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
«_07_» июля 2021 г.

РАБОЧАЯ ПРОГРАММА МОДУЛЯ

Код модуля
1156038

Модуль
Защищенные информационные системы)

Екатеринбург, 2021

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

Область образования, в рамках которых реализуется модуль образовательной программы по ФГОС ВО 3++, уровень *магистратура*:

№ п/п	Перечень областей образования, для которых разработан ФГОС ВО 3++	Уровень подготовки
1.	Инженерное дело, технологии и технические науки	*магистратура*

Программа модуля составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Коллеров Андрей Сергеевич	К.т.н., доцент	доцент	*Учебно-научный центр «Информационная безопасность»*
2	Пономарева Ольга Алексеевна		Старший преподаватель	*Учебно-научный центр «Информационная безопасность»*

Руководитель модуля - *С.В. Поршнев*

1. ОБЩАЯ ХАРАКТЕРИСТИКА МОДУЛЯ Защищенные информационные системы

1.1. Аннотация содержания модуля

Целью модуля является изучение принципов построения алгоритмов и протоколов, обеспечивающих безопасность информации, освоение принципов организации и обеспечения работы шифровальных средств, математические методы криптоанализа а также знание нормативно-правовой документации в области применения средств криптографической защиты информации.

В модуль входят: - Криптографические алгоритмы и протоколы; - Криптографические методы и средства защиты в ИСПДн, ГИС и значимых объектах КИИ.

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 и часах
1.	Криптографические алгоритмы и протоколы	*3/108*
2	Криптографические методы и средства защиты в ИСПДн, ГИС и значимых объектах КИИ	*3/108*
	ИТОГО по модулю:	*6/216*

1.3. Последовательность освоения модуля в образовательной программе

Пререквизиты модуля	*Базовое образование по информационной безопасности*
Постреквизиты и корреквизиты модуля	*Методы и средства защиты информации в информационных системах персональных данных (ИСПДн), государственных информационных системах (ГИС) и значимых объектах критической информационной инфраструктуры (КИИ)*

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

Изучение дисциплин модуля предусматривает формирование компетенций посредством последовательного освоения результатов обучения на определенном уровне сложности содержания.

Результаты обучения по дисциплине – это конкретные знания, умения, опыт и другие результаты (содержательные компоненты компетенций), которых планируется достичь на этапе изучения дисциплины модуля и которые должны будут продемонстрированы обучающимися и оценены преподавателем по индикаторам/измеряемым критериям.

Результаты обучения формулируются глаголами в активной форме или отглагольным существительным, должны содержать индикатор/измеряемый критерий (например, самостоятельно формулировать предложения…; понимать/понимание; рассчитывать необходимое количество материалов…/ расчет необходимого количества материалов… и т.д.). При выборе глаголов полезно опираться на таксономию Блума.

Индикатор – это признак / сигнал/ маркер, который показывает, на каком уровне обучающийся должен освоить результаты обучения и их предъявление должно подтвердить факт освоения предметного содержания данной дисциплины.

Индикаторы должны учитываться при выборе и составлении заданий контрольно-оценочных мероприятий (оценочных средств) текущей и промежуточной аттестации.

Таблица 2

Перечень дисциплин модуля	**Код и наименование компетенции**	**Планируемые результаты обучения (индикаторы)**
1	2	3
Методология проектирования защищенных информационных систем Организация защищенных сетевых коммуникаций в ИСПДн, ГИС и на объектах КИИ	ОПК-1 Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	З-1 - знать основы отечественных и зарубежных стандартов в области обеспечения информационной безопасности З-2 - знает направления развития и проблемы компьютерного моделирования сложных систем; направления развития технологий проектирования информационных, автоматизированных и автоматических систем. З-3 - знает современную нормативную базу и ГОСТы, регламентирующие процесс разработки ТЗ. Правила, способы и методы организации совместных разработок. З-4 - знает методы проектирования и построения систем информационной безопасности, включая методы тестирования эффективности и оценки надёжности У-1 - уметь проектировать информационные системы с учетом различных технологий обеспечения информационной безопасности. У-2 - умеет обосновывать и планировать состав и архитектуру моделируемых сложных систем; обосновывать и планировать состав и архитектуру проектируемых информационных, автоматизированных и автоматических систем. У-3 – умеет формировать актуальную модель

		угроз для АИС и учитывать её положения при формировании требований ТЗ на проектируемую систему обеспечения ИБ. У-4 - умеет разрабатывать и обосновывать критерии оценки эффективности проектируемой системы обеспечения ИБ. Оценивать эффективность решений и анализировать показатели деятельности. У-5 - умеет обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности. П-1 - владеть навыками участия в разработке системы обеспечения информационной безопасности объекта. П-2 - владеет навыками разработки концептуальных стратегий решения задач моделирования и проектирования автоматизированных информационных систем и систем обеспечения ИБ. П-3 – владеет навыками планирования и оценки трудоёмкости проекта, включая техническое, кадровое и финансовое обеспечение, принятие совместных решений.

1.5. Форма обучения

Обучение по дисциплинам модуля может осуществляться в очной форме

2. СОДЕРЖАНИЕ И ОБЕСПЕЧЕНИЕ РЕАЛИЗАЦИИ ДИСЦИПЛИН МОДУЛЯ

ПРОГРАММА МОДУЛЯ

Защищенные информационные системы

РАЗДЕЛ 2. СОДЕРЖАНИЕ И ОБЕСПЕЧЕНИЕ РЕАЛИЗАЦИИ ДИСЦИПЛИН МОДУЛЯ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ 1

Методология проектирования защищенных информационных систем

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Дудоров Евгений Николаевич	К.т.н., доцент	доцент	*Учебно-научный центр «Информационная безопасность»*

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

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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

МЕТОДОЛОГИЯ ПРОЕКТИРОВАНИЯ ЗАЩИЩЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Перечень сведений о рабочей программе дисциплины	**Учетные данные**
Модуль Защищенные информационные системы	Код модуля М 1.2
Образовательная программа Защита информации в информационных системах персональных данных, государственных информационных системах и значимых объектах критической информационной инфраструктуры	**Код ОП** 10.04.01
Направление подготовки Информационная безопасность	**Код направления и уровня подготовки** 10.04.01
Уровень подготовки Магистр	
ФГОС ВО	**Реквизиты приказа Минобрнауки РФ об утверждении ФГОС ВО: 01.12.2016 приказ № 1513**

Екатеринбург, 2020

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Поршнев Сергей Владимирович	д.т.н., профессор	Профессор, директор подразделения	Учебно-научный центр «Информационная безопасность»
2	Долганов Антон Юрьевич	Кандидат технических наук	Доцент, младший научный сотрудник	Кафедра радиоэлектроники и телекоммуникаций, ИРИТ-РТФ
3	Зубков Евгений Валерьевич	к.т.н.	Доцент	Учебно-научный центр «Информационная безопасность»

Рекомендовано учебно-методическим советом Института радиоэлектроники и информационных технологий-РтФ
Председатель учебно-методического совета Т.И. Алферьева
Протокол № 4 от 24 апреля 2020 г.

Согласовано:

Дирекция образовательных программ Р.Х. Токарева

1. ОБЩАЯ ХАРАКТЕРИСТИКА ДИСЦИПЛИНЫ «Методология проектирования защищенных информационных систем»

1.1. Аннотация содержания дисциплины

Дисциплина «Методология проектирования защищенных информационных систем» обеспечивает формирование у студентов знаний, необходимых для выбора оптимального решения при построении информационной системы (ИС) в зависимости от требований, предъявляемых к ее безопасности и функциональным возможностям. Студенты, изучившие курс, могут принимать участие в работах по проектированию и реализации информационных систем и настройке механизмов информационной безопасности.

Целью дисциплины является систематизация и формирование профессиональных знаний в области технических решений, используемых при построении ИС и влияющих на ее безопасность.

1.2. Язык реализации программы – русский.

1.3. Планируемые результаты обучения по дисциплине

Результатом обучения в рамках дисциплины является формирование у студентов следующих компетенций:

ПК-1 – способность анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты;

ПК-2 – способность разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности;

ПК-3 – способность проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов;

ПК-4 – способность разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности.

В результате освоения дисциплины студент должен:

Знать:

- архитектуру ОС семейства Linux,
- принципы дискреционной модели управления доступом,
- принципы мандатной сущностно-ролевой ДП-модели управления доступом и информационными потоками,
- способы решения основных задач администрирования,
- принципы построения корпоративного уровня сетевой инфраструктуры.

Уметь:

- формировать политику информационной безопасности путем использования встроенных механизмов разграничения доступа к ресурсам компьютерных систем,
- принимать обоснованное решение при выборе настроек компонентов информационной системы,
- осуществлять планирование и создание учетных записей пользователей и рабочих групп, выполнять настройку разграничения доступа к ресурсам компьютерных систем средствами ОС
- применять графические и консольные утилиты для решения задач администрирования ОС,
- использовать систему аудита событий в интересах безопасности системы.

Владеть:

- методологией проектирования защищенных информационных систем.

1.4. Объем дисциплины

Очная форма обучения

№ п/п	Виды учебной работы	Объем дисциплины		Распределение объема дисциплины по семестрам (час.)
		Всего часов	В т.ч. контактная работа (час.)*	3
1.	**Аудиторные занятия**	36	36	36
2.	Лекции	18	18	18
3.	Практические занятия	-	-	-
4.	Лабораторные работы	18	18	18
5.	**Самостоятельная работа студентов, включая все виды текущей аттестации**	54	5,4	54
6.	**Промежуточная аттестация**	18	2,33	Экзамен, 18
7.	**Общий объем по учебному плану, час.**	108	43,73	108
8.	**Общий объем по учебному плану, з.е.**	3		3

Заочная форма обучения не предусмотрена

*Контактная работа составляет:
в п/п 2,3,4 - количество часов, равное объему соответствующего вида занятий;
в п.5 – количество часов, равное сумме объема времени, выделенного преподавателю на консультации в группе (15% от объема аудиторных занятий) и объема времени, выделенного преподавателю на руководство курсовой работой/проектом одного студента, если она предусмотрена.
в п.6 – количество часов, равное сумме объема времени, выделенного преподавателю на проведение соответствующего вида промежуточной аттестации одного студента и объема времени, выделенного в рамках дисциплины на руководство проектом по модулю (если он предусмотрен) одного студента.

2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код раздела, темы	Раздел, тема дисциплины	Содержание
Р1, Т1	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, Т1	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, Т1	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, .
Р3, Т2	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
Р4, Т1	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.

3. РАСПРЕДЕЛЕНИЕ УЧЕБНОГО ВРЕМЕНИ

3.1. Распределение аудиторной нагрузки и мероприятий самостоятельной работы по разделам дисциплины

Раздел дисциплины			Аудиторные занятия (час.)				Самостоятельная работа: виды, количество и объемы мероприятий																						
Код раздела, темы	Наименование раздела, темы	**Всего по разделу, теме (час.)**	**Всего аудиторной работы (час.)**	Лекции	Практические занятия	Лабораторные работы	**Всего самостоятельной работы студентов (час.)**	Подготовка к аудиторным занятиям (час.)					Выполнение самостоятельных внеаудиторных работ (колич.)											Подготовка к контрольным мероприятиям текущей аттестации (колич.)			Подготов-ка к промежуточной аттестации по дисциплине (час.)		Подготовка в рамках дисциплины к промежуточной аттестации по модулю (час.)	
								Всего (час.)	Лекция	Практ., семинар. занятие	Лабораторное занятие	Н/и семинар, семинар-конфер., коллоквиум (магистратура)	**Всего (час.)**	Домашняя работа*	Графическая работа*	Реферат, эссе, творч. работа*	Проектная работа*	Расчетная работа, разработка программного продукта*	Расчетно-графическая работа*	Домашняя работа на иностр. языке*	Перевод иностр. литературы*	Курсовая работа*	Курсовой проект*	**Всего (час.)**	Контрольная работа*	Коллоквиум*				
Р1 Т1	Архитектура, назначение и области применения AstraLinux	**3**	**2**	2	0	0	**1**	**1**	1		0																	Зачет	Экзамен	Интегрированный экзамен по модулю	Проект по модулю
Р2 Т1	Основы пользовательской работы и администрирования	**14**	**8**	4	0	4	**6**	**6**	2		4																				
Р3 Т1	Мандатное управление доступом	**14**	**8**	4	0	4	**6**	**6**	2		4																				
Р3 Т2	Мандатный контроль целостности, управление доступом к объектам графической подсистемы, особенности аутентификации и аудита	**27**	**8**	4	0	4	**19**	**6**	2		4		**6**	2										7	1					
Р4 Т1	Сетевое взаимодействие в AstraLinux, организация доменной инфраструктуры	**32**	**10**	4	0	6	**22**	**8**	2		6		**14**	2																
	Всего (час), без учета промежуточной аттестации:	**90**	**36**	**18**	**0**	**18**	**54**	**27**	**9**	**0**	**18**	**0**	**20**	**20**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**7**	**7**	**0**				
	Всего по дисциплине (час.):	**108**	**36**				**72**	В т.ч. промежуточная аттестация																			**0**	**18**	**0**	**0**

4. ОРГАНИЗАЦИЯ ПРАКТИЧЕСКИХ ЗАНЯТИЙ, САМОСТОЯТЕЛЬНОЙ РАБОТЫ ПО ДИСЦИПЛИНЕ

4.1 Лабораторные работы

Код раздела, темы	Номер работы	Наименование работы	Время на выполнение работы (час.)
Р2 Т1	1	Работа с учетными записями пользователей и группами	4
Р3 Т1	2	Настройка параметров мандатного управления доступом и мандатного контроля целостности	4
Р3, Т2	3	Организация файловой системы ОССН для работы пользователей в рамках мандатного управления доступом и мандатного контроля целостности	4
Р4 Т1	4	Настройка сетевого взаимодействия	6
		Всего:	18

4.2 Практические занятия

Не предусмотрено

4.3. Примерная тематика самостоятельной работы

4.3.1. Примерный перечень тем домашних работ

- Администрирование ОССН в рамках реализации мандатного контроля целостности.
- Настройка механизмов организации замкнутой программной среды. Контроль целостности комплекса средств защиты.
- Конфигурирование службы Astra Linux Directory.
- Управление программными пакетами. Настройка системных служб.

4.3.2. Примерный перечень тем графических работ

Не предусмотрено

4.3.3. Примерный перечень тем рефератов (эссе, творческих работ)

Не предусмотрено

4.3.4 Примерная тематика индивидуальных или групповых проектов

Не предусмотрено

4.3.5. Примерный перечень тем расчетных работ (программных продуктов)

Не предусмотрено

4.3.6. Примерный перечень тем расчетно-графических работ

Не предусмотрено

4.3.7. Примерный перечень тем курсовых проектов (курсовых работ)

Не предусмотрено

4.3.8. Примерная тематика контрольных работ

- Принципы мандатной сущностно-ролевой ДП-модели управления доступом и информационными потоками в ОС семейства Linux.
- Использование графических утилит и инструментов командной строки для решения задач администрирования Astra Linux.
- Использование Astra Linux в контексте сетевой инфраструктуры.

4.3.9. Примерная тематика коллоквиумов

Не предусмотрено

5. СООТНОШЕНИЕ РАЗДЕЛОВ, ТЕМ ДИСЦИПЛИНЫ И ПРИМЕНЯЕМЫХ ТЕХНОЛОГИЙ ОБУЧЕНИЯ

Код раздела, темы дисциплины	Активные методы обучения						Дистанционные образовательные технологии и электронное обучение					
	Проектная работа	Кейс-анализ	Деловые игры	Проблемное обучение	Командная работа	Другие (указать, какие)	Сетевые учебные курсы	Виртуальные практикумы и тренажеры	Вебинары и видеоконференции	Асинхронные web-конференции и семинары	Совместная работа и разработка контента	Другие (указать, какие)
Р1, Т1 Архитектура, назначение и области применения AstraLinux				*								
Р2, Т1 Основы пользовательской работы и администрирования				*								
Р3, Т1 Мандатное управление доступом				*								
Р3, Т2 Мандатный контроль целостности, управление доступом к объектам графической подсистемы, особенности аутентификации и аудита				*	*							
Р4, Т1 Сетевое взаимодействие в Astra Linux, организация доменной инфраструктуры				*	*							

6. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ (Приложение 1)

7. ПРОЦЕДУРЫ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ (Приложение 2)

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ (Приложение 3)

9. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

9.1.Рекомендуемая литература

9.1.1. Основная литература

1. Шилов, А. К. Управление информационной безопасностью : учебное пособие / А.К. Шилов ; Министерство науки и высшего образования РФ ; Федеральное государственное автономное образовательное учреждение высшего образования «Южный федеральный университет» ; Институт компьютерных технологий и информационной безопасности .— Ростов-на-Дону|Таганрог : Издательство Южного федерального университета, 2018 .— 121 с. : ил. — Библиогр.: с. 81-82. — http://biblioclub.ru/ .— ISBN 978-5-9275-2742-7 .— <URL:http://biblioclub.ru/index.php?page=book&id=500065>.
2. Гончарук, С. В. Администрирование ОС Linux / С.В. Гончарук .— 2-е изд., испр. — Москва : Национальный Открытый Университет «ИНТУИТ», 2016 .— 165 с. : ил., табл. — Библиогр. в кн .— http://biblioclub.ru/ .— <URL:http://biblioclub.ru/index.php?page=book&id=429014>.
3. Ложников, П. С. Средства безопасности операционной системы ROSA Linux : учебное пособие / П.С. Ложников, А.О. Провоторский ; Минобрнауки России ; Омский государственный технический университет .— Омск : Издательство ОмГТУ, 2017 .— 94 с. : табл., ил. — Библиогр. в кн .— http://biblioclub.ru/ .— ISBN 978-5-8149-2502-2 .— <URL:http://biblioclub.ru/index.php?page=book&id=493349>.

9.1.2. Дополнительная литература

1. Ищейнов, В. Я. Информационная безопасность и защита информации: теория и практика : учебное пособие / В.Я. Ищейнов .— Москва|Берлин : Директ-Медиа, 2020 .— 271 с. : схем., табл. — Библиогр. в кн. — http://biblioclub.ru/ .— ISBN 978-5-4499-0496-6 .— <URL:http://biblioclub.ru/index.php?page=book&id=571485>.
2. Бражук, А. И. Сетевые средства Linux / А.И. Бражук .— 2-е изд., исправ. — Москва : Национальный Открытый Университет «ИНТУИТ», 2016 .— 148 с. : схем., ил. — Библиогр. в кн .— http://biblioclub.ru/ .— <URL:http://biblioclub.ru/index.php?page=book&id=428794>.

9.2. Методические разработки

Не предусмотрено

9.3. Программное обеспечение

ОС Astra Linux

9.4. Базы данных, информационно-справочные и поисковые системы

1. http://lib.urfu.ru/ - ЗНБ УрФУ

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

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

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

9.5.Электронные образовательные ресурсы

Не предусмотрено

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием

Специально оборудованная аудитория ИРИТ-РТФ Р-440. Персональные компьютеры –15 шт. Мультимедийный проектор с экраном. Сетевое оборудование. Локальная сеть с выходом в

сеть Интернет.

ПРИЛОЖЕНИЕ 1
к рабочей программе дисциплины

6. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

6.1. Весовой коэффициент значимости дисциплины 0,5.

6.2. Процедуры текущей и промежуточной аттестации по дисциплине

1.Лекции: коэффициент значимости совокупных результатов лекционных занятий – 0,5		
Текущая аттестация на лекциях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Посещение занятий	*3 сем. 1-18 нед.*	*20*
Домашняя работа №1	*3 сем. 1-18 нед.*	*10*
Домашняя работа №2	*3 сем. 1-18 нед.*	*10*
Домашняя работа №3	*3 сем. 1-18 нед.*	*15*
Домашняя работа №4	*3 сем. 1-18 нед.*	*15*
Контрольная работа №1	*3 сем. 1-18 нед.*	*30*
Весовой коэффициент значимости результатов текущей аттестации по лекциям – 0,5		
Промежуточная аттестация по лекциям – *экзамен* **Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – 0,5**		
2. Практические/семинарские занятия: коэффициент значимости совокупных результатов практических/семинарских занятий – *не предусмотрено*		
Текущая аттестация на практических/семинарских занятиях - *не предусмотрена*	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Весовой коэффициент значимости результатов текущей аттестации по практическим/семинарским занятиям– *не предусмотрена*		
Промежуточная аттестация по практическим/семинарским занятиям – *не предусмотрена* **Весовой коэффициент значимости результатов промежуточной аттестации по практическим/семинарским занятиям–** *не предусмотрена*		
3. Лабораторные занятия: коэффициент значимости совокупных результатов лабораторных занятий –1		
Текущая аттестация на лабораторных занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Выполнение лабораторных работ	*3 сем. 1-18 нед.*	*100*
Весовой коэффициент значимости результатов текущей аттестации по лабораторным занятиям – 1		
Промежуточная аттестация по лабораторным занятиям – *не предусмотрена* **Весовой коэффициент значимости результатов промежуточной аттестации по лабораторным занятиям– 1**		

6.3. Процедуры текущей и промежуточной аттестации курсовой работы/проекта

Не предусмотрено

6.4. Коэффициент значимости семестровых результатов освоения дисциплины

Порядковый номер семестра по учебному плану, в котором осваивается дисциплина	Коэффициент значимости результатов освоения дисциплины в семестре
Семестр 3	1

ПРИЛОЖЕНИЕ 2
к рабочей программе дисциплины

7. ПРОЦЕДУРЫ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на сайте ФЭПО http://fepo.i-exam.ru.

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на сайте Интернет-тренажеры http://training.i-exam.ru.

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на портале СМУДС УрФУ.

В связи с отсутствием Дисциплины и ее аналогов, по которым возможно тестирование, на сайтах ФЭПО, Интернет-тренажеры и портале СМУДС УрФУ, тестирование в рамках НТК не производится.

ПРИЛОЖЕНИЕ 3
к рабочей программе дисциплины

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

8.1. КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ КОНТРОЛЬНО-ОЦЕНОЧНЫХ МЕРОПРИЯТИЙ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ В РАМКАХ БРС

В рамках БРС применяются утвержденные в ИРИТ-РТФ критерии оценивания достижений студентов по каждому контрольно-оценочному мероприятию. Система критериев оценивания, как и при проведении промежуточной аттестации по модулю, опирается на три уровня освоения компонентов компетенций: пороговый, повышенный, высокий.

Компоненты компетенций	**Признаки уровня освоения компонентов компетенций**		
	Пороговый	**повышенный**	**высокий**
Знания	Студент демонстрирует знание-знакомство, знание-копию: узнает объекты, явления и понятия, находит в них различия, проявляет знание источников получения информации, может осуществлять самостоятельно репродуктивные действия над знаниями путем самостоятельного воспроизведения и применения информации.	Студент демонстрирует аналитические знания: уверенно воспроизводит и понимает полученные знания, относит их к той или иной классификационной группе, самостоятельно систематизирует их, устанавливает взаимосвязи между ними, продуктивно применяет в знакомых ситуациях.	Студент может самостоятельно извлекать новые знания из окружающего мира, творчески их использовать для принятия решений в новых и нестандартных ситуациях.
Умения	Студент умеет корректно выполнять предписанные действия по инструкции, алгоритму в известной ситуации, самостоятельно выполняет действия по решению типовых задач, требующих выбора из числа известных методов, в предсказуемо изменяющейся ситуации	Студент умеет самостоятельно выполнять действия (приемы, операции) по решению нестандартных задач, требующих выбора на основе комбинации известных методов, в непредсказуемо изменяющейся ситуации	Студент умеет самостоятельно выполнять действия, связанные с решением исследовательских задач, демонстрирует творческое использование умений (технологий)
Личностные качества	Студент имеет низкую мотивацию учебной деятельности, проявляет безразличное, безответственное отношение к учебе, порученному делу	Студент имеет выраженную мотивацию учебной деятельности, демонстрирует позитивное отношение к обучению и будущей трудовой деятельности, проявляет активность.	Студент имеет развитую мотивацию учебной и трудовой деятельности, проявляет настойчивость и увлеченность, трудолюбие, самостоятельность,

			творческий подход.

8.2. КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПРИ ИСПОЛЬЗОВАНИИ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ

Не используется

8.3. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

8.3.1. Примерные задания для проведения контрольных работ в рамках учебных занятий

Тестовые вопросы (правильные ответы отмечены жирным цветом)

1. Защищённой (доверенной) целесообразно считать ОС, которая
   Ответ:
   (1) реализует заданные априорно требования безопасности
   (2) исключает возможность внешнего контроля
   (3) адекватна угрозам безопасности, специфичным для отечественных АС
   (4) для которой отсутствует возможность несанкционированного влияния на её работу извне

2. В современных условиях перспективная отечественная защищённая ОС должна отвечать следующим требованиям:
   Ответ:
   (1) соответствовать требованиям обеспечения технологической независимости (импортозамещения) Российской Федерации в важнейших областях информатизации, телекоммуникации и связи;
   (2) быть пригодной к функционированию в компьютерных сетях, как изолированных, так и подключённых к сети Интернет (или иным телекоммуникационным сетям), в том числе ориентированных на обработку информации, отнесённой к государственной тайне, или персональных данных;
   (3) обеспечивать возможность бесперебойной эксплуатации оборудования и работы в условиях повышенной вычислительной нагрузки;
   (4) реализовывать современные механизмы обеспечения информационной безопасности, учитывающие возможность обработки в данной ОС информации, отнесённой к государственной тайне, как с точки зрения удовлетворения формальных требований соответствующих нормативных документов и стандартов, так и с точки зрения обеспечения реальной защиты от актуальных угроз безопасности.

3. К UNIX-подобным ОС не относится:
   Ответ:
   (1) Linux
   (2) FreeBSD
   (3) Mac OS X
   (4) MS Windowsc

4. Операционная система - это набор программ, реализующий интерфейсы:

Ответ:
(1) между пользователем и программами
(2) между аппаратурой и программами
(3) между пользователем и аппаратурой

5. Малое число компьютерных вирусов для ОС Linux обусловлено
Ответ:

(1) Высоким уровнем защищенности ОС
(2) Низким уровнем популярности ОС
(3) Высокими требованиями к квалификации разработчика компьютерных вирусов
(4) Отсутствием технической документации по архитектуре ОС

6. Предельный уровень защиты версии 1.6 релиза ОССН сертифицирован для использования в многопользовательских АСЗИ, пользователи которых имеют
Ответ:
(1) разные полномочия по доступу к обрабатываемой информации, по классу 3 защиты от НСД и уровню 2 контроля отсутствия НДВ
(2) равные полномочия по доступу к обрабатываемой информации, по классу 3 защиты от НСД и уровню 2 контроля отсутствия НДВ
(3) разные полномочия по доступу к обрабатываемой информации, по классу 2 защиты от НСД и уровню 3 контроля отсутствия НДВ
(4) равные полномочия по доступу к обрабатываемой информации, по классу 2 защиты от НСД и уровню 3 контроля отсутствия НДВ

7. Нормативной основой верификации непротиворечивости МРОСЛ ДП-модели являются
Ответ:
(1) ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества
(2) ГОСТ Р ИСО/МЭК 15408-3-2013 «Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий»
(3) ГОСТ Р 56545-2015 Защита информации. Уязвимости информационных систем. Правила описания уязвимостей
(4) «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий», утверждённые в 2018 г. ФСТЭК России

8. Архитектурной основой ОССН является проект
Ответ:
(1) Mandriva
(2) Debian
(3) CentOS
(4) Ubuntu

9. Обозначение релиза содержится в файле
Ответ:
(1) /etc/os-release
(2) /etc/astra-release
(3) /etc/os_version
(4) /etc/astra_version

10. Информацию о текущей версии релиза и имени релиза можно получить в консольном режиме с помощью команды
    Ответ:
    (1) lsb_release -a
    (2) uname -a
    (3) arch –version

8.3.2. Примерные контрольные задачи в рамках учебных занятий

Не предусмотрено

8.3.3. Примерные контрольные кейсы

Не предусмотрено

8.3.4. Перечень примерных вопросов для зачета

Не предусмотрено

8.3.5. Перечень примерных вопросов для экзамена

Итоговая аттестация проводится в форме экзамена по билетам. Билет к экзамену состоит из теоретического и практического вопросов. Время на подготовку — 45 минут.

Теоретические вопросы:

1. Обобщенная архитектура ОС на базе проекта GNU/Linux.
2. Подсистема PARSEC.
3. Графические утилиты управления системой.
4. Управление системой с помощью инструментов командной строки.
5. Принципы дискреционной модели управления доступом.
6. Принципы мандатной сущностно-ролевой ДП-модели управления доступом и информационными потоками.
7. Уровни доступа, уровни целостности, неиерархические категории.
8. Администрирование подсистемы аутентификации.
9. Специальные атрибуты (CCNR, CCNRI, E_Hole, W_Hole).
10. Настройка сетевой подсистемы.
11. Принципы организации корпоративного уровня сетевой инфраструктуры.

Практические вопросы:

1. Зарегистрировать в системе учетную запись пользователя, войти в систему с различными уровнями доступа и наборами неиерархических категорий, проверить возможность доступа к файлам для разных случаев.
2. Используя консольный режим создать пользователя “user01”, группу “manager”, добавить пользователя в только что созданную группу.
3. Создать каталоги с установленными специальными атрибутами CCNR, CCNRI. Объяснить особенности работы с такими каталогами.
4. Создать файлы с установленными специальными атрибутами E_Hole, W_Hole. Объяснить особенности работы с такими файлами.
5. Используя механизм привилегий осуществить запуск процесса с классификационной меткой, отличной от метки текущего пользователя
6. Отобразить в консоли данные из журнала системных событий системы инициализации systemd.
7. Отобразить содержимого файла /var/log/wtmp
8. Изменить пароль своей учетной записи с помощью графических утилит и инструментов консольного режима.
9. Отобразить в консоли список файлов домашнего каталога со значениями меток конфиденциальности.
10. Отобразить в консоли расширенные списки доступа файла. Добавить в список новое правило.

11. Отобразить в консоли список привилегий текущего пользователя.
12. Отобразить содержимое arp кэша.
13. Отобразить состояние сетевого интерфейса.
14. Отобразить список сетевых портов, ожидающих подключения.
15. Отобразить список установленных сетевых соединений.

8.3.6. Ресурсы АПИМ УрФУ, СКУД УрФУ для проведения тестового контроля в рамках текущей и промежуточной аттестации

Не предусмотрено

8.3.7. Ресурсы ФЭПО для проведения независимого тестового контроля

Не предусмотрено

8.3.8. Интернет-тренажеры

Не предусмотрено

8.3.9. Примерные задания в составе домашних работ

1. Запишите формулу, по которой вычисляется случайное число Y , если его плотность распределения на интервале (a,b) определена, и он поделен на подинтервалы (A(i),A(i+1)),i=0,...,m-1 такие, что вероятность попадания туда у одинакова и равна 1/m; x(j) – случайно распределенное число на интервале (0,1) число, k – случайно выбранное целое число из ряда 0,1,...,m-1.
2. Напишите в чем заключаются основные отличия Гарвардской архитектуры от Фон-Неймановской?

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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ОРГАНИЗАЦИЯ ЗАЩИЩЕННЫХ СЕТЕВЫХ КОММУНИКАЦИЙ В ИСПДН, ГИС И НА ОБЪЕКТАХ КИИ

<table>
<tr><th>Перечень сведений о рабочей программе дисциплины</th><th>Учетные данные</th></tr>
<tr><td>Модуль
Защищенные информационные системы</td><td>Код модуля М 1.2</td></tr>
<tr><td>Образовательная программа
Защита информации в информационных системах персональных данных, государственных информационных системах и значимых объектах критической информационной инфраструктуры</td><td>Код ОП
10.04.01</td></tr>
<tr><td>Направление подготовки
Информационная безопасность</td><td rowspan="2">Код направления и уровня подготовки
10.04.01</td></tr>
<tr><td>Уровень подготовки
Магистр</td></tr>
<tr><td>ФГОС ВО</td><td>Реквизиты приказа Минобрнауки РФ об утверждении ФГОС ВО: 01.12.2016 приказ № 1513</td></tr>
</table>

Екатеринбург, 2020

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Бородин Андрей Михайлович	Кандидат технических наук	Доцент	Учебно-научный центр «Информационная безопасность»
2	Долганов Антон Юрьевич	Кандидат технических наук	Доцент, младший научный сотрудник	Кафедра радиоэлектроники и телекоммуникаций, ИРИТ-РТФ

Рекомендовано учебно-методическим советом Института радиоэлектроники и информационных технологий-РтФ
Председатель учебно-методического совета Т.И. Алферьева
Протокол № 4 от 24 апреля 2020 г.

Согласовано:

Дирекция образовательных программ Р. Х. Токарева

1. ОБЩАЯ ХАРАКТЕРИСТИКА ДИСЦИПЛИНЫ «Организация защищенных сетевых коммуникаций в ИСПДн, ГИС и на объектах КИИ»

1.1. Аннотация содержания дисциплины

Дисциплина «Организация защищенных сетевых коммуникаций в ИСПДн, ГИС и на объектах КИИ» обеспечивает формирование у студентов знаний, необходимых для решения задач в области аудита информационной безопасности систем и средств организации защищенных сетевых коммуникаций, их аттестации по требованиям безопасности информации, организации их развертывания и модернизации. Студенты, изучившие курс, могут разворачивать и модернизировать средства обеспечения защищенных сетевых коммуникаций.

Целью дисциплины является систематизация и формирование профессиональных знаний в области организации комплексной защиты информации, в том числе ИСПДн, ГИС и значимых объектов КИИ.

1.2. Язык реализации программы – русский.

1.3. Планируемые результаты обучения по дисциплине

Результатом обучения в рамках дисциплины является формирование у студентов следующих компетенций:

ПК-9 – способность проводить аудит информационной безопасности информационных систем и объектов информатизации;

ПК-10 – способность проводить аттестацию объектов информатизации по требованиям безопасности информации;

ПК-13 – способность организовать управление информационной безопасностью;

ПК-14 – способность организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России

ПК-16 – способность разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности.

В результате освоения дисциплины студент должен:

Знать:

- особенности аудита информационной безопасности систем и средств организации защищенных сетевых коммуникаций, применяемых в ИСПДн, ГИС и на значимых объектах КИИ,
- особенности аттестации систем и средств организации защищенных сетевых коммуникаций, применяемых в ИСПДн, ГИС и на значимых объектах КИИ,
- особенности управления информационной безопасностью систем, средств и технологий организации защищенных сетевых коммуникаций, применяемых в ИСПДн, ГИС и на значимых объектах КИИ,
- назначение и принципы работы систем и средств организации защищенных сетевых коммуникаций, применяемых в ИСПДн, ГИС и на значимых объектах КИИ,
- нормативную базу для применения систем и средств организации защищенных сетевых коммуникаций в ИСПДн, ГИС и на значимых объектах КИИ,
- состав эксплуатационной документации для систем и средств организации защищенных сетевых коммуникаций, применяемых в ИСПДн, ГИС и на значимых объектах КИИ.

Уметь:

- производить настройку систем и средств организации защищенных сетевых коммуникаций в ИСПДн, ГИС и на значимых объектах КИИ с учетом требований информационной безопасности.

- составлять эксплуатационную документацию для систем и средств организации защищенных сетевых коммуникаций, применяемых в ИСПДн, ГИС и на значимых объектах КИИ.

Владеть:

- методами обеспечения информационной безопасности ИСПДн, ГИС и значимых объектов КИИ с применением систем и средств организации защищенных сетевых коммуникаций.

1.4. Объем дисциплины

Очная форма обучения

№ п/п	Виды учебной работы	Объем дисциплины		Распределение объема дисциплины по семестрам (час.)
		Всего часов	В т.ч. контактная работа (час.)*	2
1.	**Аудиторные занятия**	36	36	36
2.	Лекции	18	18	18
3.	Практические занятия	-	-	-
4.	Лабораторные работы	18	18	18
5.	**Самостоятельная работа студентов, включая все виды текущей аттестации**	54	5,4	54
6.	**Промежуточная аттестация**	18	2,33	Экзамен, 18
7.	**Общий объем по учебному плану, час.**	108	43,73	108
8.	**Общий объем по учебному плану, з.е.**	3		3

Заочная форма обучения не предусмотрена

*Контактная работа составляет:

в п/п 2,3,4 - количество часов, равное объему соответствующего вида занятий;

в п.5 – количество часов, равное сумме объема времени, выделенного преподавателю на консультации в группе (15% от объема аудиторных занятий) и объема времени, выделенного преподавателю на руководство курсовой работой/проектом одного студента, если она предусмотрена.

в п.6 – количество часов, равное сумме объема времени, выделенного преподавателю на проведение соответствующего вида промежуточной аттестации одного студента и объема времени, выделенного в рамках дисциплины на руководство проектом по модулю (если он предусмотрен) одного студента.

2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код раздела, темы	Раздел, тема дисциплины	Содержание
Р1, Т1	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, Т1	Защитные механизмы	Средства разграничения доступа к

	телекоммуникационного оборудования	телекоммуникационному оборудованию. Средства контроля доступа к среде передачи данных. Технология VLAN. Агрегирование каналов.
P2, T2	Средства терминального доступа	Принцип работы средств терминального доступа. Протоколы SSH, X11, RDP, VNC, SPICE.
P2, T3	Средства организации виртуальных частных сетей	Назначение и принцип работы виртуальных частных сетей. Реализация виртуальных частных сетей на различных уровнях модели OSI. Протоколы PPPoE, PPTP, IPsec, SSL/TLS.
P2, T4	Средства межсетевого экранирования	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.

3. РАСПРЕДЕЛЕНИЕ УЧЕБНОГО ВРЕМЕНИ

3.1. Распределение аудиторной нагрузки и мероприятий самостоятельной работы по разделам дисциплины

4. ОРГАНИЗАЦИЯ ПРАКТИЧЕСКИХ ЗАНЯТИЙ, САМОСТОЯТЕЛЬНОЙ РАБОТЫ ПО ДИСЦИПЛИНЕ

4.1 Лабораторные работы

Код раздела, темы	Номер работы	Наименование работы	Время на выполнение работы (час.)
P2, T1	1	Применение телекоммуникационного оборудования для обеспечения информационной безопасности компьютерных сетей	4
P2, T2	2	Организация терминального доступа к компьютерным системам с применением протокола SSH	4
P2, T3	3	Организация виртуальной частной сети с применением ПО ViPNet	4
P2, T4	4	Настройка межсетевого экрана Netfilter	4
P2, T4	5	Настройка прокси-сервера Squid	2
		Всего:	18

4.2 Практические занятия

Не предусмотрено

4.3. Примерная тематика самостоятельной работы

4.3.1. Примерный перечень тем домашних работ

1. Составление пакета эксплуатационной документации для компьютерной сети ИСПДн, ГИС или значимого объекта КИИ.
2. Организация терминального доступа к компьютерным системам с применением протокола X11.
3. Организация виртуальной частной сети с применением ПО OpenVPN
4. Организация защищенного канала передачи данных с применением протокола HTTPS.
5. Защита данных электронной почты с применением ПО КриптоПро.
6. Настройка межсетевого экрана в сети с демилитаризованной зоной и узлом-бастионом.
7. Настройка прокси-сервера для работы в прозрачном режиме.

4.3.2. Примерный перечень тем графических работ

Не предусмотрено

4.3.3. Примерный перечень тем рефератов (эссе, творческих работ)

Не предусмотрено

4.3.4 Примерная тематика индивидуальных или групповых проектов

Не предусмотрено

4.3.5. Примерный перечень тем расчетных работ (программных продуктов)

Не предусмотрено

4.3.6. Примерный перечень тем расчетно-графических работ

Не предусмотрено

4.3.7. Примерный перечень тем курсовых проектов (курсовых работ)

Не предусмотрено

4.3.8. Примерная тематика контрольных работ

1. Нормативные требования к сетям в ИСПДн, ГИС, объектам КИИ.
2. Проверка соответствия настроек средств организации виртуальной частной сети политике информационной безопасности.
3. Проверка соответствия правил межсетевого экранирования политике информационной безопасности.

4.3.9. Примерная тематика коллоквиумов

Не предусмотрено

5. СООТНОШЕНИЕ РАЗДЕЛОВ, ТЕМ ДИСЦИПЛИНЫ И ПРИМЕНЯЕМЫХ ТЕХНОЛОГИЙ ОБУЧЕНИЯ

Код раздела, темы дисциплины	Активные методы обучения						Дистанционные образовательные технологии и электронное обучение					
	Проектная работа	Кейс-анализ	Деловые игры	Проблемное обучение	Командная работа	Другие (указать, какие)	Сетевые учебные курсы	Виртуальные практикумы и тренажеры	Вебинары и видеоконференции	Асинхронные web-конференции и семинары	Совместная работа и разработка контента	Другие (указать, какие)
Р1.Т1. Особенности организации защищенных сетевых коммуникаций в ИСПДн, ГИС и на объектах КИИ				*								
Р2.Т1. Защитные механизмы телекоммуникационного оборудования				*								
Р2.Т2. Средства терминального доступа				*								
Р2.Т3. Средства организации виртуальных частных сетей				*								
Р2.Т4. Средства межсетевого экранирования				*								

6. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ (Приложение 1)

7. ПРОЦЕДУРЫ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ (Приложение 2)

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ (Приложение 3)

9. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

9.1.Рекомендуемая литература

9.1.1. Основная литература

1. Сетевая защита на базе технологий фирмы Cisco Systems. Практический курс : учебное пособие / А.Н. Андрончик, А.С. Коллеров, Н.И. Синадский, М.Ю. Щербаков ; под общ. ред. Н. И. Синадский ; Министерство образования и науки Российской Федерации ; Уральский федеральный университет им. первого Президента России Б. Н. Ельцина .— Екатеринбург : Издательство Уральского университета, 2014 .— 179 с. : ил. — Библиогр. в кн .— http://biblioclub.ru/ .— ISBN 978-5-7996-1201-6 .— <URL:http://biblioclub.ru/index.php?page=book&id=275694>.
2. Романец, Юрий Васильевич. Защита информации в компьютерных системах и сетях / Ю.В. Романец, П.А. Тимофеев, В.Ф. Шаньгин; Под ред. В.Ф. Шаньгина .— 2-е изд., перераб. и доп. — М. : Радио и связь, 2001 .— 376 с. : ил. ; 22 см .— Библиогр.: с. 366-372 (126 назв.). — без грифа .— ISBN 5-256-01518-4 : 97.51.

9.1.2. Дополнительная литература

1. Сетевая защита на базе технологий фирмы Cisco Systems. Практический курс : учебное пособие / А.Н. Андрончик, А.С. Коллеров, Н.И. Синадский, М.Ю. Щербаков ; под общ. ред. Н. И. Синадский ; Министерство образования и науки Российской Федерации ; Уральский федеральный университет им. первого Президента России Б. Н. Ельцина .— Екатеринбург : Издательство Уральского университета, 2014 .— 179 с. : ил. — Библиогр. в кн .— http://biblioclub.ru/ .— ISBN 978-5-7996-1201-6 .— <URL:http://biblioclub.ru/index.php?page=book&id=275694>.
2. A Complete Guide to the Common Vulnerability Scoring System Version 3.0 [Электронный ресурс] http://www.first.org/cvss/cvss-guide.html.

9.1.3. Правовые нормативные акты

1. Выписка из концепции государственной системы обнаружения, предупреждения и ликвидации компьютерных атак на информационные ресурсы Российской Федерации (Концепция утверждена Президентом Российской Федерации 12 декабря 2014 г. № К 1274).
2. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
3. Приказ ФСТЭК России от 14 марта 2014 г. № 31 «Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».
4. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. — М.: 2007.
5. ГОСТ Р ИСО/МЭК 15408-1-2012. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. — М.: 2012.

6. ГОСТ Р ИСО/МЭК 15408-2-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности. — М.: 2013.
7. ГОСТ Р ИСО/МЭК 15408-3-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности. — М.: 2013.
8. ГОСТ Р ИСО/МЭК 17799-2006. Информационная технология. Практические правила управления информационной безопасностью. — М.: 2006.
9. СТО БР ИББС-1.0-2014.Обеспечение информационной безопасности организаций банковской системы Российской федерации. Общие положения.
10. СТО БР ИББС-1.1-2007. Аудит информационной безопасности.
11. РС БР ИББС-2.1-2007. Руководство по самооценке соответствия информационной безопасности организации банковской системы РФ требованиям СТО БР ИББС-1.0-2006.
12. СТО БР ИББС-1.2-2014. Методика оценки соответствия информационной безопасности организации банковской системы РФ требованиям СТО БР ИББС-1.0-2014.

9.2. Методические разработки

Не предусмотрено

9.3. Программное обеспечение

Дистрибутивы ПО ViPNet, КриптоПро (демонстрационные версии)

ОС Astra Linux SE 1.6.

9.4. Базы данных, информационно-справочные и поисковые системы

1. http://lib.urfu.ru/ - ЗНБ УрФУ

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

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

4. http://rtf.urfu.ru - официальный сайт ИРИТ-РтФ

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

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

9.5.Электронные образовательные ресурсы

Не предусмотрено

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием

Специально оборудованная аудитория ИРИТ-РТФ Р-440. Персональные компьютеры –15 шт. Мультимедийный проектор с экраном. Сетевое оборудование. Локальная сеть с выходом в сеть Интернет.

ПРИЛОЖЕНИЕ 1
к рабочей программе дисциплины

6. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

6.1. Весовой коэффициент значимости дисциплины 0,5.

6.2. Процедуры текущей и промежуточной аттестации по дисциплине

1.Лекции: коэффициент значимости совокупных результатов лекционных занятий – 0,5		
Текущая аттестация на лекциях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Посещение занятий	*2 сем. 1-18 нед.*	*20*
Домашняя работа №1	*2 сем. 1-18 нед.*	*15*
Домашняя работа №2	*2 сем. 1-18 нед.*	*15*
Домашняя работа №3	*2 сем. 1-18 нед.*	*15*
Домашняя работа №4	*2 сем. 1-18 нед.*	*15*
Контрольная работа №1	*2 сем. 1-18 нед.*	*20*
Весовой коэффициент значимости результатов текущей аттестации по лекциям – 0,5		
Промежуточная аттестация по лекциям – *экзамен* **Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – 0,5**		
2. Практические/семинарские занятия: коэффициент значимости совокупных результатов практических/семинарских занятий – 0		
Текущая аттестация на практических/семинарских занятиях - – *не предусмотрена*	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Весовой коэффициент значимости результатов текущей аттестации по практическим/семинарским занятиям – 0		
Промежуточная аттестация по практическим/семинарским занятиям – *не предусмотрена* **Весовой коэффициент значимости результатов промежуточной аттестации по практическим/семинарским занятиям– 0**		
3. Лабораторные занятия: коэффициент значимости совокупных результатов лабораторных занятий – 0,5		
Текущая аттестация на лабораторных занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Выполнение лабораторных работ	*2 сем. 1-18 нед.*	*100*
Весовой коэффициент значимости результатов текущей аттестации по лабораторным занятиям – 1		
Промежуточная аттестация по лабораторным занятиям – *не предусмотрена* **Весовой коэффициент значимости результатов промежуточной аттестации по лабораторным занятиям– 0**		

6.3. Процедуры текущей и промежуточной аттестации курсовой работы/проекта

Не предусмотрено

6.4. Коэффициент значимости семестровых результатов освоения дисциплины

Порядковый номер семестра по учебному плану, в котором осваивается дисциплина	Коэффициент значимости результатов освоения дисциплины в семестре
Семестр 2	1

ПРИЛОЖЕНИЕ 2
к рабочей программе дисциплины

7. ПРОЦЕДУРЫ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на сайте ФЭПО http://fepo.i-exam.ru.

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на сайте Интернет-тренажеры http://training.i-exam.ru.

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на портале СМУДС УрФУ.

В связи с отсутствием Дисциплины и ее аналогов, по которым возможно тестирование, на сайтах ФЭПО, Интернет-тренажеры и портале СМУДС УрФУ, тестирование в рамках НТК не производится.

ПРИЛОЖЕНИЕ 3
к рабочей программе дисциплины

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

8.1. КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ КОНТРОЛЬНО-ОЦЕНОЧНЫХ МЕРОПРИЯТИЙ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ В РАМКАХ БРС

В рамках БРС применяются утвержденные в ИРИТ-РТФ критерии оценивания достижений студентов по каждому контрольно-оценочному мероприятию. Система критериев оценивания, как и при проведении промежуточной аттестации по модулю, опирается на три уровня освоения компонентов компетенций: пороговый, повышенный, высокий.

Компоненты компетенций	**Признаки уровня освоения компонентов компетенций**		
	Пороговый	**повышенный**	**высокий**
Знания	Студент демонстрирует знание-знакомство, знание-копию: узнает объекты, явления и понятия, находит в них различия, проявляет знание источников получения информации, может осуществлять самостоятельно репродуктивные действия над знаниями путем самостоятельного воспроизведения и применения информации.	Студент демонстрирует аналитические знания: уверенно воспроизводит и понимает полученные знания, относит их к той или иной классификационной группе, самостоятельно систематизирует их, устанавливает взаимосвязи между ними, продуктивно применяет в знакомых ситуациях.	Студент может самостоятельно извлекать новые знания из окружающего мира, творчески их использовать для принятия решений в новых и нестандартных ситуациях.
Умения	Студент умеет корректно выполнять предписанные действия по инструкции, алгоритму в известной ситуации, самостоятельно выполняет действия по решению типовых задач, требующих выбора из числа известных методов, в предсказуемо изменяющейся ситуации	Студент умеет самостоятельно выполнять действия (приемы, операции) по решению нестандартных задач, требующих выбора на основе комбинации известных методов, в непредсказуемо изменяющейся ситуации	Студент умеет самостоятельно выполнять действия, связанные с решением исследовательских задач, демонстрирует творческое использование умений (технологий)
Личностные качества	Студент имеет низкую мотивацию учебной деятельности, проявляет безразличное, безответственное отношение к учебе, порученному делу	Студент имеет выраженную мотивацию учебной деятельности, демонстрирует позитивное отношение к обучению и будущей трудовой деятельности, проявляет активность.	Студент имеет развитую мотивацию учебной и трудовой деятельности, проявляет настойчивость и увлеченность, трудолюбие, самостоятельность,

			творческий подход.

8.2. КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПРИ ИСПОЛЬЗОВАНИИ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ

Не используется

8.3. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

8.3.1. Примерные задания для проведения контрольных работ в рамках учебных занятий

Отметьте правильный ответ в вопросах теста.

1. Какую максимальную длину маски сети можно задать для сети из 10 узлов?
   a) 29
   b) 28
   c) 27
   d) 26

2. Максимальное расстояние между активным устройствами в ЛВС при использовании витой пары составляет:
   a) 50 м
   b) 100 м
   c) 200 м
   d) 500 м

3. Устройство, которое собирает информацию о топологии межсетевых соединений и на ее основании пересылает пакеты сетевого уровня в сеть получателя, называется:
   a) маршрутизатор
   b) коммутатор
   c) концентратор
   d) мост
   e) медиаконвертер

4. Средства шифрования предназначены для:
   a) защиты от навязывания ложной информации
   b) защиты конфиденциальности информации при передаче по каналам связи или при ее обработке и хранении
   c) создания закрытых и открытых ключей электронной подписи

5. Цифровой документ, подтверждающий соответствие между открытым ключом и информацией, идентифицирующей владельца ключа, называется:
   a) сертификатом
   b) закрытым ключом
   c) имитовставкой
   d) электронной подписью

6. Схема Диффи-Хелмана является{
   a) симметричным алгоритмом шифрования
   b) методом безопасного распределения ключей шифрования

c) ассиметричным алгоритмом шифрования

8.3.2. Примерные контрольные задачи в рамках учебных занятий

Не предусмотрено

8.3.3. Примерные контрольные кейсы

Не предусмотрено

8.3.4. Перечень примерных вопросов для зачета

Не предусмотрено

8.3.5. Перечень примерных вопросов для экзамена

Итоговая аттестация проводится в форме экзамена по билетам. Билет к экзамену состоит из теоретического и практического вопросов. Время на подготовку — 45 минут.

Теоретические вопросы:

1. Нормативные требования к сетям в ИСПДн.
2. Нормативные требования к сетям в ГИС.
3. Нормативные требования к сетям объектов КИИ.
4. Методы и средства защиты информации в сетях.
5. Средства разграничения доступа к телекоммуникационному оборудованию.
6. Средства контроля доступа к среде передачи данных. Технология VLAN. Агрегирование каналов.
7. Протоколы и средства терминального доступа.
8. Назначение, принцип работы и классификация виртуальных частных сетей.
9. Назначение, принцип работы и классификация межсетевых экранов.
10. Схемы подключения межсетевых экранов.
11. Алгоритм обработки пакетов межсетевым экраном Netfilter
12. Алгоритм обработки пакетов списками доступа маршрутизаторов Cisco Systems.

Практические вопросы:

1. Оценить соответствие эксплуатационной документации компьютерной сети нормативным требованиям к ИСПДн.
2. Оценить соответствие эксплуатационной документации компьютерной сети нормативным требованиям к ГИС.
3. Оценить соответствие эксплуатационной документации компьютерной сети нормативным требованиям к объектам КИИ.
4. Оценить соответствие настроек телекоммуникационного оборудования политике информационной безопасности. Описать угрозы информационной безопасности.
5. Оценить соответствие настроек средства терминального доступа политике информационной безопасности. Описать угрозы информационной безопасности.
6. Оценить соответствие настроек средства организации виртуальной частной сети политике информационной безопасности. Описать угрозы информационной безопасности.
7. Оценить соответствие настроек межсетевого экрана политике информационной безопасности. Описать угрозы информационной безопасности.
8. Настроить службу SSH на сервере под управлением ОС Astra Linux SE 1.6.
9. Настроить терминальный режим доступа по протоколу X11 к серверу под управлением ОС Astra Linux SE 1.6.
10. Связать две локальные сети виртуальной частной сетью, созданной с помощью ПО OpenVPN.
11. Настроить web-сервер для работы по протоколу HTTPS.
12. Зашифровать электронное письмо с использованием стандарта S/MIME и ПО КриптоПро.
13. Обеспечить сокрытие структуры локальной сети при доступе ее узлов к внешним серверам с использованием технологии трансляции сетевых адресов.

14. Обеспечить сокрытие структуры локальной сети при доступе внешних узлов к ее серверам с использованием технологии трансляции сетевых адресов.
15. Разрешить с использованием механизма контроля состояния соединений межсетевого экрана доступ узлов внутренней сети лишь к web-серверам внешней.

8.3.6. Ресурсы АПИМ УрФУ, СКУД УрФУ для проведения тестового контроля в рамках текущей и промежуточной аттестации

Не предусмотрено

8.3.7. Ресурсы ФЭПО для проведения независимого тестового контроля

Не предусмотрено

8.3.8. Интернет-тренажеры

Не предусмотрено

8.3.9. Примерные задания в составе домашних работ

Добавление статических записей в таблицу осуществляется с помощью команды режима глобального конфигурирования (пример приведен для MAC-адреса **11-11-22-22-33-33** в Vlan номер 99 на интерфейсе **fa1/17**):

```
Switch(config)# mac-address-table static 1111.2222.3333 vlan 99 int fa1/17.
```

Выполнить следующие задания:

1) Добавить статические записи о компьютерах PC2 и PC4.
2) Выполнить команды ping на PC1 в адрес PC2 и на PC3 в адрес PC4.
3) Вывести содержимое таблицы коммутации коммутатора.

Удаление динамических записей из таблицы коммутации осуществляется с помощью команды привилегированного режима:

```
Switch#clear mac-address-table dynamic
```

а статических записей — с помощью команды режима глобального конфигурирования (пример приведен для MAC-адреса **11-11-22-22-33-33** в Vlan номер 99 на интерфейсе **fa1/17**):

```
Switch(config)#no mac-address-table static 1111.2222.3333 vlan 99 int fa1/17
```

Очистка таблицы коммутации осуществляется с помощью команды привилегированного режима:

```
Switch#clear mac-address-table
```

Выполнить следующие задания:

1) Удалить статическую запись о компьютере PC2 и вывести содержимое таблицы коммутации коммутатора.
2) Удалить динамические записи из таблицы коммутации и вывести содержимое таблицы коммутации коммутатора.
3) Очистить таблицу коммутации, убедиться в том, что в ней нет записей.