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
1156038	Защищенные информационные системы

Екатеринбург

Перечень сведений о рабочей программе модуля	Учетные данные
Образовательная программа 1. Защита информации в информационных системах персональных данных, государственных информационных системах и значимых объектах критической информационной инфраструктуры	**Код ОП** 1. 10.04.01/22.01
Направление подготовки 1. Информационная безопасность	**Код направления и уровня подготовки** 1. 10.04.01

Программа модуля составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Коллеров Андрей Сергеевич	к.т.н., доцент	доцент	УНЦ ИБ
2	Пономарева Ольга Алексеевна	кандидат технических наук, без ученого звания	Старший преподаватель	

Согласовано:

Управление образовательных программ Р.Х. Токарева

1. ОБЩАЯ ХАРАКТЕРИСТИКА МОДУЛЯ Защищенные информационные системы

1.1. Аннотация содержания модуля

Целью модуля является формирование знаний и умений в области аудита информационной безопасности систем и средств организации защищенных сетевых коммуникаций, их аттестации по требованиям безопасности информации, организации их развертывания и модернизации, выбора оптимального решения при построении информационной системы (ИС) в зависимости от требований, предъявляемых к ее безопасности и функциональным возможностям. В модуле изучаются особенности организации защищенных сетевых коммуникаций в информационных системах персональных данных, государственных информационных системах и значимых объектах критической информационной инфраструктуры; защитные механизмы телекоммуникационного оборудования; средства терминального доступа; средства организации виртуальных частных сетей; средства межсетевого экранирования; основы пользовательской работы и администрирования защищенной операционной системы; мандатное управление доступом (МУД); мандатный контроль целостности, управление доступом к объектам графической подсистемы, особенности аутентификации и аудита. Студенты проектируют безопасные проводные и беспроводные телемеханические системы, и специализированные вычислительные сети. В модуль входят: - Организация защищенных сетевых коммуникаций в ИСПДн, ГИС и на объектах КИИ; - Методология проектирования защищенных информационных систем; - Защита информации в системах беспроводной связи.

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	Защита информации в системах беспроводной связи	3
2	Организация защищенных сетевых коммуникаций в ИСПДн, ГИС и на объектах КИИ	3
3	Методология проектирования защищенных информационных систем	3
	ИТОГО по модулю:	9

1.3.Последовательность освоения модуля в образовательной программе

Пререквизиты модуля	1. Гуманитарные аспекты информационной безопасности
Постреквизиты и кореквизиты модуля	1. Криптографические методы защиты информации 2. Обнаружение и предупреждение компьютерных атак на объектах критической информационной инфраструктуры (КИИ)

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 в системах беспроводной связи	ПК-2 - Способен проводить анализ безопасности компьютерных систем	З-1 - Различать принципы построения компьютерных систем и сетей З-2 - Распознавать уязвимости компьютерных систем и сетей З-4 - Понимать принципы построения систем управления базами данных З-5 - Использовать средства анализа конфигураций З-6 - Различать национальные, межгосударственные и международные стандарты в области защиты информации 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-3 - Оценивать соответствие механизмов безопасности компьютерной системы требованиям существующих нормативных документов, а также их адекватности существующим рискам П-4 - Готовить аналитический отчет по результатам проведенного анализа

		П-5 - Формулировать предложения по устранению выявленных уязвимостей
	ПК-3 - Способен проводить экспертизу при расследовании компьютерных преступлений, правонарушений и инцидентов	З-1 - Различать уязвимости компьютерных систем и сетей У-1 - Составлять и оформлять аналитический отчет по результатам проведенной экспертизы
Методология проектирования защищенных информационных систем	ПК-1 - Способен решать типовые задачи анализа информации в ИАС государственных органов, обеспечивающих национальную безопасность	У-1 - Проверять гипотезы и границы их применения в задачах анализа информации в ИАС У-2 - Разрабатывать и применять математические модели и методы решения задач анализа информации в ИАС, создавая соответствующее программное и математическое обеспечение
	ПК-2 - Способен проводить анализ безопасности компьютерных систем	У-2 - Прогнозировать возможные пути развития действий нарушителя информационной безопасности П-2 - Оценивать риски, связанные с осуществлением угроз безопасности в отношении компьютерных систем
Организация защищенных сетевых коммуникаций в ИСПДн, ГИС и на объектах КИИ	ПК-1 - Способен решать типовые задачи анализа информации в ИАС государственных органов, обеспечивающих национальную безопасность	З-2 - Определять способы измерения свойств объектов предметной области З-4 - Применять математические модели, методы и алгоритмы решения типовых задач анализа информации в ИАС З-8 - Различать нормативные правовые акты в области защиты информации З-9 - Использовать руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации З-10 - Применять организационные меры по защите информации У-3 - Представлять результаты решения аналитических задач в стандартном виде У-4 - Интерпретировать профессиональный смысл получаемых результатов анализа информации в ИАС

		П-1 - Выдвигать гипотезы, определения границ их применения и подтверждения или опровержения их на практике П-2 - Решать типовые задачи анализа информации в ИАС П-3 - Интерпретировать профессиональный смысл получаемых формальных результатов

1.5. Форма обучения

Обучение по дисциплинам модуля может осуществляться в очной формах.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Защита информации в системах беспроводной связи

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Дудоров Евгений Николаевич	кандидат технических наук, доцент	Доцент	
2	Коллеров Андрей Сергеевич	к.т.н., доцент	доцент	УНЦ ИБ
3	Пономарева Ольга Алексеевна	кандидат технических наук, без ученого звания	Старший преподаватель	

Рекомендовано учебно-методическим советом института Радиоэлектроники и информационных технологий - РТФ

Протокол № _9_ от _20.09.2021_ г.

1. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

Авторы:

- **Дудоров Евгений Николаевич, Доцент,**
- **Коллеров Андрей Сергеевич, доцент, УНЦ ИБ**
- **Пономарева Ольга Алексеевна, Старший преподаватель,**

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
1	Угрозы безопасности беспроводных сетей и модели нарушителей	Особенности передачи данных в неконтролируемой среде. Угроза доступности информации. Угроза целостности информации. Угроза конфиденциальности информации. Определение зоны, в пределах которой может быть осуществлено атакующее воздействие. Основные способы защиты беспроводного канала. Шифрование передаваемой информации. Маскировка канала связи. Смена частоты. Резервирование канала связи. Умышленное изменение стандартного протокола связи. Организация резервного канала связи. Контроль целостности передаваемых данных.
2	Криптографическая защита в беспроводной сети	Угрозы конфиденциальности и целостности данных в беспроводных сетях и их нейтрализация при помощи криптографической защиты. Основные криптографические механизмы защиты информации. Алгоритм DES, алгоритм 3DES, алгоритм AES, алгоритм RSA, алгоритм MD5, алгоритм SHA1. Российские криптографические алгоритмы. Перечень данных, для защиты которых требуется применять Российские криптографические алгоритмы. Причины, по которым в критических системах необходимо использовать алгоритмы по ГОСТ. Сравнение криптостойкости различных алгоритмов.

		Алгоритмы обеспечения целостности передаваемых данных. Распределение ключей шифрования. Внесение избыточности в передаваемую информацию.
3	Безопасность систем спутниковой и радиорелейной связи	Разновидности спутниковой связи: симплексная с обратным наземным каналом и дуплексная. Атака типа «Рыбалка» на абонентов спутниковой связи.
4	Безопасность систем мобильной радиосвязи	Алгоритмы шифрования, применяемые в стандарте GSM. Возможности по злоумышленника по перехвату дешифровке сигнала. Возможности оператора связи по позиционированию абонента. Возможности мобильного терминала по собственному позиционированию. Шпионские функции мобильных терминалов. Скрытая передача данных вредоносным программным обеспечением.
5	Безопасность беспроводных компьютерных сетей (Wi-Fi, Wi-MAX)	Стандарт Wi-Fi. Семейство стандартов IEEE 802.11. Стандарты передачи данных. Разделение на каналы, частотные диапазоны. Основные типы устройств стандарта Wi-Fi. Типы соединений. Проблема «скрытого узла». Разграничение доступа к среде. Сигнал маяка. Идентификатор сети. Обеспечение уникальности идентификатора сети. Стандарты криптографической защиты: WEP, WPA, WPA2. Механизмы распределения ключей PSK, Enterprise. Уязвимости протокола WEP. Протокол смены ключей TKIP. Уязвимости WPA/WPA2. Перехват «рукопожатия» в WPA. Типовой сценарий атаки на беспроводную сеть. Программное обеспечение, позволяющее производить взлом сети. Современные технически возможности по перебору ключа сети. Дополнительные факторы защиты (фильтрация по MAC, скрытие идентификатора сети, ограничение зоны вещания и т.д.). Использование ГОСТовских криптографических алгоритмов путём организации ВЧС туннеля внутри беспроводного соединения. Подавление сигнала Wi-Fi. Мониторинг радио обстановки. Источники активынх/пассивных помех распространению сигнала. Команды управления беспроводной стею. Использование утилит, передающих клиентам сети команды на отключение/смену частоты. Подмена точки доступа. Системы централизованного управления беспроводными точками. Позиционирование абонента. Использование серверов централизованной аутентификации (Контроллер домена, RADIUS и т.д.). Технология MESH. Особенности построения. Преимущества и недостатки. Существующие технические решения. Опасность перехвата информации в транзитных узлах. Стандарт Wi-MAX.
6	Безопасность радиочастотных подключения (Bluetooth)	Частотные и энергетические характеристики Bluetooth. Криптографические алгоритмы, применяемые для защиты Bluetooth. Алгоритм проверки подлинности абонента. Формат

		идентификаторов устройств. Влияние знания идентификатора на безопасность связи.
7	Безопасность охранных радиосистем	Разновидность стандартов передачи данных, используемых для контроля объекта. Использование GSM канала и системы позиционирования ГЛОНАС/GPS. Возможные негативные последствия использования систем дистанционного контроля двигателя (вредоносное ПО для электронных блоков управления двигателем).
8	Правовые аспекты использования беспроводных систем	Распределение частотного ресурса в РФ. Организации, контролирующие использование частот. Нормативные документы, регламентирующие использование частот. Порядок производства и ввоза на территорию РФ радиопередающих устройств. Порядок производства и ввоза на территорию РФ криптографических средств. Ответственность за нарушение правил эксплуатации радиопередающих/принимающих устройства. Лицензирование в области радиосвязи. Лицензирование в сфере услуг предоставления доступа к сетям общего пользования. Использование СОРМ. Права и обязанности оператора мобильной связи по контролю трафика абонента. Возможности по позиционированию абонента. Порядок предоставления данных о положении абонента правоохранительным органам. Возможности по отслеживанию похищенных мобильных терминалов. Текущее законодательство РФ в сфере поиска похищенных мобильных терминалов.

1.3. Направление, виды воспитательной деятельности и используемые технологии

Направления воспитательной деятельности сопрягаются со всеми результатами обучения компетенций по образовательной программе, их освоение обеспечивается содержанием всех дисциплин модулей.

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации .

2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Защита информации в системах беспроводной связи

Электронные ресурсы (издания)

1. , Вострецова, Е. В., Саблина, Н. Г., Самусевич, Г. А.; Моделирование случайных величин : метод. указания для студентов всех форм обучения специальностей 220200 - Автоматизир. системы обраб. информ. и упр., 201200 - Средства связи с подвиж. объектами.; [УМЦ УПИ], Екатеринбург; 2004; http://library.ustu.ru/dspace/handle/123456789/1867 (Электронное издание)

2. , Вострецова, Е. В., Лучинин, А. С.; Электротехника и электроника : метод. указания по выполнению лаб. работ для студентов дистанц. формы обучения направления "Автоматизир. системы обраб. информ. и упр." : [в 2 ч.]. Ч. 1. ; [УГТУ-УПИ], Екатеринбург; 2005; http://library.ustu.ru/dspace/handle/123456789/1863 (Электронное издание)

Печатные издания

1. Прокис, Прокис Дж., Кловский, Д. Д., Николаев, Б. И.; Цифровая связь; Радио и связь, Москва; 2000 (6 экз.)

2. Гаранин, М. В., Журавлев, В. И., Кунегин, С. В.; Системы и сети передачи информации : Учеб. пособие для студентов вузов, обучающихся по специальностям "Криптография", "Компьютерная безопасность", "Комплексное обеспечение информац. безопасности автоматизир. систем", "Информац. безопасность телекоммуникац. систем".; Радио и связь, Москва; 2001 (21 экз.)

3. Столлингс, Столлингс В., Высоцкий, А. В., Голобородько, Н. А., Гроза, Е. Г., Назаренко, А. В.; Беспроводные линии связи и сети; Вильямс, Москва; СПб.; Киев; 2003 (11 экз.)

4. Максим, Максим М., Поллино, Поллино Д., Семенов, А. В.; Безопасность беспроводных сетей; ДМК Пресс : Компания АйТи, Москва; 2004 (2 экз.)

5. , Вишневский, В. М., Ляхов, А. И., Портной, С. Л., Шахнович, И. В.; Широкополосные беспроводные сети передачи информации; Техносфера, Москва; 2005 (8 экз.)

Профессиональные базы данных, информационно-справочные системы

http://www.intuit.ru/intuitdestination=intuituser%2Fuserpage%2F1196462

на курс А.В. Калачев. Аппаратные и программные решения для беспроводных сенсорных сетей.

Учебный курс. 2014 http://www.intuit.ru/goods_store/ebooks/9711

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

Министерство образования и науки Российской Федерации (http:минобрнауки.рф).

Федеральный портал _Российское образование_ (http:www.edu.ru).

ООО Научная электронная библиотека (http:elibrary.ru).

Зональная научная библиотека УрФУ(http:lib.urfu.ru).

Электронный научный архив УрФУ (https://elar.urfu.ru)

3. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Защита информации в системах беспроводной связи

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 Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами Подключение к сети Интернет 1. Сертифицированный программно-аппаратный комплекс межсетевого экранирования. 2. Общесистемное и прикладное программное обеспечение, средства защиты информации.	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES
2	Консультации	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Периферийное устройство Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES

		санитарными правилами и нормами Подключение к сети Интернет 1. Сертифицированный программно-аппаратный комплекс межсетевого экранирования. 2. Общесистемное и прикладное программное обеспечение, средства защиты информации.	
3	Самостоятельная работа студентов	Периферийное устройство Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами Подключение к сети Интернет	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES
4	Лабораторные занятия	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Периферийное устройство Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами Подключение к сети Интернет 1. Сертифицированный программно-аппаратный	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES

		комплекс межсетевого экранирования. 2. Общесистемное и прикладное программное обеспечение, средства защиты информации.	
5	Текущий контроль и промежуточная аттестация	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Периферийное устройство Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами Подключение к сети Интернет 1. Сертифицированный программно-аппаратный комплекс межсетевого экранирования. 2. Общесистемное и прикладное программное обеспечение, средства защиты информации.	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Организация защищенных сетевых коммуникаций в ИСПДн, ГИС и на объектах КИИ

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Агафонов Алексей Владимирович	кандидат технических наук, без ученого звания	Доцент	
2	Пономарева Ольга Алексеевна	кандидат технических наук, без ученого звания	Старший преподаватель	

Рекомендовано учебно-методическим советом института Радиоэлектроники и информационных технологий - РТФ

Протокол № _9_ от _20.09.2021_ г.

1. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

Авторы:

- **Агафонов Алексей Владимирович, Доцент,**
- **Пономарева Ольга Алексеевна, Старший преподаватель,**

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	Особенности организации защищенных сетевых коммуникаций в ИСПДн, ГИС и на объектах КИИ	Нормативные требования к сетям в ИСПДн, ГИС, на объектах КИИ. Методы и средства защиты информации в сетях.
Р2	Защитные механизмы телекоммуникационного оборудования	Средства разграничения доступа к телекоммуникационному оборудованию. Средства контроля доступа к среде передачи данных. Технология VLAN. Агрегирование каналов. Принцип работы средств терминального доступа. Протоколы SSH, X11, RDP, VNC, SPICE.
Р3	Средства организации виртуальных частных сетей	Назначение и принцип работы виртуальных частных сетей. Реализация виртуальных частных сетей на различных уровнях модели OSI. Средства организации виртуальных частных сетей. Назначение и принцип работы межсетевых экранов. Реализация межсетевых экранов на различных уровнях модели OSI. Схемы подключения межсетевых экранов. Межсетевой экран Netfilter. Списки доступа маршрутизаторов Cisco Systems. Прокси-сервер Squid.

1.3. Направление, виды воспитательной деятельности и используемые технологии

Направления воспитательной деятельности сопрягаются со всеми результатами обучения компетенций по образовательной программе, их освоение обеспечивается содержанием всех дисциплин модулей.

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации .

2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Организация защищенных сетевых коммуникаций в ИСПДн, ГИС и на объектах КИИ

Электронные ресурсы (издания)

1. ; Сетевая защита на базе технологий фирмы Cisco Systems. Практический курс : учебное пособие.; Издательство Уральского университета, Екатеринбург; 2014; http://biblioclub.ru/index.phppage=book&id=275694 (Электронное издание)

Печатные издания

1. , Андрончик, А. Н., Богданов, В. В., Домуховский, Н. А., Коллеров, А. С., Синадский, Н. И., Хорьков, Д. А., Щербаков, М. Ю.; Защита информации в компьютерных сетях. Практический курс : учебное пособие для студентов вузов, обучающихся по специальностям 090102 - "Компьютерная безопасность", 090105 - "Комплексное обеспечение информационной безопасности автоматизированных систем", 090106 - "Информационная безопасность телекоммуникационных систем".; УГТУ-УПИ, Екатеринбург; 2008 (1 экз.)

2. , Синадский, Н. И.; Защита информации в компьютерных сетях : практ. курс.; УГТУ-УПИ, Екатеринбург; 2008 (2 экз.)

Профессиональные базы данных, информационно-справочные системы

Официальный сайт Федеральной службы по техническому и экспортному контролю http://www.fstec.ru

Банк данных угроз безопасности информации - Официальный сайт Федеральной службы по техническому и экспортному контролю http://www.fstec.ru

Стандарты - Интернет портал ISO27000.RU http://www.iso27000.ru

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

Министерство образования и науки Российской Федерации (http:минобрнауки.рф).

Федеральный портал _Российское образование_ (http:www.edu.ru).

ООО Научная электронная библиотека (http:elibrary.ru).

Зональная научная библиотека УрФУ(http:lib.urfu.ru).

3. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Организация защищенных сетевых коммуникаций в ИСПДн, ГИС и на объектах КИИ

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 Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами Подключение к сети Интернет 1. Сертифицированный программно-аппаратный комплекс межсетевого экранирования. 2. Общесистемное и прикладное программное обеспечение, средства защиты информации.	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES
2	Консультации	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES

		Доска аудиторная Периферийное устройство Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами Подключение к сети Интернет 1. Сертифицированный программно-аппаратный комплекс межсетевого экранирования. 2. Общесистемное и прикладное программное обеспечение, средства защиты информации.	
3	Самостоятельная работа студентов	Периферийное устройство Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами Подключение к сети Интернет	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES
4	Лабораторные занятия	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Периферийное устройство Персональные компьютеры по количеству обучающихся	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES

		Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами Подключение к сети Интернет 1. Сертифицированный программно-аппаратный комплекс межсетевого экранирования. 2. Общесистемное и прикладное программное обеспечение, средства защиты информации.	
5	Текущий контроль и промежуточная аттестация	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Периферийное устройство Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами Подключение к сети Интернет 1. Сертифицированный программно-аппаратный комплекс межсетевого экранирования. 2. Общесистемное и прикладное программное обеспечение, средства защиты информации.	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Методология проектирования защищенных информационных систем

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Зубков Евгений Валерьевич	кандидат технических наук, без ученого звания	Доцент	
2	Коллеров Андрей Сергеевич	к.т.н., доцент	доцент	УНЦ ИБ
3	Пономарева Ольга Алексеевна	кандидат технических наук, без ученого звания	Старший преподаватель	

Рекомендовано учебно-методическим советом института Радиоэлектроники и информационных технологий - РТФ

Протокол № _9_ от _20.09.2021_ г.

1. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

Авторы:

- **Зубков Евгений Валерьевич, Доцент,**
- **Коллеров Андрей Сергеевич, доцент, УНЦ ИБ**
- **Пономарева Ольга Алексеевна, Старший преподаватель,**

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	Архитектура, назначение и области применения AstraLinux	Понятие защищенной операционной системы; вектор развития организационных и технологических решений; обеспечение конфиденциальности информации; стандартизация и сертификация функциональных решений; требования к процессу разработки критически важного ПО; обобщенная архитектура ОС на базе проекта GNU/Linux; особенности реализации; поддержка различных аппаратных архитектур; варианты модульного ядра проекта GNU/Linux; загружаемые модули ядра (LKM); подсистема PARSEC; организация пользовательских сессий; подсистема Fly; функции общего ПО; сервисы формирования доменной сетевой инфраструктуры; подсистема виртуализации; функции механизмов защиты; области применения.
Р2	Основы пользовательской работы и администрирования	Режимы загрузки ОС; вывод данных из журнала системных событий; последовательность загрузки CLI- и GUI-интерфейсов; диалог выбора атрибутов безопасности; элементы экрана входа в систему; режимы сессии; элемент управления «Меню»; утилита fly-admin-dm; завершение сеанса (утилита fly-shutdown-dialog); менеджер окон (Fly Window Manager); рабочий стол Fly; панель управления (fly-admin-center); интегрированная в Fly поддержка механизмов защиты; файловый менеджер (fly-fm); основные задачи администрирования; администрирование учетных записей

		пользователей и групп; администрирование процессов; администрирование устройств
Р3	Мандатное управление доступом (МУД)	Принципы мандатной сущностно-ролевой ДП-модели управления доступом и информационными потоками в ОС семейства Linux; проблемы реализации МУД в ОС; приемы обхода МУД; двунаправленные информационные потоки; совместимость в прикладным ПО; присвоение уровней конфиденциальности системным и служебным сущностям; асинхронный ввод-вывод; реализация МУД в Astra Linux; повышение защищенности; отказ от SELinux; порядок взаимодействия PARSEC с другими компонентами ОС; настройка мандатных уровней и неиерархических категорий; назначение мандатных атрибутов учетным записям пользователей; мандатные атрибуты текущего сеанса; мандатные уровни корневого и системных каталогов; виртуализация домашних каталогов пользователей; администрирование МУД; использование утилиты «Управление политикой безопасности» (fly-admin-smc); привилегии, связанные с администрированием МУД; параметры МУД для нового сеанса; получение параметров МУД текущего сеанса и сущностей, .
Р4	Мандатный контроль целостности, управление доступом к объектам графической подсистемы, особенности аутентификации и аудита	Принципы работы мандатного контроля целостности; небезопасность X Window System; изоляция сущностей графической подсистемы; запуск приложения в изолированной среде; подключаемые модули аутентификации (Pluggable Authentication Modules – PAM); использование fly-admin-smc для администрирования подсистемы аутентификации (регистрация учетной записи, параметры блокировки учетной записи, настройка аудита, назначение привилегий, сроки действия паролей); утилиты командной строки для работы с привилегиями; настройка общесистемных политик (блокировки, паролей, создания учетных записей пользователей); архитектура аудита PARSEC; утилита просмотра зарегистрированных событий (fly-admin-view); управление политикой аудита с помощью fly-admin-smc; утилиты командной строки для управления подсистемой аудита
Р5	Сетевое взаимодействие в Astra Linux, организация доменной инфраструктуры	Логические уровни сетевой инфраструктуры; формирование базового уровня сетевой инфраструктуры; формирование корпоративного уровня сетевой инфраструктуры; единое пространство пользователей; служба ALD; администрирование доменной сетевой инфраструктуры; служба FreeIPA; формирование гетерогенной доменной сетевой инфраструктуры.

1.3. Направление, виды воспитательной деятельности и используемые технологии

Направления воспитательной деятельности сопрягаются со всеми результатами обучения компетенций по образовательной программе, их освоение обеспечивается содержанием всех дисциплин модулей.

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации .

2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Методология проектирования защищенных информационных систем

Электронные ресурсы (издания)

1. , Вострецова, Е. В., Мальцев, А. П.; Теория радиотехнических сигналов и цепей : Метод. указания к лаб. работам N 5, 6, 7, 8, 9 для студентов всех форм обучения радиотех. специальностей.; УПИ, Екатеринбург; 1992; http://library.ustu.ru/dspace/handle/123456789/499 (Электронное издание)

Печатные издания

1. Петерсен, Петерсен Р.; LINUX: руководство по операционной системе : Пер. с англ..; BHV, Киев; 1997 (2 экз.)

2. Зубков, С. В.; Assembler для DOS, Windows и Unix; ДМК, Москва; 2000 (2 экз.)

3. Уэнстром, М., Сивак, А. Г.; Организация защиты сетей Cisco; Вильямс, Москва [и др.]; 2003 (1 экз.)

Профессиональные базы данных, информационно-справочные системы

Официальный сайт Федеральной службы по техническому и экспортному контролю http://www.fstec.ru

Банк данных угроз безопасности информации - Официальный сайт Федеральной службы по техническому и экспортному контролю http://www.fstec.ru

Стандарты - Интернет портал ISO27000.RU http://www.iso27000.ru

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

Министерство образования и науки Российской Федерации (http:минобрнауки.рф).

Федеральный портал Российское образование (http:www.edu.ru).

ООО Научная электронная библиотека (http:elibrary.ru).

Зональная научная библиотека УрФУ(http:lib.urfu.ru).

Электронный научный архив УрФУ (https://elar.urfu.ru)

3. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Методология проектирования защищенных информационных 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 Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами Подключение к сети Интернет 1. Сертифицированный программно-аппаратный комплекс межсетевого экранирования. 2. Общесистемное и прикладное программное обеспечение, средства защиты информации.	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES
2	Консультации	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Периферийное устройство Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES

		Подключение к сети Интернет 1. Сертифицированный программно-аппаратный комплекс межсетевого экранирования. 2. Общесистемное и прикладное программное обеспечение, средства защиты информации.	
3	Самостоятельная работа студентов	Периферийное устройство Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами Подключение к сети Интернет	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES
4	Лабораторные занятия	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Периферийное устройство Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами Подключение к сети Интернет 1. Сертифицированный программно-аппаратный комплекс межсетевого экранирования.	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES

		2. Общесистемное и прикладное программное обеспечение, средства защиты информации.	
5	Текущий контроль и промежуточная аттестация	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Периферийное устройство Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами Подключение к сети Интернет 1. Сертифицированный программно-аппаратный комплекс межсетевого экранирования. 2. Общесистемное и прикладное программное обеспечение, средства защиты информации.	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES