеть:
ОПК-5-В1 Методикой генерации псевдослучайных последовательностей для дальнейшего использования в криптографических алгоритмах

4. СТРУКТУРА И СОДЕРЖАНИЕ

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Формируемые индикаторы компетенций	Литература и эл. ресурсы	Примечание	КМ	Выполняемые работы
	Раздел 1. Криптографическая защита информации							
1.1	Проблемы современной криптографии /Лек/	1	2	ОПК-5-З1	Л1.4 Л1.5 Л1.7Л2.3Л3.4 Э1			
1.2	Изучение протоколов разбиения секрета. Выполнение раздела 1 практической работы 1. /Пр/	1	2	ОПК-5-У1	Л1.4 Л1.5 Л1.7Л2.3Л3.4 Э1			
1.3	Изучение протоколов разделения секрета. Выполнение раздела 2 практической работы 1. /Пр/	1	1	ОПК-5-У1	Л1.4 Л1.5 Л1.7Л2.3Л3.4 Э1			
1.4	Подготовка к защите практической работы № 1 /Ср/	1	6	ОПК-5-З1 ОПК-5-У1	Л1.4 Л1.5 Л1.7Л2.3Л3.4 Э1			
1.5	Практическая работа № 2. Изучение шифра Плейфера /Пр/	1	2	ОПК-5-У1	Л1.4 Л1.5 Л1.7Л2.3Л3.4 Э1			Р2
1.6	Подготовка к защите практической работы № 2 /Ср/	1	6	ОПК-5-З1 ОПК-5-У1	Л1.4 Л1.5 Л1.7Л2.3Л3.4 Э1			
1.7	Практическая работа № 3. Дешифрование шифра простой перестановки при помощи метода биграмм /Пр/	1	2	ОПК-5-У1	Л1.4 Л1.5 Л1.7Л2.3Л3.4 Э1			Р3

1.8	Подготовка к защите практической работы № 3 /Ср/	1	6	ОПК-5-З1 ОПК-5-У1	Л1.4 Л1.5 Л1.7Л2.3Л3.4 Э1			
1.9	Практическая работа № 4. Изучение регистров сдвига с линейной обратной связью как генераторов псевдослучайных чисел /Пр/	1	2	ОПК-5-В1	Л1.5Л2.1Л3.4 Э1			Р4
1.10	Подготовка к защите практической работы № 4 /Ср/	1	6	ОПК-5-З1 ОПК-5-В1	Л1.5Л2.1Л3.4 Э1			
	Раздел 2. Моделирование систем защиты информации							
2.1	Риск-ориентированный подход в системах защиты информации /Лек/	1	2	ПК-3-З1	Л1.6Л2.7Л3.2 Э1			
2.2	Обзор методик анализа рисков информационной безопасности /Лек/	1	1	ПК-3-З1	Л1.6Л2.7Л3.2 Э1			
2.3	Практическая работа № 5. Изучение модели информационной безопасности с полным перекрытием угроз /Пр/	1	2	ПК-3-У2	Л1.6Л2.8Л3.2 Э1 Э2			Р5
2.4	Подготовка к защите практической работы № 5 /Ср/	1	6	ПК-3-З1 ПК-3-У2	Л1.6Л2.8Л3.2 Э1			
2.5	Практическая работа № 6. Анализ рисков информационной безопасности /Пр/	1	2	ПК-3-У1 ПК-3-В1	Л1.6Л2.7Л3.2 Э1 Э2			Р6
2.6	Подготовка к защите практической работы № 6 /Ср/	1	6	ПК-3-З1 ПК-3-З3 ПК-3-У1	Л1.6Л2.7Л3.2 Э1			
2.7	Практическая работа № 7. Изучение системы поддержки принятия решений в области проектирования системы защиты информации на предприятии /Пр/	1	2	ПК-3-У3	Л1.6Л2.4 Л2.5Л3.5 Э1			Р7
2.8	Подготовка к защите практической работы № 7 /Ср/	1	6	ПК-3-З3 ПК-3-У3	Л1.6Л2.4 Л2.5Л3.5 Э1			
2.9	Практическая работа № 8. Разработка сценариев действий нарушителя информационной безопасности с использованием сети Петри /Пр/	1	2	ПК-3-У1	Л1.6Л2.8Л3.2 Э1 Э2			Р8
2.10	Подготовка к защите практической работы № 8 /Ср/	1	6	ПК-3-З2 ПК-3-У1	Л1.6Л2.8Л3.2 Э1			
	Раздел 3. Защита цифрового контента от угроз информационной безопасности							

3.1	Технологии защиты электронного документооборота /Лек/	1	2	ОПК-5-З3	Л1.1 Л1.3Л2.2Л3. 1 Л3.4 Э1			
3.2	Практическая работа № 9. Защита программного обеспечения методами стеганографии /Пр/	1	2	ОПК-5-У3	Л1.1 Л1.3Л2.2Л3. 1 Л3.4 Э1			Р9
3.3	Подготовка к защите практической работы № 9 /Ср/	1	7	ОПК-5-З3 ОПК-5-У3	Л1.1 Л1.3Л2.2Л3. 1 Л3.4 Э1			
3.4	Практическая работа № 10. Защита электронных документов с использованием цифровых водяных знаков /Пр/	1	2	ОПК-5-У3	Л1.1 Л1.3Л2.2Л3. 1 Л3.4 Э1			Р10
3.5	Подготовка к защите практической работы № 10 /Ср/	1	6	ОПК-5-З3 ОПК-5-У3	Л1.1 Л1.3Л2.2Л3. 1 Л3.4 Э1			
3.6	Практическая работа № 11. Стегокомплексы, допускающие использование аудиоконтейнеров /Пр/	1	2	ОПК-5-У3	Л1.1 Л1.3Л2.2Л3. 1 Л3.4 Э1			Р11
3.7	Подготовка к защите практической работы № 11 /Ср/	1	6	ОПК-5-З3 ОПК-5-У3	Л1.1 Л1.3Л2.2Л3. 1 Л3.4 Э1			
	Раздел 4. Квантовые технологии защиты информации							
4.1	Квантовая криптография и перспективы квантовых технологий защиты информации /Лек/	1	2	ОПК-5-З2	Л1.2Л2.6Л3. 3 Э1			
4.2	Практическая работа № 12. Расчет критической длины линии связи при PNS-атаке на квантовый канал /Пр/	1	2	ОПК-5-У2	Л1.2Л2.6Л3. 3 Э1			Р12
4.3	Подготовка к защите практической работы № 12 /Ср/	1	7	ОПК-5-З2 ОПК-5-У2	Л1.2Л2.6Л3. 3 Э1			

5. ФОНД ОЦЕНОЧНЫХ МАТЕРИАЛОВ

5.1. Контрольные мероприятия (контрольная работа, тест, коллоквиум, экзамен и т.п), вопросы для самостоятельной подготовки

Код КМ	Контрольное мероприятие	Проверяемые индикаторы компетенций	Вопросы для подготовки
КМ1	Защита практической работы № 1.	ОПК-5-З1;ОПК-5-У1	Для чего необходимо применение шифрования с открытым ключом в тайных многосторонних вычислениях? Как происходит генерация ключей в алгоритме RSA? Что означает (m, n)–пороговая схема разделения секрета. Назначение интерполяционного полинома Лагранжа. Сущность китайской теоремы об остатках. Чем отличается разбиение секрета от разделения секрета? Чем отличается разбиение секрета от тайных многосторонних вычислений?

КМ2	Защита практической работы № 2.	ОПК-5-З1;ОПК-5-У1	К какому классу шифров относится шифр Плейфера? Укажите особенности подобных шифров. Опишите процедуры шифрования и расшифрования по методу Плейфера. Оцените криптостойкость изученного метода шифрования и возможности использования подобных методов в современных криптосистемах. Зашифруйте свою фамилию шифром Плейфера вручную. Сравните результаты ручного шифрования и полученные с помощью программы Playfair.exe.
КМ3	Защита практической работы № 3.	ОПК-5-З1;ОПК-5-У1	В чем заключается описанный в работе метод вскрытия криптограмм? В чем заключается метод шифрования (расшифрования) с использованием перестановок? Какие перестановочные методы шифрования вы знаете? Приведите примеры использования алгоритма перестановки в современных симметричных криптосистемах. Какие требования к исходным текстам и длинам ключей шифрования обеспечат максимальный эффект для использования изученного метода дешифрования?
КМ4	Защита практической работы № 4.	ОПК-5-З1;ОПК-5-В1	Что такое М-последовательность? Каковы ее свойства? Какая отводная последовательность позволяет ее получить? Опишите процесс работы четырехбитового РгСсЛОС: откуда берется выходной бит и как формируется псевдослучайная последовательность, как происходит сдвиг регистра, как меняется его состояние, как образуется бит функции обратной связи (приведите таблицу истинности для операции XOR от 1, 2, 3, 4 переменных) Что определяет свойство периодичности РгСсЛОС? От чего зависит период РгСсЛОС? Какие многочлены являются неприводимыми по модулю 2? Где и для чего их можно применять на практике? Что входит в понятие «Линейная сложность бинарной последовательности»? Как ее можно использовать для оценки псевдослучайной бинарной последовательности? Что определяет свойство периодичности РгСсЛОС? От чего зависит период РгСсЛОС? Что такое отводная последовательность? Для чего она нужна в РгСсЛОС и на какие его параметры влияет? Что такое инициальное состояние РгСсЛОС? Какие есть ограничения на значение инициального состояния? Почему? Что такое ГСПЧ? На чем они могут быть основаны? Какие у них преимущества и недостатки?
КМ5	Защита практической работы № 5.	ПК-3-У2;ПК-3-З1	Что такое угроза информационной безопасности? Приведите примеры. Каким образом могут быть классифицированы угрозы информационной безопасности? Что такое уязвимость и чем она отличается от угрозы? Каким образом может быть проведена классификация уязвимостей? Какие модели защиты информации Вы знаете? Какие предположения лежат в основе модели с полным перекрытием угроз? Назовите преимущества и недостатки модели с полным перекрытием угроз.

КМ6	Защита практической работы № 6.	ПК-3-З1;ПК-3-З3;ПК-3-У1;ПК-3-У2;ПК-3-В1	Какая информация должна быть собрана на объекте оценки для проведения анализа информационных рисков? В каких единицах измеряется риск информационной безопасности? Выберите оптимальную стратегию управления рисками в следующем случае: веб-сервер компании находится внутри корпоративной сети и его программное обеспечеие, возможно, содержит уязвимости. Какую информацию необходимо получить на объекте оценки для определения ущерба по угрозе «нарушение целостности информации»? Какую информацию необходимо получить на объекте оценки для определения ущерба по угрозе «нарушение конфиденциальности информации»? В случае анализа рисков информационной системы на базовом уровне какими стандартами в области защиты информации необходимо руководствоваться? В случае полного анализа рисков информационных систем какие подходы обычно используются на практике? Какие этапы должен включать аудит информационной безопасности? Как осущесвляется анализ информационных рисков, угрозы и уязвимости системы по двум факторам? Как осущесвляется анализ информационных рисков, угрозы и уязвимости системы по двум факторам?
КМ7	Защита практической работы № 7.	ПК-3-У3	Какие требования предъявляются к набору критериев для оценки альтернативных решений? Как оценивается важность критериев? Приведите классификацию задач принятия решений в области проектирования систем защиты информации. Назовите основные этапы принятия управленческих решений в области построения защищенных систем обработки информации. Приведите пример генерирования множества альтернатив с применением экспертных методов при разработке системы защиты информации. Приведите пример использования метода строчных сумм для составления матрицы альтернативных проектов системы защиты информации. Сформулируйте принцип Парето. В чем достоинства и недостатки его практического применения для принятия управленческих решений в области построения защищенных систем обработки информации? Что понимается под парето-оптимальным множеством? Какие дополнительные возможности предоставляет метод достижимых целей для принятия управленческих решений в области построения защищенных систем обработки информации? Опишите последовательность шагов при использовании парето-оптимизации в выборе альтернативных проектов системы защиты информации.
КМ8	Защита практической работы № 8.	ПК-3-В1;ПК-3-З2	В чем отличие сетей Петри от других способов моделирования в системах защиты информации? Каким образом можно интерпретировать позиции и переходы при разработке сценариев действия нарушителя на объекте информатизации с использованием сети Петри? Приведите конкретные примеры. В чем заключается ограниченность использования сетей Петри для моделирования процессов, происходящих в информационных системах? Каким образом можно интерпретировать использование маркеров в сети Петри при моделировании действий нарушителя? Приведите конкретные примеры. Какие выводы можно сделать о достижимости конечной цели атак при запуске разработанной сети Петри?

КМ9	Защита практической работы № 9.	ОПК-5-З3;ОПК-5-У3	Перечислите способы защиты программных продуктов. Укажите их достоинства и недостатки. Какие методы включает юридическая защита программных продуктов? Охарактеризуйте основные из них. Перечислите основные международные и отечественные источники защиты прав авторов программ. В чем заключается процедура лицензирования программ? Какими нормативными документами регулируется процесс лицензирования программ? Перечислите технические методы защиты программных продуктов. Кратко охарактеризуйте каждый из них. Какие методы стеганографии могут использоваться для защиты программных продуктов? Сравните методы стеганографической защиты и технической защиты ПО. Какие особенности структуры PE-файлов дают возможность эффективного внедрения цифровых водяных знаков? Опишите суть метода внедрения кода в PE-файлы за счет размещения кода в свободном месте программы (интеграция). Какой из методов внедрения кода в PE-файлы используется в програм ме Filigrana? Опишите суть этого метода, его достоинства и недостатки. Какие способы обнаружения, извлечения и модификации ЦВЗ вы можете предложить для изученного метода защиты ПО?
КМ10	Защита практической работы № 10.	ОПК-5-З3;ОПК-5-У3	Перечислите способы защиты цифровых графических изображений от модификации и несанкционированного использования. Укажите их достоинства и недостатки. В чем особенность робастных, хрупких и полухрупких цифровых водяных знаков? Каковы ограничения в их использования для защиты электронных документов? Перечислите основные международные и отечественные источники защиты прав авторов цифрового графического контента. Алгоритм Хсу и Ву – особенности реализации, достоинства и недостатки. Алгоритм Фридрих – особенности реализации, достоинства и недостатки. Какие методы стеганографии могут использоваться для защиты графических файлов? Сравните методы стеганографической защиты и криптографической защиты. Алгоритм В. А. Митекина – особенности реализации, достоинства и недостатки. В чем заключается усовершенствование алгоритма В.А. Митекина в программных продуктах, использованных в лабораторной работе? Оцените эффективность исследованного алгоритма для встраивания ЦВЗ ? Подсчитайте максимальных объем встраиваемого ЦВЗ в бинарное изображение размером 1024×128 пикселей: а) в блоки 3×3 пикселя, б) в блоки 7×7 пикселей. Подсчитайте максимальных объем встраиваемого ЦВЗ в полутоновое изображение (256 градаций серого) размером 512×256 пикселей: а) в блоки 3×3 пикселя, б) в блоки 7×7 пикселей.

КМ11	Защита практической работы № 11.	ОПК-5-З3;ОПК-5-У3	Сформулируйте основные отличия стеганографических и криптографических методов защиты информационных ресурсов. В чем достоинства и недостатки каждого из методов? Перечислите шесть основных режимов работы программы Invisible Secrets-4. В каких случаях вы можете порекомендовать использование каждого из режимов? Оцените эффективность работы программы Invisible Secrets-4 с графическими и аудио файлами различных типов. Для этого в режиме “стеганография” встройте данные в контейнеры различных форматов, сравните пустые и заполненные контейнеры, сделайте выводы. При встраивании данных в режиме “стеганография” используйте различные алгоритмы для шифрования встраиваемых данных. Сравните пустые и заполненные контейнеры, как изменяется размер заполненных контейнеров в зависимости от метода шифрования? Почему вы получили такие результаты, обоснуйте.
КМ12	Защита практической работы № 12.	ОПК-5-З2;ОПК-5-У2	Какие физические принципы лежат в основе квантовой криптографии? Поясните назначение и принцип работы алгоритма BB84. Опишите алгоритм Беннета. В чем заключаются его особенности? Какие уязвимости квантовых криптосистем Вам известны? Приведите примеры. Что такое квантовая запутанность и в каких приложениях квантовых технологий защиты информации она используется? Опишите протокол квантового распределения ключей с использованием ЭПР. Каким образом может быть осуществлена атака на протокол BB84? Каким образом может быть осуществлена атака на протокол B92? Что такое PNS-атака и каким образом она осуществляется? Что такое критическая длина линии связи и каким образом она вычисляется в случае PNS-атаки?

5.2. Перечень работ, выполняемых по дисциплине (Курсовая работа, Курсовой проект, РГР, Реферат, ЛР, ПР и т.п.)

Код работы	Название работы	Проверяемые индикаторы компетенций	Содержание работы
Р1	Практическая работа №1. Изучение протоколов разбиения и разделения секрета	ОПК-5-У1	Изучение на практических примерах протокола тайных многосторонних вычислений на основе алгоритма RSA, схемы разбиения секрета с помощью гаммирования, схем разделения секрета с помощью интерполяционных полиномов Лагранжа и китайской теоремы об остатках.
Р2	Практическая работа № 2. Симметричные криптоалгоритмы. Шифр Плейфера.	ОПК-5-У1	Изучение принципов построения шифров замены на примере шифра Плейфера.
Р3	Практическая работа № 3. Дешифрование шифра простой перестановки при помощи метода биграмм.	ОПК-5-У1	Изучение шифров перестановки и простейших методов их криптоанализа
Р4	Практическая работа № 4. Изучение регистров сдвига с линейной обратной связью как генераторов псевдослучайных чисел	ОПК-5-В1	Изучение принципа работы генератора псевдослучайных последовательностей, основанного на регистре сдвига с линейной обратной связью.

Р5	Практическая работа № 5. Изучение модели информационной безопасности с полным перекрытием угроз	ПК-3-У2	Изучение принципов построения политик безопасности и моделей информационной безопасности. Составление модели с полным перекрытием угроз на примере конкретного предприятия.
Р6	Практическая работа №6. Анализ рисков информационной безопасности	ПК-3-З1;ПК-3-У2;ПК-3-В1	Анализ рисков информационной безопасности предприятия по методике COBIT.
Р7	Практическая работа № 7. Изучение системы поддержки принятия решений в области проектирования системы защиты информации на предприятии	ПК-3-У3	Изучение принципов Парето-оптимизации и системы поддержки принятия решений в области проектирования системы защиты информации на предприятии, построенной на основании метода достижимых целей.
Р8	Практическая работа № 8. Разработка сценариев действий нарушителя информационной безопасности с использованием сети Петри.	ПК-3-З2;ПК-3-У2;ПК-3-В1	Изучение принципов построения сетей Петри и разработка сценариев действий нарушителя информационной безопасности с их использованием.
Р9	Практическая работа № 9. Защита программного обеспечения методами стеганографии	ОПК-5-У3	Изучение способов защиты программного обеспечения. Применение стеганографических методов.
Р10	Практическая работа № 10. Защита электронных документов с использованием цифровых водяных знаков	ОПК-5-У3	Изучение способов защиты электронных документов с использованием цифровых водяных знаков.
Р11	Практическая работа № 11. Стегокомплексы, допускающие использование аудиоконтейнеров	ОПК-5-У3	Изучение программного комплекса INVISIBLE SECRET и принципов стеганографического встраивания информации в аудиоконтейнеры.
Р12	Практическая работа № 12. Расчет критической длины линии связи при PNS-атаке на квантовый канал	ОПК-5-У2	Изучение атак на канал квантовой связи и расчет критической длины линии связи при PNS-атаке на квантовый канал.
5.3. Оценочные материалы, используемые для экзамена (описание билетов, тестов и т.п.)			
Экзамен по данной дисциплине не предусмотрен.			

5.4. Методика оценки освоения дисциплины (модуля, практики. НИР)

Требования к оцениванию: зачет.

Система оценивания, используемая для оценки успеваемости по дисциплине балльно-рейтинговая. Итоговая успеваемость обучающегося за семестр оценивается с помощью текущего контроля и промежуточной аттестации.

Текущий контроль представляет собой проверку усвоения учебного материала теоретического и практического характера, регулярно осуществляемую на протяжении семестра. Основные формы текущего контроля (текущей аттестации) – отчёты по выполненным практическим работам и их защита. Освоение дисциплины, её успешное завершение на стадии промежуточного контроля возможно только при регулярной работе во время семестра и планомерном прохождении текущего контроля.

Промежуточная аттестация осуществляется в конце семестра и проходит в виде зачета.

Для завершения работы в семестре и для получения допуска к промежуточной аттестации обучающийся должен выполнить все мероприятия текущего контроля, предусмотренные учебным планом и программой дисциплины, включающие полный комплект подготовленных и защищённых отчётов по практическим работам.

Критерии оценивания отчетов по практическим работам:

«отлично»: обучающийся демонстрирует системность и глубину знаний, владеет научной терминологией в области современных технологий защиты информации, стилистически грамотно, логически правильно и исчерпывающе освещает поставленные вопросы; даёт полные и аргументированные ответы на дополнительные вопросы;

«хорошо»: обучающийся демонстрирует достаточную полноту знаний (при наличии лишь несущественных неточностей в освещении отдельных вопросов), владеет научной терминологией в области современных технологий защиты информации, стилистически грамотно, логически правильно и достаточно полно (пропуская или неточно излагая отельные существенные детали) освещает поставленные вопросы; при ответах на дополнительные вопросы недостаточно полно раскрывает их сущность, допускает незначительные ошибки, но исправляется при наводящих вопросах;

«удовлетворительно»: обучающийся демонстрирует достаточные знания по основным вопросам в рамках программы дисциплины, но допускает при этом неточности; в достаточной мере использует научную терминологию в области метрологии, стандартизации и сертификации, в основном структурировано и содержательно излагает сущность вопросов, допуская при этом незначительные ошибки, которые при наводящих вопросах может исправить; при ответах на дополнительные вопросы допускает ошибки непринципиального характера;

«неудовлетворительно»: обучающийся демонстрирует фрагментарные знания в рамках программы дисциплины, не владеет минимально необходимой научной терминологией в области современных технологий защиты информации; допускает грубые логические ошибки, отвечая на поставленные вопросы, которые не может исправить самостоятельно.

Условия получения зачета: зачет по дисциплине проставляется обучающемуся, выполнившему на положительные оценки все практические работы и набравшему в итоге не менее 36 баллов.

Методика расчёта баллов (первое число – минимальные баллы для положительной оценки, второе число – максимальные баллы):
– оценка по практической работе (в баллах) = оценка за составление и защиту отчёта = 3 – 5;

Сумма набранных баллов за выполнение обучающимся двенадцати практических работ: (3 – 5) х 12 = 36 – 60.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Библиотека	Издательство, год
Л1.1	Фабричнов А. Г., Дёмушкин А. С., Кондрашова Т. В., Куняев Н. Н.	Конфиденциальное делопроизводство и защищенный электронный документооборот: учебник	Электронная библиотека	Москва: Логос, 2011
Л1.2	Ильичев Е. В., Гринберг Я. С.	Квантовая информатика и квантовые биты на основе сверхпроводниковых джозефсоновских структур: учебник	Электронная библиотека	Новосибирск: Новосибирский государственный технический университет, 2013

	Авторы, составители	Заглавие	Библиотека	Издательство, год
Л1.3	Нестеров С. А.	Основы информационной безопасности: учебное пособие	Электронная библиотека	Санкт-Петербург: Издательство Политехнического университета, 2014
Л1.4	Ищукова Е. А., Лобова Е. А.	Криптографические протоколы и стандарты: учебное пособие	Электронная библиотека	Таганрог: Южный федеральный университет, 2016
Л1.5	Кирпичников А. П., Хайбуллина З. М.	Криптографические методы защиты компьютерной информации: учебное пособие	Электронная библиотека	Казань: Казанский научно-исследовательский технологический университет (КНИТУ), 2016
Л1.6	Мельников В. П., Клейменов С. А., Петраков А. М., Клейменов С. А.	Информационная безопасность и защита информации: учеб. пособие для студ. вузов, обуч. по спец. 230201 "Информационные системы и технологии"	Библиотека МИСиС	М.: ACADEMIA, 2008
Л1.7	Костин В. Н.	Методы и средства защиты компьютерной информации. Криптографические методы защиты информации (N 3086): учеб. пособие	Электронная библиотека	М.: [МИСиС], 2018

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Библиотека	Издательство, год
Л2.1	Башлы П. Н., Баранова Е. К., Бабаш А. В.	Информационная безопасность: учебно-практическое пособие: учебное пособие	Электронная библиотека	Москва: Евразийский открытый институт, 2011
Л2.2	Минин И. В., Минин О. В.	Защита конфиденциальной информации при электронном документообороте: учебное пособие	Электронная библиотека	Новосибирск: Новосибирский государственный технический университет, 2011
Л2.3	Лапонина О. Р.	Криптографические основы безопасности: учебное пособие	Электронная библиотека	Москва: Национальный Открытый Университет «ИНТУИТ», 2016
Л2.4	Доррер Г. А.	Методы и системы принятия решений: учебное пособие	Электронная библиотека	Красноярск: Сибирский федеральный университет (СФУ), 2016
Л2.5	Целых А. Н., Целых Л. А., Барковский С. А.	Адаптивные информационные системы для поддержки принятия решений: монография	Электронная библиотека	Ростов-на-Дону, Таганрог: Южный федеральный университет, 2018
Л2.6	Белинский А. В.	Квантовые измерения: учебное пособие	Электронная библиотека	Москва: БИНОМ. Лаборатория знаний, 2015
Л2.7	Вишняков Я. Д., Радаев Н. Н.	Общая теория рисков: учеб. пособие для студ. вузов, обуч. по спец. "Менеджмент организации"	Библиотека МИСиС	М.: ACADEMIA, 2007
Л2.8	Адигамов А. Э., Макаров П. В., Семенова Н. В.	Элементы теории графов и оптимизация на сетях	Библиотека МИСиС	, 2009

6.1.3. Методические разработки

	Авторы, составители	Заглавие	Библиотека	Издательство, год
Л3.1	Макаревич О. Б., Бабенко Л. К., Шилов А. К., Коваленко А. В.	Основы защищенного делопроизводства: по курсу Технология защищенного документооборота: методическое пособие	Электронная библиотека	Таганрог: Издательство ТРТУ, 2000

	Авторы, составители	Заглавие	Библиотека	Издательство, год
Л3.2	Киселева И. А.	Моделирование рисковых ситуаций: учебно-методический комплекс	Электронная библиотека	Москва: Евразийский открытый институт, 2011
Л3.3	Векилов Ю. Х., Кузьмич И. П., Кадышевич А. Е.	Теоретическая физика: Разд.: Квантовая механика: Учеб. пособие для практ. занятий для студентов спец. 0406, 0629, 0606	Библиотека МИСиС	М.: Учеба, 1981
Л3.4	Бахаров Л. Е.	Информационная безопасность и защита информации (разделы криптография и стеганография) (N 3854): практикум	Электронная библиотека	М.: [МИСиС], 2019
Л3.5	Петров А. Е.	Математические модели принятия решений (N 3092): учебно-метод. пособие	Электронная библиотека	М.: [МИСиС], 2018

6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

Э1	Курс "Современные технологии защиты информации" в ЭОИС Canvas. Режим доступа - URL: https://lms.misis.ru/login/canvas (дата обращения 06.08.21)	https://lms.misis.ru/login/canvas
Э2	Официальный сайт Федеральной службы РФ по таможенному и экспортному контролю. Режим доступа URL: https://fstec.ru/ (дата обращения 01.07.2021).	https://fstec.ru/

6.3 Перечень программного обеспечения

П.1	Win Pro 10 32-bit/64-bit
П.2	LMS Canvas
П.3	MS Teams
П.4	WinRAR

6.4. Перечень информационных справочных систем и профессиональных баз данных

И.1	1. Банк данных угроз безопасности информации (https://bdu.fstec.ru/)
И.2	2. Единое окно доступа к образовательным ресурсам (http://window.edu.ru)
И.3	3. Электронно-библиотечная система "Лань" (https://e.lanbook.com)
И.4	4. ScienceDirect - база полнотекстовых научных журналов и книг издательства Elsevier (https://www.sciencedirect.com)
И.5	5. Scopus - единая реферативная база данных научных публикаций (https://www.scopus.com)

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

Ауд.	Назначение	Оснащение
Л-731	Учебная аудитория	доска аудиторная меловая, экран проекционный, проектор, стационарные компьютеры 15 шт. ПО-Visual Studio; Electronic WorkBench; APACHE; MySQL; XAMPP; Python, комплект учебной мебели, пакет лицензионных программ MS Office
Любой корпус Мультимедийная	Учебная аудитория для проведения занятий лекционного типа и/или для проведения практических занятий:	комплект учебной мебели до 36 мест для обучающихся, мультимедийное оборудование, магнитно-маркерная доска, рабочее место преподавателя, ПКс доступом к ИТС «Интернет», ЭИОС университета через личный кабинет на платформе LMS Canvas, лицензионные программы MS Office, MS Teams, ESET Antivirus
Б-библиотека правый класс	Учебная аудитория	комплект учебной мебели на 32 рабочих места

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ

Дисциплина относится к точным наукам и требует значительного объема самостоятельной работы. Отдельные учебные вопросы выносятся на самостоятельную проработку и контролируются посредством текущей аттестации. Качественное освоение дисциплины возможно только при систематической самостоятельной работе. Курсовая работа проводится с широким использованием компьютерных программ, как для выполнения, так и для оформления работы. Практические работы выполняются с помощью компьютерных программ имитационного моделирования. Так как ситуация в сфере

информационной безопасности непрерывно изменяется, кроме рекомендованной литературы, обучающимся следует активно использовать материалы периодической печати, сети интернет и социальных сетей, затрагивающие вопросы защиты информации. Приветствуется также посещение студентами специализированных выставок по направлению информационной безопасности и защиты информации с тем, чтобы сформировать наиболее целостное и актуальное представление об изучаемой дисциплине.

Практические занятия по дисциплине проводятся в компьютерных классах в ауд. Л-728, Л-731 (15 ПК в каждой). Все компьютеры объединены в локальную сеть с выходом в Интернет).