Подписано и утверждено в СЭД 17.03.2022 20:32:44ИД задачи 2585573

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»

УТВЕРЖДАЮ
Директор по образовательной
деятельности

_____ С.Т. Князев
«___» _____

РАБОЧАЯ ПРОГРАММА МОДУЛЯ

Код модуля	Модуль
1157335	Теоретические и организационно-правовые основы информационной безопасности

Екатеринбург

Перечень сведений о рабочей программе модуля	Учетные данные
Образовательная программа 1. Математические методы защиты информации	**Код ОП** 1. 10.05.01/22.01
Направление подготовки 1. Компьютерная безопасность	**Код направления и уровня подготовки** 1. 10.05.01

Программа модуля составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Баранский Виталий Анатольевич	доктор физико-математических наук, профессор	Профессор	алгебры и фундаментальной информатики
2	Синадский Николай Игоревич	кандидат технических наук, Доцент	Доцент	УНЦ "Информационная безопасность"

Согласовано:

Управление образовательных программ Р.Х. Токарева

1. ОБЩАЯ ХАРАКТЕРИСТИКА МОДУЛЯ Теоретические и организационно-правовые основы информационной безопасности

1.1. Аннотация содержания модуля

Модуль «Теоретические и организационно-правовые основы информационной безопасности» предполагает получение студентами компетенций по разработке математических моделей защищаемых процессов и средств защиты информации и систем, обеспечивающих информационную безопасность объектов. В модуль входят следующие дисциплины: «Модели безопасности компьютерных систем», «Основы информационной безопасности», «Организационно-правовое обеспечение информационной безопасности», «Защита информации от утечки по техническим каналам»

1.2. Структура и объем модуля

Таблица 1

№ п/п	Перечень дисциплин модуля в последовательности их освоения	Объем дисциплин модуля и всего модуля в зачетных единицах
1	Модели безопасности компьютерных систем	3
2	Организационно-правовое обеспечение информационной безопасности	3
3	Основы информационной безопасности	3
4	Защита информации от утечки по техническим каналам	3
	ИТОГО по модулю:	12

1.3.Последовательность освоения модуля в образовательной программе

Пререквизиты модуля	Не предусмотрены
Постреквизиты и кореквизиты модуля	Не предусмотрены

1.4. Распределение компетенций по дисциплинам модуля, планируемые результаты обучения (индикаторы) по модулю

Таблица 2

Перечень дисциплин модуля	Код и наименование компетенции	Планируемые результаты обучения (индикаторы)
1	2	3

Защита информации от утечки по техническим каналам	ОПК-4 - Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности	З-2 - Описывать основы микроэлектронной техники У-2 - Анализировать и применять модели явлений, процессов и объектов (включая схемы электронных устройств) при решении инженерных задач в профессиональной деятельности П-1 - Осуществлять обоснованный выбор из основных методов теоретического и экспериментального исследования физических явлений и процессов, в том числе лежащих в основе микроэлектронной техник
	ОПК-9 - Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации	З-1 - Классифицировать технические каналы утечки информации З-2 - Классифицировать способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации З-3 - Описывать принципы работы элементов и функциональных узлов электронной аппаратуры З-4 - Классифицировать уязвимости основных телекоммуникационных технологий З-5 - Классифицировать технологии, средства и методы обеспечения информационной безопасности телекоммуникационных систем У-1 - Анализировать и оценивать угрозы информационной безопасности объекта У-2 - Анализировать безопасность функционирования телекоммуникационных систем У-3 - Измерять и рассчитывать основные характеристики сигналов и помех У-4 - Оценивать синхронные и асинхронные защищенные резервные хранилища данных П-1 - Иметь практический опыт работы с методами и средствами технической защиты информации

		П-2 - Осуществлять рациональный выбор средств и методов защиты информации на объектах информатизации
Модели безопасности компьютерных систем	ОПК-11 - Способен разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации	З-1 - Классифицировать основные виды политик управления доступом и информационными потоками в компьютерных системах З-2 - Классифицировать основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков У-1 - Формулировать модели угроз и модели нарушителя безопасности компьютерных систем У-2 - Формулировать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками П-1 - Предлагать методы моделирования безопасности компьютерных систем, в том числе моделирования управления доступом и информационными потоками в компьютерных системах
	ОПК-19 - Способен разрабатывать и анализировать математические модели механизмов защиты информации	З-6 - Классифицировать основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков У-1 - Выбирать математические методы и модели для решения задач профессиональной деятельности П-1 - Иметь практический опыт решения математических задач в области профессиональной деятельности
	ПК-2 - Способен разрабатывать требования по защите, формирование политик безопасности компьютерных систем и сетей	З-1 - Описывать принципы построения компьютерных систем и сетей З-2 - Характеризовать модели безопасности компьютерных систем З-3 - Различать виды политик безопасности компьютерных систем и сетей

		З-4 - Описывать принципы построения средств криптографической защиты информации З-6 - Возможности используемых и планируемых к использованию средств защиты информации З-9 - Классифицировать организационные меры по защите информации У-1 - Анализировать компьютерную систему с целью определения необходимого уровня защищенности и доверия У-2 - Разрабатывать профили защиты компьютерных систем У-3 - Формулировать задания по безопасности компьютерных систем У-4 - Выполнять анализ безопасности компьютерных систем и разрабатывать рекомендации по эксплуатации системы защиты информации У-5 - Формировать политики безопасности компьютерных систем и сетей П-1 - Выполнять формирование политик безопасности компьютерных систем П-2 - Разрабатывать рекомендации по вопросам безопасности компьютерных систем П-3 - Выполнять разработку профилей защиты и заданий по безопасности П-4 - Выполнять разработку технических заданий на создание средств защиты информации П-5 - Разрабатывать рекомендации о необходимости защиты информации, содержащейся в информационной системе П-6 - Сделать вывод о классификации информационной системы по требованиям защиты информации П-7 - Сделать вывод об угрозах безопасности информации, реализация которых может привести к нарушению безопасности информации в компьютерной системе и сети

		П-8 - Выполнять разработку модели угроз безопасности информации П-9 - Разрабатывать рекомендации о требованиях к защите информации компьютерной системы П-10 - Выполнять разработку руководящих документов по защите информации в организации
	ПК-3 - Способен проводить анализ безопасности компьютерных систем	З-1 - Описывать принципы построения компьютерных систем и сетей З-2 - Характеризовать уязвимости компьютерных систем и сетей З-5 - Характеризовать средства анализа конфигураций З-9 - Классифицировать организационные меры по защите информации У-1 - Анализировать компьютерную систему с целью определения уровня защищенности и доверия У-2 - Прогнозировать возможные пути развития действий нарушителя информационной безопасности У-3 - Производить анализ политики безопасности на предмет адекватности У-4 - Проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в операционных системах У-5 - Составлять и оформлять аналитический отчет по результатам проведенного анализа У-6 - Разрабатывать предложения по устранению выявленных уязвимостей П-1 - Сделать вывод об уровне защищенности и доверия в компьютерных системах П-2 - Сделать вывод о рисках, связанных с осуществлением угроз безопасности в отношении компьютерных систем П-3 - Сделать вывод о соответствии механизмов безопасности компьютерной системы требованиям существующих

		нормативных документов, а также их адекватности существующим рискам П-4 - Подготовить аналитический отчета по результатам проведенного анализа П-5 - Разрабатывать рекомендации по устранению выявленных уязвимостей
	ПК-4 - Способен проводить инструментальный мониторинг защищенности компьютерных систем и сетей	З-1 - Описывать принципы построения компьютерных систем и сетей З-2 - Описывать формальные модели безопасности компьютерных систем и сетей З-10 - Классифицировать организационные меры по защите информации У-1 - Формализовывать задачу управления безопасностью компьютерных систем У-2 - Применять инструментальные средства проведения мониторинга защищенности компьютерных систем У-3 - Применять методы анализа защищенности компьютерных систем и сетей П-1 - Сделать вывод о защищенности компьютерных систем с использованием сканеров безопасности П-2 - Сделать вывод о защищенности сетевых сервисов с использованием средств автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей
Организационно-правовое обеспечение информационной безопасности	УК-2 - Способен управлять проектом на всех этапах его жизненного цикла	З-1 - Характеризовать базовые принципы системного анализа и принятия решений З-2 - Описывать процедуры планирования профессиональной, в том числе проектной, деятельности З-3 - Сделать обзор действующих правовых норм и ограничений, оказывающих регулирующее воздействие на профессиональную деятельность У-1 - Определять круг задач, цели, основные этапы и направления реализации задач профессиональной, в том числе проектной, деятельности с учетом имеющихся ресурсов и ограничений

		У-2 - Выбирать оптимальные способы решения профессиональных задач с учетом действующих правовых норм, имеющихся ресурсов и ограничений У-3 - Вырабатывать алгоритмы решения задач в процессе интеллектуальной деятельности П-1 - Формировать план-график реализации задач в рамках поставленной цели и план контроля ее выполнения П-2 - Предлагать способы решения поставленных задач, прогнозировать результаты профессиональной деятельности с учетом действующих правовых норм, имеющихся ресурсов и ограничений
	УК-10 - Способен формировать нетерпимое отношение к коррупционному поведению	З-1 - Описывать основные права и обязанности человека и гражданина и способы воспитания нетерпимого отношения к коррупции в различных областях жизнедеятельности З-2 - Характеризовать законодательные нормы, направленные на борьбу с коррупционным поведением, манипулятивные технологии формирования ложных и антиправовых действий У-1 - Распознавать признаки коррупционного поведения в различных областях жизнедеятельности и определять свою жизненную позицию на основе гражданских ценностей, социальной ответственности и нетерпимости к коррупции У-2 - Оценивать политические и социально-экономические события и ситуации, выявлять действия, направленные на манипулирование людьми, и определять способы противостояния психологической манипуляции П-1 - Иметь опыт решения проблемных ситуаций, связанных с коррупционным поведением граждан, нарушением гражданских прав, применением манипулятивных технологий формирования ложных и антиправовых действий, опираясь на законодательные нормы и собственную

		позицию нетерпимого отношения к коррупции
	ОПК-1 - Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	З-1 - Перечислить угрозы информационной безопасности государства З-3 - Изложить цели и задачи государственной политики в сфере ИБ З-4 - Перечислить виды информации ограниченного распространения З-5 - Сформулировать понятия компьютерной информации, интеллектуальной собственности, сертификации, государственной тайны, информационного общества З-6 - Изложить требования к организаторам распространения информации в сети «Интернет» У-1 - Оценивать и применять основные методы обеспечения информационной безопасности П-1 - Осуществлять обоснованный выбор базовых методов выявления и классификации угроз информационной безопасности современного общества, основными подходами к противодействию угрозам информационной безопасности
	ОПК-5 - Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	З-1 - Изложить методологию обеспечения режима защиты информации З-2 - Сформулировать понятия компьютерной информации, интеллектуальной собственности, сертификации, государственной тайны З-3 - Изложить порядок отнесения сведений к государственной тайне З-4 - Перечислить ограничения, связанные с государственной тайной З-5 - Изложить процедуры ограничения доступа к интернет-ресурсам З-6 - Изложить полномочия государственных органов по лицензированию и сертификации

		З-7 - Перечислить виды сертификатов и сертифицируемых средств в сфере информационной безопасности У-1 - Правильно интерпретировать и применять действующую нормативную базу, нормативные правовые акты, нормативные и методические документы для принятия правовых и организационных мер по защите информации У-2 - Формулировать проекты нормативно-правовых актов и организационно-распорядительных документов, регламентирующих деятельность по защите информации У-3 - Правильно интерпретировать уголовно-правовые запреты в сфере информационной безопасности У-4 - Правильно интерпретировать содержание нормативных правовых актов по охране интеллектуальной собственности У-5 - Правильно интерпретировать содержание нормативных требований по защите государственной тайны П-1 - Осуществлять обоснованный выбор методов поиска и анализа нормативных правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации
	ОПК-6 - Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по	З-1 - Перечислить правовые и организационные меры защиты информации, в том числе информации ограниченного доступа З-2 - Изложить содержание нормативных правовых актов, нормативных и методических документов уполномоченных федеральных органов исполнительной власти (в том числе Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю) по защите информации З-3 - Изложить цели, задачи, принципы и основные направления обеспечения режима

	техническому и экспертному контролю	защиты информации, в том числе ограниченного доступа З-5 - Перечислить обязанности права оператора персональных данных У-1 - Формулировать организационно-распорядительные документы, регламентирующие защиту информации ограниченного доступа в автоматизированных системах У-3 - Анализировать деятельность по обеспечению информационной безопасности с учетом требований по лицензированию и сертификации в данной сфере П-1 - Осуществлять обоснованный выбор способов применения действующей нормативной базы в области защиты информации ограниченного доступа
	ОПК-11 - Способен разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации	З-3 - Изложить содержание нормативных правовых актов в сфере информационной безопасности У-1 - Формулировать модели угроз и модели нарушителя безопасности компьютерных систем
	ОПК-17 - Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе формирования гражданской позиции и развития патриотизма	З-2 - Перечислить цели и задачи государственной политики в сфере информационной безопасности У-2 - Формулировать интересы государства сфере информационной безопасности П-1 - Сделать вывод для формирования собственной гражданской позиции и развития патриотизма на основе принципов историзма и научной объективности
	ПК-1 - Способен проводить контрольные проверки работоспособности и эффективности применяемых	З-4 - Описывать принципы построения подсистем защиты информации в компьютерных системах

	программно-аппаратных средств защиты информации	З-9 - Изложить национальные, межгосударственные и международные стандарты в области защиты информации З-10 - Воспроизвести нормативные правовые акты в области защиты информации З-11 - Воспроизвести руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации З-12 - Классифицировать организационные меры по защите информации У-4 - Применять разработанные методики оценки защищенности программно-аппаратных средств защиты информации У-5 - Анализировать программно-аппаратные средства защиты с целью определения уровня обеспечиваемой ими защищенности и доверия П-3 - Сделать вывод об уровне защищенности и доверия программно-аппаратных средств защиты информации
	ПК-2 - Способен разрабатывать требования по защите, формирование политик безопасности компьютерных систем и сетей	З-5 - Изложить национальные, межгосударственные и международные стандарты в области защиты информации З-6 - Возможности используемых и планируемых к использованию средств защиты информации З-7 - Воспроизвести нормативные правовые акты в области защиты информации З-8 - Воспроизвести руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации З-9 - Классифицировать организационные меры по защите информации У-3 - Формулировать задания по безопасности компьютерных систем У-4 - Выполнять анализ безопасности компьютерных систем и разрабатывать рекомендации по эксплуатации системы защиты информации

		У-5 - Формировать политики безопасности компьютерных систем и сетей П-4 - Выполнять разработку технических заданий на создание средств защиты информации П-5 - Разрабатывать рекомендации о необходимости защиты информации, содержащейся в информационной системе П-9 - Разрабатывать рекомендации о требованиях к защите информации компьютерной системы П-10 - Выполнять разработку руководящих документов по защите информации в организации
	ПК-3 - Способен проводить анализ безопасности компьютерных систем	З-1 - Описывать принципы построения компьютерных систем и сетей З-6 - Изложить национальные, межгосударственные и международные стандарты в области защиты информации З-7 - Воспроизвести нормативные правовые акты в области защиты информации З-8 - Воспроизвести руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации З-9 - Классифицировать организационные меры по защите информации У-2 - Прогнозировать возможные пути развития действий нарушителя информационной безопасности У-3 - Производить анализ политики безопасности на предмет адекватности У-5 - Составлять и оформлять аналитический отчет по результатам проведенного анализа П-1 - Сделать вывод об уровне защищенности и доверия в компьютерных системах П-3 - Сделать вывод о соответствии механизмов безопасности компьютерной системы требованиям существующих

		нормативных документов, а также их адекватности существующим рискам
	ПК-4 - Способен проводить инструментальный мониторинг защищенности компьютерных систем и сетей	З-1 - Описывать принципы построения компьютерных систем и сетей З-5 - Воспроизвести порядок создания и структуру отчета, создаваемого по результатам проверок З-8 - Воспроизвести нормативные правовые акты в области защиты информации З-9 - Воспроизвести руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации З-10 - Классифицировать организационные меры по защите информации У-4 - Структурировать аналитическую информацию для включения в отчет П-3 - Оформить отчет по результатам проверок
	ПК-5 - Способен проводить экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов	З-6 - Воспроизвести порядок фиксации и документирования следов компьютерных преступлений, правонарушений и инцидентов З-7 - Перечислить нормы уголовного и административного права в сфере компьютерной информации З-8 - Описывать характеристики правонарушений в области связи и информации З-9 - Характеризовать виды преступлений в сфере компьютерной информации З-10 - Воспроизвести порядок проведения экспертизы вычислительной техники и носителей компьютерной информации с учетом нормативных правовых актов З-13 - Воспроизвести порядок подготовки научно-технических экспертных заключений по результатам выполненных работ по информационно-аналитической и технической экспертизе компьютерных систем

		З-14 - Объяснять методы проведения расследования компьютерных преступлений, правонарушений и инцидентов З-17 - Воспроизвести нормативные правовые акты в области защиты информации З-18 - Воспроизвести руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации З-19 - Классифицировать организационные меры по защите информации У-1 - Применять нормативные и правовые акты при проведении криминалистической экспертизы и криминалистического анализа У-6 - Применять действующую законодательную базу в области обеспечения защиты информации П-15 - Сделать вывод об участниках события, их роли, места, условий, при которых была создана, модифицирована или удалена информация П-16 - Сделать вывод о соответствии либо несоответствии действий с информацией специальному регламенту (правилам) П-17 - Подготовить экспертное заключение
	ПК-6 - Способен разрабатывать программные и программно-аппаратные средства для систем защиты информации автоматизированных систем	З-12 - Воспроизвести нормативные правовые акты в области защиты информации З-13 - Воспроизвести руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации У-2 - Разрабатывать технические задания на создание подсистем безопасности информации автоматизированных систем, проектировать такие подсистемы с учетом требований нормативных документов, ЕСКД и ЕСПД П-1 - Выполнять разработку технической документации в соответствии с требованиями Единой системы

		конструкторской документации (ЕСКД) и Единой системы программной документации (ЕСПД) на компоненты автоматизированных систем
Основы информационной безопасности	УК-1 - Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	З-1 - Сделать обзор основных принципов критического мышления, методов анализа и оценки информации У-1 - Критически анализировать информацию, формировать собственное мнение и формулировать аргументы для защиты своей позиции У-2 - Определять достоверность и обоснованность выводов, выявлять и анализировать типовые ошибки в рассуждениях и когнитивные искажения в работе с информацией У-3 - Критически оценивать надежность источников информации в условиях неопределенности и избытка/недостатка информации для решения поставленных задач П-1 - Определять пути решения поставленных задач, опираясь на методики поиска, системного анализа и коррекции информации
	ОПК-1 - Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	З-1 - Перечислить угрозы информационной безопасности государства З-2 - Изложить содержание информационной войны, методы и средства ее ведения З-3 - Изложить цели и задачи государственной политики в сфере ИБ З-4 - Перечислить виды информации ограниченного распространения У-1 - Оценивать и применять основные методы обеспечения информационной безопасности П-1 - Осуществлять обоснованный выбор базовых методов выявления и классификации угроз информационной безопасности современного общества, основными подходами к противодействию угрозам информационной безопасности

		П-2 - Осуществлять обоснованный выбор поиска эффективных вариантов решения потенциально рискованных инновационных задач в области прикладной информатики
	ОПК-17 - Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе формирования гражданской позиции и развития патриотизма	З-2 - Перечислить цели и задачи государственной политики в сфере информационной безопасности У-2 - Формулировать интересы государства сфере информационной безопасности П-1 - Сделать вывод для формирования собственной гражданской позиции и развития патриотизма на основе принципов историзма и научной объективности

1.5. Форма обучения

Обучение по дисциплинам модуля может осуществляться в очной формах.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Модели безопасности компьютерных систем

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Бакланов Валентин Викторович	кандидат технических наук, доцент	Доцент	Департамент радиоэлектроники и связи
2	Синадский Николай Игоревич	кандидат технических наук, Доцент	Доцент	УНЦ "Информационная безопасность"

Рекомендовано учебно-методическим советом института Естественных наук и математики

Протокол № _7_ от _21.10.2021_ г.

1. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

Авторы:

- **Бакланов Валентин Викторович, Доцент, Департамент радиоэлектроники и связи**
- **Синадский Николай Игоревич, Доцент, УНЦ "Информационная безопасность"**

1.1. Технологии реализации, используемые при изучении дисциплины модуля

- Традиционная (репродуктивная) технология
- Разноуровневое (дифференцированное) обучение
  - Базовый уровень

**Базовый I уровень – сохраняет логику самой науки и позволяет получить упрощенное, но верное и полное представление о предмете дисциплины, требует знание системы понятий, умение решать проблемные ситуации. Освоение данного уровня результатов обучения должно обеспечить формирование запланированных компетенций и позволит обучающемуся на минимальном уровне самостоятельности и ответственности выполнять задания;*
Продвинутый II уровень – углубляет и обогащает базовый уровень как по содержанию, так и по глубине проработки материала дисциплины. Это происходит за счет включения дополнительной информации. Данный уровень требует умения решать проблемы в рамках курса и смежных курсов посредством самостоятельной постановки цели и выбора программы действий. Освоение данного уровня результатов обучения позволит обучающемуся повысить уровень самостоятельности и ответственности до творческого применения знаний и умений.

1.2. Содержание дисциплины

Таблица 1.1

Код раздела, темы	Раздел, тема дисциплины*	Содержание
Р1	Модели компьютерных систем с дискреционным управлением доступом	Тема 1. Сущность, субъект, доступ, информационный поток Основные элементы теории компьютерной безопасности (сущность, субъект, доступ, право доступа, информационные потоки по памяти или по времени). Основная аксиома. Проблема построения защищенной КС. Модели ценности информации: аддитивная модель, порядковая шкала, решетка многоуровневой безопасности. Тема 2. Угрозы безопасности информации. Политика безопасности Классификация угроз безопасности информации. Угрозы конфиденциальности, целостности, доступности информации, раскрытия параметров КС. Понятие политики безопасности. Модель нарушителя. Основные виды политик управления доступом и информационными потоками. Политики дискреционного, мандатного, ролевого управления доступом, изолированной программной среды и безопасности информационных потоков. Тема 3. Модель матрицы доступов Харрисона-РуззоУльмана Модель матрицы доступов Харрисона-Руззо-Ульмана (ХРУ). Анализ безопасности систем ХРУ. Монооперационные системы ХРУ. Алгоритмическая неразрешимость задачи проверки безопасности систем ХРУ. Тема 4. Модель

		типизированной матрицы доступов Модель типизированной матрицы доступов (ТМД). Монотонные системы ТМД и их каноническая форма. Граф создания. Ациклические монотонные ТМД и алгоритм проверки их безопасности. Тема 5. Классическая модель распространения прав доступа Take-Grant Классическая модель Take-Grant. Де-юре правила преобразования графов доступов. Условия передачи прав доступа в графе доступов, состоящем только из субъектов. Остров, мост, пролеты моста. Условия передачи прав доступа в произвольном графе доступов при отсутствии ограничений на кооперацию субъектов. Тема 6. Расширенная модель распространения прав доступа Take-Grant Расширенная модель Take-Grant. Де-факто правила преобразования графов доступов и информационных потоков. Условия реализации информационных потоков. Алгоритм построения замыкания графа доступов и информационных потоков. Представление систем Take-Grant системами ХРУ и ТМД.
Р2	Модели компьютерных систем с мандатным управлением доступом	Тема 7. Классическая модель Белла-ЛаПадулы Классическая модель Белла-ЛаПадулы. Свойства безопасности. Безопасный доступ, состояние, система. Базовая теорема безопасности. Интерпретации модели Белла-ЛаПадулы: модель реализации политики low-watermark, безопасность переходов, модель мандатной политики целостности информации Биба. Недостатки модели Белла-ЛаПадулы. Примеры реализации запрещенных информационных потоков. Тема 8. Интерпретации модели Белла-ЛаПадулы Интерпретации модели Белла-ЛаПадулы: модель реализации политики low-watermark, безопасность переходов, модель мандатной политики целостности информации Биба. Недостатки модели Белла-ЛаПадулы. Примеры реализации запрещенных информационных потоков по памяти или по времени. Тема 9. Модель систем военных сообщений Неформальное и формальное описания модели систем военных сообщений. Безопасное состояние. Безопасность переходов. Потенциальная модификация сущности с источником. Смыслы безопасности функции переходов.
Р3	Модели безопасности информационных потоков и изолированной программной среды	Тема 10. Автоматная, программная и вероятностная модели безопасности информационных потоков Автоматная модель безопасности информационных потоков. Программная модель контроля информационных потоков. Контролирующий механизм защиты. Вероятностная модель безопасности информационных потоков. Информационное невлияние.

		Тема 11. Субъектно-ориентированная модель изолированной программной среды Субъектно-ориентированная модель изолированной программной среды (ИПС). Объекты, функционально ассоциированные с субъектами. Мониторы безопасности обращений и порождения субъектов. Базовая теорема ИПС.
Р4	Модели компьютерных систем с ролевым управлением доступом	Тема 12. Базовая модель ролевого управления доступом. Модель администрирования ролевого управления доступом Описание базовой модели ролевого управления доступом. Иерархия ролей. Механизм ограничений. Модель администрирования ролевого управления доступом. Администрирование множеств авторизованных ролей пользователей, прав доступа, которыми обладает роли, иерархии ролей. Тема 13. Субъектно-ориентированная модель изолированной программной среды Модель мандатного ролевого управления доступом. Задание иерархии ролей и ограничений в соответствии с требованиями либерального или строгого мандатного управления доступом. Безопасность информационных потоков. Защита от угроз конфиденциальности и целостности информации.

1.3. Направление, виды воспитательной деятельности и используемые технологии

Таблица 1.2

Направление воспитательной деятельности	Вид воспитательной деятельности	Технология воспитательной деятельности	Компетенция	Результаты обучения
Профессиональное воспитание	учебно-исследовательская, научно-исследовательская	Технология формирования уверенности и готовности к самостоятельной успешной профессиональной деятельности	ПК-3 - Способен проводить анализ безопасности компьютерных систем	У-1 - Анализировать компьютерную систему с целью определения уровня защищенности и доверия

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации .

2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Модели безопасности компьютерных систем

Электронные ресурсы (издания)

1. Богульская, , Н. А.; Модели безопасности компьютерных систем : учебное пособие.; Сибирский федеральный университет, Красноярск; 2019; http://www.iprbookshop.ru/100055.html (Электронное издание)

Печатные издания

1. Гайдамакин, Н. А.; Разграничение доступа к информации в компьютерных системах; Изд-во Урал. ун-та, Екатеринбург; 2003 (23 экз.)

2. Гайдамакин, Н. А.; Автоматизированные информационные системы, базы и банки данных : Учеб. пособие. Ч. 2. ; Изд-во Урал. гос. ун-та, Екатеринбург; 1999 (18 экз.)

3. Девянин, П. Н.; Модели безопасности компьютерных систем. Управление доступом и информационными потоками : учеб. пособие для студентов вузов, обучающихся по специальностям направления подгот. 090300 - "Информ. безопасность вычисл., автоматизир. и телекоммуникац. систем" и направлению подгот. 090900 - "Информ. безопасность".; Горячая линия - Телеком, Москва; 2011 (5 экз.)

4. Платонов, В. В.; Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей : учеб. пособие для студентов вузов, обучающихся по специальностям 090102, 090105.; Академия, Москва; 2006 (10 экз.)

Профессиональные базы данных, информационно-справочные системы

Гайдамакин Н.А. Теоретические основы компьютерной безопасности / Гайдамакин

Н.А. — <URL:http://study.urfu.ru/view/Aid_view.aspx?AidId=11073>. — 2008 .— Курс "Теоретические основы компьютерной безопасности" предназначен для студентов специальности "Компьютерная безопасность".

Материалы для лиц с ОВЗ

Весь контент ЭБС представлен в виде файлов специального формата для воспроизведения синтезатором речи, а также в тестовом виде, пригодном для прочтения с использованием экранной лупы и настройкой контрастности.

Базы данных, информационно-справочные и поисковые системы

http://www.intuit.ru/ - Национальный открытый университет «ИНТУИТ»

http://www.edu.ru/ - Федеральный портал. Российское образование.

http://study.ustu.ru –портал информационно-образовательных ресурсов УрФУ

http://rtf.ustu.ru - официальный сайт ИРИТ-РтФ

Портал информационно-образовательных ресурсов УрФУ

http://study.ustu.ru/info/default.aspx

Официальный сайт ИРИТ-РтФ http://rtf.ustu.ru

Официальный сайт кафедры ТОР УрФУ http://tor.rtf.ustu.ru

Сайт библиотеки университета http://lib.urfu.ru/

3. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Модели безопасности компьютерных систем

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием и программным обеспечением

Таблица 3.1

№ п/п	Виды занятий	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения
1	Лекции	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Периферийное устройство Подключение к сети Интернет	Office 365 EDUA1 ShrdSvr ALNG SubsVL MVL PerUsr Faculty EES Свободное ПО:Google Crome
2	Практические занятия	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Персональные компьютеры по количеству обучающихся Подключение к сети Интернет	Office 365 EDUA1 ShrdSvr ALNG SubsVL MVL PerUsr Faculty EES Свободное ПО:Google Crome
3	Консультации	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная	**Не требуется**
4	Текущий контроль и промежуточная аттестация	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная	**Не требуется**
5	Самостоятельная работа студентов	Мебель аудиторная с количеством рабочих мест в	Office 365 EDUA1 ShrdSvr ALNG SubsVL MVL PerUsr Faculty EES

		соответствии с количеством студентов Персональные компьютеры по количеству обучающихся Подключение к сети Интернет	Свободное ПО:Google Crome

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Организационно-правовое обеспечение информационной безопасности

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Бакланов Валентин Викторович	кандидат технических наук, доцент	Доцент	Департамент радиоэлектроники и связи
2	Челноков Владислав Валерьевич	кандидат юридических наук	Доцент	алгебры и фундаментальной информатики

Рекомендовано учебно-методическим советом института Естественных наук и математики

Протокол № _7_ от _21.10.2021_ г.

1. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

Авторы:

- **Бакланов Валентин Викторович, Доцент, Департамент радиоэлектроники и связи**
- **Челноков Владислав Валерьевич, Доцент, алгебры и фундаментальной информатики**

1.1. Технологии реализации, используемые при изучении дисциплины модуля

- Традиционная (репродуктивная) технология
- Разноуровневое (дифференцированное) обучение
    - Базовый уровень

**Базовый I уровень – сохраняет логику самой науки и позволяет получить упрощенное, но верное и полное представление о предмете дисциплины, требует знание системы понятий, умение решать проблемные ситуации. Освоение данного уровня результатов обучения должно обеспечить формирование запланированных компетенций и позволит обучающемуся на минимальном уровне самостоятельности и ответственности выполнять задания;*
Продвинутый II уровень – углубляет и обогащает базовый уровень как по содержанию, так и по глубине проработки материала дисциплины. Это происходит за счет включения дополнительной информации. Данный уровень требует умения решать проблемы в рамках курса и смежных курсов посредством самостоятельной постановки цели и выбора программы действий. Освоение данного уровня результатов обучения позволит обучающемуся повысить уровень самостоятельности и ответственности до творческого применения знаний и умений.

1.2. Содержание дисциплины

Таблица 1.1

Код раздела, темы	Раздел, тема дисциплины*	Содержание
Р1	Основные положения государственной политики в сфере обеспечения информационной безопасности (ИБ) РФ	Основы и содержание информационной безопасности; субъекты и объекты правоотношений в сфере ее обеспечения. Доктрина информационной безопасности РФ. Национальные интересы РФ в информационной сфере и их обеспечение. Виды и источники угроз информационной безопасности РФ.
Р2	Принципы правового регулирования отношений и основные понятия в сфере информации, информационных технологий и защиты информации. Ограничение доступа к информации	Конституционные гарантии интересов личности в информационной сфере. Законодательная база обеспечения ИБ. Разделение информации по категориям доступа. Конфиденциальность информации. Виды информации ограниченного доступа и режимы ее защиты. Разделение информации по категориям доступа. Конфиденциальность информации. Виды информации ограниченного доступа и режимы ее защиты: коммерческая тайна, банковская тайна, налоговая тайна, тайна связи, врачебная тайна. Ответственность за нарушение защиты информации ограниченного доступа.

Р3	Охрана государственной тайны	Государственная тайна (ГТ) как особый вид защищаемой информации; принципы и порядок отнесения сведений к ГТ; перечни сведений, составляющих ГТ. Степени секретности сведений и грифы секретности их носителей. Порядок рассекречивания сведений и их носителей. Распоряжение сведениями, составляющими ГТ. Ограничение прав собственности на информацию в связи с ее засекречиванием. Система защиты ГТ в РФ. Функции, задачи и полномочия органов защиты ГТ.
Р4	Правовое регулирование распространения информации	Разделение информации в зависимости от порядка ее предоставления или распространения. Общедоступная информация, распространение которой ограничено или запрещено и ее виды. Понятие организатора распространения информации в сети «Интернет» и его обязанности. Процедуры ограничения доступа к противозаконно распространяемой информации с использованием информационно-телекоммуникационных сетей. Обеспечение доступа к информации о деятельности государственных органов и органов местного самоуправления.
Р5	Правовая охрана результатов интеллектуальной деятельности в сфере компьютерной информации	Результаты интеллектуальной деятельности, которым предоставляется правовая охрана — интеллектуальная собственность. Виды интеллектуальных прав. Авторское право и его объекты в сфере компьютерной информации. Ответственность за нарушение авторского права. Правомерное использование программ для ЭВМ и баз данных.
Р6	Лицензирование и сертификация в сфере ИБ	Виды лицензируемой деятельности в области защиты информации. Порядок и системы лицензирования. Сертификация (подтверждение соответствия) средств защиты информации и защищенных автоматизированных систем. Системы и порядок сертификации ФСТЭК и ФСБ России.
Р7	Преступления в сфере компьютерной информации	Понятие об информационных и компьютерных преступлениях. Компьютер как орудие преступления. Компьютер как средство преступления и хранилище информации о преступной деятельности. Компьютер как предмет преступления. Понятие компьютерной информации. Составы преступлений, предусмотренные ст. 272 – 274.1 УК РФ.
Р8	Организация защиты информации (ЗИ).	Организационные основы ЗИ в учреждении, предприятии. Допуск персонала к защищаемой информации. Организация охраны и внутриобъектового режима. Организация выявления

	Компетенции специалистов в сфере ИБ	и расследования инцидентов ИБ. Взаимосвязь должностей, групп компетенций и видов профессиональной деятельности специалистов в области ИБ. Возможности сотрудничества с правоохранительными органами в сфере ИБ. Права и обязанности лица, выступающего в качестве специалиста или эксперта при расследовании административных правонарушений и уголовных дел.
Р9	Правовое регулирование обработки персональных данных (ПДн). Обеспечение безопасности ПДн в организации	Отношения, регулируемые ФЗ «О персональных данных». Понятия ПДн, оператора ПДн, информационной системы ПДн. Принципы и условия обработки ПДн. Обязанности и права оператора ПДн. Права субъекта ПДн. Биометрические ПДн и правила их обработки. Специальные категории ПДн и условия их обработки. Меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных ФЗ «О персональных данных». Меры, по обеспечению безопасности ПДн при их обработке. Понятие угроз безопасности ПДн. Определение уровня защищенности ПДн. Государственные органы, уполномоченные осуществлять контроль и надзор за выполнением мер по обеспечению безопасности ПДн. Ответственность за правонарушения (преступления) в сфере защиты ПДн. Порядок ограничения доступа к информации, обрабатываемой с нарушением законодательства Российской Федерации в области ПДн.

1.3. Направление, виды воспитательной деятельности и используемые технологии

Таблица 1.2

Направление воспитательной деятельности	Вид воспитательной деятельности	Технология воспитательной деятельности	Компетенция	Результаты обучения
Профессиональное воспитание	учебно-исследовательская, научно-исследовательская	Технология формирования уверенности и готовности к самостоятельной успешной профессиональн	ПК-2 - Способен разрабатывать требования по защите, формирование политик безопасности	П-10 - Выполнять разработку руководящих документов по защите информации в

		ой деятельности	компьютерных систем и сетей	организации

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации .

2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Организационно-правовое обеспечение информационной безопасности

Электронные ресурсы (издания)

1. Рассолов, И. М.; Интернет-право : учебное пособие.; Юнити, Москва; 2015; https://biblioclub.ru/index.php?page=book&id=114528 (Электронное издание)

2. Галатенко, В. А., Бетелин, В. Б.; Стандарты информационной безопасности : курс лекций.; Интернет-Университет Информационных Технологий (ИНТУИТ), Москва; 2006; https://biblioclub.ru/index.php?page=book&id=233065 (Электронное издание)

Печатные издания

1. Гайдамакин, Н. А.; Автоматизированные информационные системы, базы и банки данных. Вводный курс : учеб. пособие для студентов вузов, обучающихся по специальностям "Компьютерная безопасность", "Комплексное обеспечение информ. безопасности автоматизир. систем".; Гелиос АРВ, Москва; 2002 (14 экз.)

2. Гайдамакин, Н. А.; Разграничение доступа к информации в компьютерных системах; Изд-во Урал. ун-та, Екатеринбург; 2003 (23 экз.)

3. Рассолов, И. М.; Информационное право : учеб. для студентов вузов, обучающихся по юрид. специальностям.; Юрайт, Москва; 2011 (32 экз.)

Профессиональные базы данных, информационно-справочные системы

Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и подготовленные проекты документов по технической защите информации

https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty

Нормативные правовые акты в сфере информационных технологий

https://15.rkn.gov.ru/law/p8182/

Материалы для лиц с ОВЗ

Весь контент ЭБС представлен в виде файлов специального формата для воспроизведения синтезатором речи, а также в тестовом виде, пригодном для прочтения с использованием экранной лупы и настройкой контрастности.

Базы данных, информационно-справочные и поисковые системы

http://www.intuit.ru/ - Национальный открытый университет «ИНТУИТ»

http://www.edu.ru/ - Федеральный портал. Российское образование.

http://study.ustu.ru –портал информационно-образовательных ресурсов УрФУ

http://rtf.ustu.ru - официальный сайт ИРИТ-РтФ

Портал информационно-образовательных ресурсов УрФУ http://study.ustu.ru/info/default.aspx

Официальный сайт ИРИТ-РтФ http://rtf.ustu.ru

Официальный сайт кафедры ТОР УрФУ http://tor.rtf.ustu.ru

Сайт библиотеки университета http://lib.urfu.ru/

3. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Организационно-правовое обеспечение информационной безопасности

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием и программным обеспечением

Таблица 3.1

№ п/п	Виды занятий	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения
1	Лекции	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Периферийное устройство Подключение к сети Интернет	Office 365 EDUA1 ShrdSvr ALNG SubsVL MVL PerUsr Faculty EES Свободное ПО:Google Crome
2	Практические занятия	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Персональные компьютеры по количеству обучающихся Подключение к сети Интернет	Office 365 EDUA1 ShrdSvr ALNG SubsVL MVL PerUsr Faculty EES Свободное ПО:Google Crome
3	Консультации	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная	**Не требуется**

4	Текущий контроль и промежуточная аттестация	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная	**Не требуется**
5	Самостоятельная работа студентов	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Персональные компьютеры по количеству обучающихся Подключение к сети Интернет	Office 365 EDUA1 ShrdSvr ALNG SubsVL MVL PerUsr Faculty EES Свободное ПО:Google Crome

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Основы информационной безопасности

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Бакланов Валентин Викторович	кандидат технических наук, доцент	Доцент	Департамент радиоэлектроники и связи

Рекомендовано учебно-методическим советом института Естественных наук и математики

Протокол № _7_ от _21.10.2021_ г.

1. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

Авторы:

- **Бакланов Валентин Викторович, Доцент, Департамент радиоэлектроники и связи**

1.1. Технологии реализации, используемые при изучении дисциплины модуля

- Традиционная (репродуктивная) технология
- Разноуровневое (дифференцированное) обучение
  - Базовый уровень

**Базовый I уровень – сохраняет логику самой науки и позволяет получить упрощенное, но верное и полное представление о предмете дисциплины, требует знание системы понятий, умение решать проблемные ситуации. Освоение данного уровня результатов обучения должно обеспечить формирование запланированных компетенций и позволит обучающемуся на минимальном уровне самостоятельности и ответственности выполнять задания;*
Продвинутый II уровень – углубляет и обогащает базовый уровень как по содержанию, так и по глубине проработки материала дисциплины. Это происходит за счет включения дополнительной информации. Данный уровень требует умения решать проблемы в рамках курса и смежных курсов посредством самостоятельной постановки цели и выбора программы действий. Освоение данного уровня результатов обучения позволит обучающемуся повысить уровень самостоятельности и ответственности до творческого применения знаний и умений.

1.2. Содержание дисциплины

Таблица 1.1

Код раздела, темы	Раздел, тема дисциплины*	Содержание
Р1	Информационная безопасность в системе национальной безопасности Российской Федерации	Понятие национальной безопасности. Виды безопасности и сферы жизнедеятельности личности, общества и государства: экономическая, внутриполитическая, социальная, международная, информационная, военная, пограничная, экологическая и другие. Виды защищаемой информации. Основные понятия и общеметодологические принципы теории информационной безопасности. Роль информационной безопасности в обеспечении национальной безопасности государства.
Р2	Информационная война, методы и средства ее ведения	Национальные интересы и угрозы информационной безопасности Российской Федерации в информационной сфере и их обеспечение. Интересы личности в информационной сфере. Интересы общества в информационной сфере. Интересы государства в информационной сфере. Основные составляющие национальных интересов Российской Федерации в информационной сфере. Угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России. Угрозы информационному обеспечению государственной политики Российской Федерации. Угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции

		на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов. Угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России. Внешние источники угроз. Внутренние источники угроз. Направления обеспечения информационной безопасности государства. Проблемы региональной информационной безопасности. Информационная безопасность и информационное противоборство. Субъекты информационного противоборства. Цели информационного противоборства. Составные части и методы информационного противоборства. Информационное оружие, его классификация и возможности.

1.3. Направление, виды воспитательной деятельности и используемые технологии

Таблица 1.2

Направление воспитательной деятельности	Вид воспитательной деятельности	Технология воспитательной деятельности	Компетенция	Результаты обучения
Профессиональное воспитание	учебно-исследовательская, научно-исследовательская	Технология формирования уверенности и готовности к самостоятельной успешной профессиональной деятельности	ОПК-1 - Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	У-1 - Оценивать и применять основные методы обеспечения информационной безопасности

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации .

2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основы информационной безопасности

Электронные ресурсы (издания)

1. Галатенко, В. А., Бетелин, В. Б.; Основы информационной безопасности: Курс лекций : учебное пособие.; Интернет-Университет Информационных Технологий (ИНТУИТ), Москва; 2006; https://biblioclub.ru/index.php?page=book&id=233063 (Электронное издание)

2. ; Введение в информационную безопасность и защиту информации : учебное пособие.; Новосибирский государственный технический университет, Новосибирск; 2017; https://biblioclub.ru/index.php?page=book&id=575113 (Электронное издание)

Печатные издания

1. Расторгуев, С. П.; Основы информационной безопасности : учеб. пособие для студентов вузов, обучающихся по специальностям "Компьютерная безопасность", "Комплексное обеспечение информ. безопасности автоматизир. систем" и "Информ. безопасность телекоммуникац. систем".; Академия, Москва; 2009 (11 экз.)

2. , Белов, Е. Б., Лось, В. П., Мещеряков, Р. В., Шелупанов, А. А.; Основы информационной безопасности : учеб. пособие для студентов вузов, обучающихся по специальностям в области информ. безопасности.; Горячая линия - Телеком, Москва; 2006 (26 экз.)

3. Бакланов, В. В.; Введение в информационную безопасность. Направления информационной защиты : курс лекций.; Изд-во Уральского университета, Екатеринбург; 2007 (3 экз.)

Профессиональные базы данных, информационно-справочные системы

1. Бакланов, В. В. Основы информационной безопасности / Бакланов В.В. — 2007. — Курс "Основы информационной безопасности" является по своей сути введением в специальность "Компьютерная безопасность". Рассматриваются исторически сложившиеся направления информационной защиты. Излагаются качественные модели информационной защиты. Обсуждаются информационные преступления и информационные войны. Включает учебное пособие, программу дисциплины, экзаменационные материалы, презентации. Предназначен для студентов специальности "Компьютерная безопасность". — в корпоративной сети УрФУ. — <URL:http://study.urfu.ru/view/Aid_view.aspx?AidId=11063>.

2. Бакланов, В. В. Основы информационной безопасности / Бакланов В.В., Вострецова Е.В., Гайдамакин Н.А., Лучинин А.С. — УМК. — 2010 .— Дисциплина «Основы информационной безопасности» имеет целью обучить студентов принципам обеспечения информационной безопасности государства, подходам к анализу его информационной инфраструктуры и решению задач обеспечения информационной безопасности компьютерных систем. «Основы информационной безопасности» в соответствии с государственными образовательными стандартами является обязательной дисциплиной для специальности Информационная безопасность телекоммуникационных систем. — в корпоративной сети УрФУ .—

<URL:http://study.urfu.ru/view/Aid_view.aspx?AidId=9407>.

Материалы для лиц с ОВЗ

Весь контент ЭБС представлен в виде файлов специального формата для воспроизведения синтезатором речи, а также в тестовом виде, пригодном для прочтения с использованием экранной лупы и настройкой контрастности.

Базы данных, информационно-справочные и поисковые системы

http://www.intuit.ru/ - Национальный открытый университет «ИНТУИТ»

http://www.edu.ru/ - Федеральный портал. Российское образование.

http://study.ustu.ru –портал информационно-образовательных ресурсов УрФУ

http://rtf.ustu.ru - официальный сайт ИРИТ-РтФ

Портал информационно-образовательных ресурсов УрФУ http://study.ustu.ru/info/default.aspx

Официальный сайт ИРИТ-РтФ http://rtf.ustu.ru

Официальный сайт кафедры ТОР УрФУ http://tor.rtf.ustu.ru

Сайт библиотеки университета http://lib.urfu.ru/

3. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основы информационной безопасности

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием и программным обеспечением

Таблица 3.1

№ п/п	Виды занятий	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения
1	Лекции	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Периферийное устройство Подключение к сети Интернет	Office 365 EDUA1 ShrdSvr ALNG SubsVL MVL PerUsr Faculty EES Свободное ПО:Google Crome
2	Консультации	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная	**Не требуется**
3	Текущий контроль и промежуточная аттестация	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная	**Не требуется**
4	Самостоятельная работа студентов	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов	Office 365 EDUA1 ShrdSvr ALNG SubsVL MVL PerUsr Faculty EES Свободное ПО:Google Crome

		Персональные компьютеры по количеству обучающихся Подключение к сети Интернет	

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Защита информации от утечки по техническим каналам

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Бакланов Валентин Викторович	кандидат технических наук, доцент	Доцент	Департамент радиоэлектроники и связи
2	Лучинин Александр Сергеевич	кандидат технических наук, доцент	Доцент	Департамент радиоэлектроники и связи

Рекомендовано учебно-методическим советом института Естественных наук и математики

Протокол № _7_ от _21.10.2021_ г.

1. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

Авторы:

- **Бакланов Валентин Викторович, Доцент, Департамент радиоэлектроники и связи**
- **Лучинин Александр Сергеевич, Доцент, Департамент радиоэлектроники и связи**

1.1. Технологии реализации, используемые при изучении дисциплины модуля

- Традиционная (репродуктивная) технология
- Разноуровневое (дифференцированное) обучение
  - Базовый уровень

**Базовый I уровень – сохраняет логику самой науки и позволяет получить упрощенное, но верное и полное представление о предмете дисциплины, требует знание системы понятий, умение решать проблемные ситуации. Освоение данного уровня результатов обучения должно обеспечить формирование запланированных компетенций и позволит обучающемуся на минимальном уровне самостоятельности и ответственности выполнять задания;*
Продвинутый II уровень – углубляет и обогащает базовый уровень как по содержанию, так и по глубине проработки материала дисциплины. Это происходит за счет включения дополнительной информации. Данный уровень требует умения решать проблемы в рамках курса и смежных курсов посредством самостоятельной постановки цели и выбора программы действий. Освоение данного уровня результатов обучения позволит обучающемуся повысить уровень самостоятельности и ответственности до творческого применения знаний и умений.

1.2. Содержание дисциплины

Таблица 1.1

Код раздела, темы	Раздел, тема дисциплины*	Содержание
Р1	Концепция технической защиты информации	Характеристика технической защиты информации как области информационной безопасности. Основные проблемы технической защиты информации. Представление сил и средств защиты информации в виде системы. Основные параметры системы защиты информации. Цели и задачи защиты информации. Ресурсы, выделяемы на защиту информации. Принципы защиты информации техническими средствами. Основные направления технической защиты информации. Показатели эффективности технической защиты информации.
Р2	Теоретические основы технической защиты информации	Информации как предмет защиты. Источники опасных сигналов. Понятие об опасном сигнале. Основные и вспомогательные технические средства и системы как источники опасных сигналов. Характеристика технической разведки. Основные задачи и органы технической разведки. Принципы технической разведки. Основные этапы и процессы добывания информации технической разведкой. Классификация технической разведки. Технические каналы утечки информации. Понятие и особенности утечки информации. Структура, классификация и основные характеристики технических каналов утечки информации. Средства технической разведки. Визуально-

		оптические приборы. Оптоэлектронные приборы наблюдения в видимом и инфракрасном диапазонах. Акустические приемники. Экранирование. Компенсация излучения двухпроводной линии. Применение витых пар. Электростатические экраны. Влияние крышек и металлических корпусов. Одновременное экранирование электрического и магнитного полей. Влияние отверстий и щелей. Конструкция крышек экранов. Экранирование электромагнитного поля излучения. Организованные каналы утечки (съема) информации – закладные устройства. Закладные устройства с проводными каналами передачи. Типы закладных устройств. Примеры схемных реализаций и конструктивного исполнения. Обеспечение энергетической скрытности. Проблемы обнаружения и борьбы с закладными устройствами. Потенциал радиоканала.
Р3	Методы и технические средства обнаружения каналов утечки информации. Методы и технические средства защиты информации	Методы обнаружения каналов утечки по ПЭМИН и через закладные устройства. Физические процессы при подавлении опасных сигналов. Методы инженерной защиты и технической охраны объектов. Классификация способов инженерной защиты и технической охраны объектов. Методы скрытия информации и ее носителей. Пространственное скрытие объектов наблюдения и сигналов. Структурное и энергетическое скрытие объектов наблюдения. Средства предотвращения утечки информации по техническим каналам. Средства маскировки и дезинформирования в оптическом и радиодиапазонах. Средства звукоизоляции из звукопоглощения. Средства обнаружения, локализации и подавления сигналов закладных устройств.
Р4	Организационные основы технической защиты информации	Государственная система защиты информации. Основные задачи, структура и характеристика государственной системы противодействия технической разведке. Основные руководящие, нормативные и методические документы по защите информации и противодействия технической разведке. Основные организационные и технические меры по защите информации. Аттестация объектов, лицензирование деятельности по защите информации и сертифицирование ее средств. Контроль эффективности инженернотехнической защиты информации. Виды контроля эффективности инженерно-технической защиты информации. Виды зон безопасности. Методы технического контроля. Особенности инструментального контроля эффективности инженерно-технической защиты информации.

1.3. Направление, виды воспитательной деятельности и используемые технологии

Таблица 1.2

Направление воспитательной деятельности	Вид воспитательной деятельности	Технология воспитательной деятельности	Компетенция	Результаты обучения

Профессиональное воспитание	учебно-исследовательская, научно-исследовательская	Технология формирования уверенности и готовности к самостоятельной успешной профессиональной деятельности	ОПК-4 - Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности	У-2 - Анализировать и применять модели явлений, процессов и объектов (включая схемы электронных устройств) при решении инженерных задач в профессиональной деятельности

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации .

2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Защита информации от утечки по техническим каналам

Электронные ресурсы (издания)

1. Голиков, А. М.; Защита информации от утечки по техническим каналам : учебное пособие.; Томский государственный университет систем управления и радиоэлектроники, Томск; 2015; https://biblioclub.ru/index.php?page=book&id=480636 (Электронное издание)

Печатные издания

1. Бузов, Г. А., Калинин, С. В., Кондратьев, А. В.; Защита от утечки информации по техническим каналам : учеб. пособие для подгот. экспертов системы Гостехкомиссии России.; Горячая линия - Телеком, Москва; 2005 (17 экз.)

2. Торокин, А. А.; Инженерно-техническая защита информации : учеб. пособие для студентов вузов, обучающихся по специальностям в области информ. безопасности.; Гелиос АРВ, Москва; 2005 (15 экз.)

3. Мельников, В. П., Клейменов, С. А., Петраков, А. М.; Информационная безопасность и защита информации : учеб. пособие для студентов вузов, обучающихся по специальности 230201 "Информ. системы и технологии".; Академия, Москва; 2009 (5 экз.)

4. Меньшаков, Ю. К.; Защита объектов и информации от технических средств разведки : Учеб. пособие.; РГГУ, Москва; 2002 (20 экз.)

5. Петраков, А. В.; Основы практической защиты информации : Учеб. пособие по специальности 20. 18. 00 "Защищенные системы связи".; Радио и связь, Москва; 2001 (10 экз.)

Профессиональные базы данных, информационно-справочные системы

Материалы для лиц с ОВЗ

Весь контент ЭБС представлен в виде файлов специального формата для воспроизведения синтезатором речи, а также в тестовом виде, пригодном для прочтения с использованием экранной лупы и настройкой контрастности.

Базы данных, информационно-справочные и поисковые системы

http://www.intuit.ru/ - Национальный открытый университет «ИНТУИТ»

http://www.edu.ru/ - Федеральный портал. Российское образование.

http://study.ustu.ru –портал информационно-образовательных ресурсов УрФУ

http://rtf.ustu.ru - официальный сайт ИРИТ-РтФ

Портал информационно-образовательных ресурсов УрФУ http://study.ustu.ru/info/default.aspx

Официальный сайт ИРИТ-РтФ http://rtf.ustu.ru

Официальный сайт кафедры ТОР УрФУ http://tor.rtf.ustu.ru

Сайт библиотеки университета http://lib.urfu.ru/

3. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Защита информации от утечки по техническим каналам

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием и программным обеспечением

Таблица 3.1

№ п/п	Виды занятий	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения
1	Лекции	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Периферийное устройство Подключение к сети Интернет	Office 365 EDUA1 ShrdSvr ALNG SubsVL MVL PerUsr Faculty EES Свободное ПО:Google Crome
2	Лабораторные занятия	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная	Office 365 EDUA1 ShrdSvr ALNG SubsVL MVL PerUsr Faculty EES Свободное ПО:Google Crome

		Персональные компьютеры по количеству обучающихся Подключение к сети Интернет	
3	Консультации	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная	**Не требуется**
4	Текущий контроль и промежуточная аттестация	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная	**Не требуется**
5	Самостоятельная работа студентов	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Персональные компьютеры по количеству обучающихся Подключение к сети Интернет	Office 365 EDUA1 ShrdSvr ALNG SubsVL MVL PerUsr Faculty EES Свободное ПО:Google Crome