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
1156041

Модуль
Методы и средства защиты информации в информационных системах персональных данных (ИСПДн), государственных информационных системах (ГИС) и значимых объектах критической информационной инфраструктуры (КИИ)

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*

Согласовано:

Управление образовательных программ Р.Х.Токарева

1. ОБЩАЯ ХАРАКТЕРИСТИКА МОДУЛЯ Защищенные информационные системы

1.1. Аннотация содержания модуля

Целью модуля является приобретение новых и/или совершенствование существующих компетенций учащихся в сфере информационной безопасности. Изучаются требования к мерам защиты информации от несанкционированного доступа и принцип их выбора; установка, настройка и администрирование средств защиты информации от несанкционированного доступа; оценивание и инструментальные средства анализа защищенности компьютерных систем, экспертное оценивание трудно формализуемых свойств (параметров); методы и стандарты оценки защищённости, правовые аспекты ИСПДн, ГИС и значимых объектов КИИ.

В модуль входят: - Меры и средства защиты информации от несанкционированного доступа (НСД) в ИСПДн, ГИС и значимых объектах КИИ; - Методы контроля защищенности информации ИСПДн, ГИС и значимых объектов КИИ; - Стандарты и методы оценки защищенности ИСПДн, ГИС и значимых объектов 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.	Меры и средства защиты информации от несанкционированного доступа в ИСПДн, ГИС и значимых объектах КИИ	*3/108*
2	Методы контроля защищенности информации ИСПДн, ГИС и значимых объектов КИИ	*3/108*
3	Стандарты и методы оценки защищенности ИСПДн, ГИС и значимых объектов КИИ	*3/108*
	ИТОГО по модулю:	*9/324*

1.3. Последовательность освоения модуля в образовательной программе

Пререквизиты модуля	*Базовое образование по информационной безопасности*
Постреквизиты и кореквизиты 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
Меры и средства защиты информации от несанкционированного доступа в ИСПДн, ГИС и значимых объектах КИИ Методы контроля защищенности информации ИСПДн, ГИС и значимых объектов КИИ Стандарты и методы оценки защищенности ИСПДн, ГИС и значимых объектов КИИ	ПК 1. Способен решать типовые задачи анализа информации в ИАС государственных органов обеспечивающих национальную безопасность.	З-1 Методологические основы теории принятия решений, теории измерений, теории прогнозирования и планирования З-2 Способы измерения свойств объектов предметной области З-3 Методы теории вероятностей, теории случайных процессов и математической статистики З-4 Математические модели, методы и алгоритмы решения типовых задач анализа информации в ИАС З-5

		Программное обеспечение процесса решения задач анализа информации в ИАС З-6 Методические подходы к интерпретации профессионального смысла получаемых результатов анализа информации в ИАС З-7 Методы оценки эффективности и качества в задачах прогнозирования, планирования, принятия решений при различной априорной неопределенности имеющейся информации З-8 Нормативные правовые акты в области защиты информации З-9 Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации З-10 Организационные меры по защите информации 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 У-3 Строить алгоритмы решения типовых задач анализа информации в ИАС и создавать программы их реализации

		У-4 Представлять результаты решения аналитических задач в стандартном виде У-5 Интерпретировать профессиональный смысл получаемых результатов анализа информации в ИАС П-1 Выдвижение гипотез, определение границ их применения и подтверждение или опровержение их на практике П-2 Решение типовых задач анализа информации в ИАС П-3 Интерпретация профессионального смысла получаемых формальных результатов
Меры и средства защиты информации от несанкционированного доступа в ИСПДн, ГИС и значимых объектах КИИ Методы контроля защищенности информации ИСПДн, ГИС и значимых объектов КИИ Стандарты и методы оценки защищенности ИСПДн, ГИС и значимых объектов КИИ	ПК 5. Способен разработать и смоделировать программно-технические средства защиты информации от несанкционированного доступа	*З-1* *Нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа, проектирования средств защиты информации, сертификации средств защиты информации на соответствие требованиям по безопасности информации и аттестации объектов информатизации на соответствие требованиям по защите информации* *З-2* *Стандарты ЕСКД, ЕСТД и ЕСПД* *З-3* *Современные информационные технологии (операционные системы, базы данных, вычислительные сети)* *З-4* *Способы реализации несанкционированного доступа к информации и специальных программных воздействий на информацию и ее носители в автоматизированных системах* *З-5*

		Основные классы и виды уязвимостей программного обеспечения *З-6* *Методы и технологии защиты информации от несанкционированного доступа и специальных программных воздействий на нее* *З-7* *Программные (программно-технические) средства защиты автоматизированных систем от несанкционированного доступа к информации и специальных программных воздействий на нее* *З-8* *Методы контроля защищенности информации от несанкционированного доступа и специальных программных воздействий* *З-9* *Средства контроля защищенности информации от несанкционированного доступа* *З-10* *Методики контроля защищенности информации от несанкционированного доступа* *З-11* *Средства проектирования электронных схем* *З-12* *Языки и современные технологии программирования* *З-13* *Технологии производства электронной аппаратуры* *У-1* *Разрабатывать техническое задание на создание программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее* *У-2* *Разрабатывать проектно-сметную документацию на создание программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее*

		У-3 *Проектировать с использованием современных программных средств проектирования программно-техническое средство защиты информации от несанкционированного доступа и специальных воздействий на нее* *У-4* *Разрабатывать конструкторскую, технологическую и эксплуатационную документацию по правилам, установленным стандартами ЕСКД, ЕСТД и ЕСПД* *У-5* *Изготавливать опытный образец программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее* *У-6* *Разрабатывать программы и методики испытаний программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее* *У-7* *Проводить испытания программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее* *П-1* *Разработка технического задания на создание программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее* *П-2* *Разработка проектно-сметной документации на создание программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее* *П-3* *Разработка предварительных проектных решений по созданию программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее* *П-4*

		Разработка технического (эскизного) проекта программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее *П-5* *Разработка конструкторской и технологической документации на программное (программно-техническое) средство защиты информации от несанкционированного доступа и специальных воздействий на нее по правилам, установленным стандартами ЕСКД, ЕСТД и ЕСПД* *П-6* *Изготовление опытного образца программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее* *П-7* *Разработка программы и методик испытаний программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее* *П-8* *Испытания программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее* *П-9* *Разработка рабочей и эксплуатационной документации на техническое средство защиты* *П-10* *информации от несанкционированного доступа и специальных воздействий на нее*

1.5. Форма обучения

Обучение по дисциплинам модуля может осуществляться в очной форме

2. СОДЕРЖАНИЕ И ОБЕСПЕЧЕНИЕ РЕАЛИЗАЦИИ ДИСЦИПЛИН МОДУЛЯ

ПРОГРАММА МОДУЛЯ

Методы и средства защиты информации в информационных системах персональных данных (ИСПДн), государственных информационных системах (ГИС) и значимых объектах критической информационной инфраструктуры (КИИ)

РАЗДЕЛ 2. СОДЕРЖАНИЕ И ОБЕСПЕЧЕНИЕ РЕАЛИЗАЦИИ ДИСЦИПЛИН МОДУЛЯ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ 1

Меры и средства защиты информации от несанкционированного доступа в ИСПДн, ГИС и значимых объектах КИИ

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

2. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ 1

Меры и средства защиты информации от несанкционированного доступа в ИСПДн, ГИС и значимых объектах КИИ

2.1. Технологии обучения, используемые при изучении дисциплины модуля

- Традиционная (репродуктивная) технология *(ориентирована на передачу знаний и умений, обеспечивающая усвоение обучающимися содержания обучения, проверку и оценку его качества на репродуктивном уровне);*

2.2. Содержание дисциплины 1

Таблица 1.3

Код раздела, темы	Раздел, тема дисциплины*	Содержание
1	Общие сведения о системах	Введение. Цели, задачи и структура курса. Основные понятия и определения. Структура системы передачи сообщений. Количественные характеристики источников информации. Особенности образования и характеристики речевых сигналов. Определение и классификация сигналов. Обобщенные спектральные представления сигналов. Преобразование типа сигнала. Виды и особенности формирования первичных сигналов связи. Основные характеристики первичных сигналов. Согласование сигнала с каналом связи. Корреляционные и спектральные характеристики сигналов. Методы аналого-цифрового преобразования сигналов. Общие сведения о системах
~~**2**~~	Кодирование источников сообщений и сигналов в системах передачи информации. Основные методы модуляции и демодуляции аналоговых и дискретных сигналов при передаче в каналах связи	Основные понятия и классификация методов кодирования. Кодирование источника и кодирование сигнала в канале с шумами. Основы экономного кодирования. Избыточность и относительная скорость кода. Дискретные источники без памяти. Примитивное (безызбыточное) кодирование. Принципы статистического кодирования. Основы помехоустойчивого кодирования. Линейные блочные коды, порождающие матрицы. Декодирование линейных кодов. Проверочные матрицы. Циклические коды. Сверточные (решетчатые) коды. Блочные корректирующие коды. Обнаружение и исправление ошибок. Алгоритмы декодирования. Применение корректирующего кодирования в системах передачи информации. Виды модуляции: основные понятия и определения. Сигналы при непрерывной модуляции: амплитудная и угловая модуляции, их разновидности. Методы импульсной модуляции при передаче непрерывных сообщений: амплитудно-импульсная модуляция, широтно-импульсная модуляция, время-импульсная

		модуляция структура спектра, связь с параметрами сообщения, принципы демодуляции. Сигналы при дискретной модуляции: амплитудная манипуляция, частотная манипуляция, фазовая манипуляция, квадратурная амплитудная манипуляция. Методы модуляции с расширением спектра. Системы с прямым расширением спектра и па основе псевдослучайной (программной) перестройки рабочей частоты (ППРЧ).
~~3~~	Математические модели каналов передачи информации.	Классификация каналов передачи информации. Случайные линейные каналы и их характеристики, особенности проводных и радиоканалов, замирания сигналов. Флуктуационные, сосредоточенные и импульсные помехи, их вероятностные характеристики. Модели непрерывных каналов. Модели дискретного канала. Модели волоконно- оптических каналов связи. Марковские модели каналов. Уравнение состояния и наблюдения в скалярной и векторной форме. Моделирование каналов на основе метода переменных состояний.

2.3. Программа дисциплины реализуется на государственном языке Российской Федерации

2.4. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Управление информационной безопасностью ИСПДн, ГИС и значимых объектов КИИ

Электронные ресурсы (издания)

- *ЭБС, на которые есть подписка,*
- *elar.urfu.ru,*
- *study.urfu.ru,*
- *иные сайты в домене urfu.ru.*

Сведения берутся из электронного каталога библиотеки http://lib.urfu.ru/course/view.php?id=76 и включаются в рабочую программу после проверки их доступности (должен открываться полный текст, а не ознакомительный фрагмент).]

Печатные издания

Гаранин, М.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» / М.В. Гаранин, В.И. Журавлев, С.В. Кунегин. – М. : Радио и связь, 2001. – 336 с. 2. Башлы, П.Н. Информационная безопасность: учебно-практическое пособие [Электронный ресурс] / П.Н. Башлы, Е.К. Баранова, А.В. Бабаш. – Москва : Евразийский открытый институт, 2011. – 375 с. – URL: http://biblioclub.ru/index.php?page=book&id=90539. 3. Сычев, Ю.Н. Основы информационной безопасности : учебно-практическое пособие [Электронный ресурс] / Ю.Н. Сычев. – Москва : Евразийский открытый институт, 2010. – 328 с. – URL: http://biblioclub.ru/index.php?page=book&id=90790.

9.1.2 Дополнительная литература

1. Прозоров, В.М. Общеканальная система сигнализации No 7 : учеб. пособие для студентов вузов, обучающихся по специальностям 200900 (210406) – «Сети связи и системы коммутации», 201000 (210404) – «Многоканал. телекоммуникац. системы», 201200 (210402) – «Средства связи с подвиж. объектами» / В.М. Прозоров, А.И. Стебленко, А.В. Абилов. – Москва : Горячая линия - Телеком, 2008. – 152 с. 2. Информационные технологии в радиотехнических системах : учеб. пособие для студентов вузов, обучающихся по специальностям «Радиотехника» и «Радиоэлектрон. системы» направления подгот. дипломир. специалистов «Радиотехника» / [В.А. Васин, И.Б. Власов, Ю. М. Егоров и др.] ; под ред. И. Б. Федорова. – Изд. 2-е, перераб. и доп. – М. : МГТУ им. Н. Э. Баумана, 2004. – 768 с. 3. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы,
18
применение : [учебное пособие для вузов] / Р. Морелос-Сарагоса ; пер. с англ. В. Б. Афанасьева. – М. : Техносфера, 2005. – 319 с.
9.1.3 Методические разработки
1. Синадский Н.И. Информационная безопасность и защита информации / Н.И. Синадский. – УМК. – 2007. – в корпоративной сети УрФУ. <URL:http://study.urfu.ru/view/Aid_view.aspx?AidId=716

Профессиональные базы данных, информационно-справочные системы

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

www.consultant.ru. - www.garant.ru. - Электронно- библиотечная **система** ZNANIUM.COM – режим доступа www.znanium.com.
- Научная электронная библиотека eLIBRARY.RU – режим доступа http://elibrary.ru.
- Электронная библиотека Grebennikon – режим доступа http://grebennikon.ru/.
- Универсальная справочно-информационная полнотекстовая **база данных** периодических изданий EastViewhttp://ebiblioteka.ru/.

2.5. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Управление информационной безопасностью ИСПДн, ГИС и значимых объектов 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. Реквизиты подтверждающего документа
	Лекции; Практические занятия; Консультации; Самостоятельная работа студентов;	*1. Компьютерный класс. 2. Персональный компьютер преподавателя с мультимедиа-проектором и экраном. 3. Сертифицированный программно-аппаратный комплекс межсетевого экранирования.*	1. Microsoft Windows 7 Enterprise SP1, Windows Server 2008 R2 Enterprise; 2. Microsoft Windows XP SP3, Microsoft Windows Server 2003 R2 Enterprise; 3. Microsoft Internet Information Services 6.0. 4. Программное

		4. Общесистемное и прикладное программное обеспечение, средства защиты информации:	обеспечение Microsoft Office версии не менее 2010. Лабораторные стенды для выполнения практических работ - 8 шт.

ПРОГРАММА МОДУЛЯ

Методы контроля защищенности информации ИСПДн, ГИС и значимых объектов КИИ

РАЗДЕЛ 2. СОДЕРЖАНИЕ И ОБЕСПЕЧЕНИЕ РЕАЛИЗАЦИИ ДИСЦИПЛИН МОДУЛЯ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ 2

Методы контроля защищенности информации ИСПДн, ГИС и значимых объектов КИИРабочая программа дисциплины составлена авторами:

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

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

2. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ 2

Методология проектирования защищенных информационных систем

2.1. Технологии обучения, используемые при изучении дисциплины модуля

- Традиционная (репродуктивная) технология *(ориентирована на передачу знаний и умений, обеспечивающая усвоение обучающимися содержания обучения, проверку и оценку его качества на репродуктивном уровне);*

2.2. Содержание дисциплины

Таблица 1.3

Код раздела, темы	Раздел, тема дисциплины*	Содержание
1	Классификация вредоносных программ	Понятие об опасных компьютерных программах и данных. Оценка опасностей, связанных с разработкой и использованием программ для ЭВМ. Состав вредоносных программ и команд. Классификация вредоносных программ по основным свойствам и признакам. Основные признаки и возможности компьютерных вирусов, программных закладок, «логических бомб», сетевых «червей», программ «удаленного администрирования» и иных видов опасных программ. Инструментарий, используемый вирмейкерами для создания вредоносных программ. Изучение функциональных возможностей вредоносных программ. Программные воздействия, заведомо приводящие к опасным последствиям. Сущность вредоносных блокирования, удаления, модификации защищаемой компьютерной информации. Программно-управляемые формы несанкционированного копирования информации. Механизмы вирусного заражения. Виды и формы программно-управляемого нарушения работы ЭВМ. Способы несанкционированного запуска опасных программ и команд. Способы внедрения и запуска вредоносных программ. Уязвимые места программного обеспечения автоматизированных систем, способствующие внедрению, запуску, сокрытию, и распространению вредоносных программ. Способы проникновения вредоносных программ в локальные и сетевые ЭВМ. Потенциально опасные функции операционной системы. Уязвимости ОС и штатного программного обеспечения, способствующие распространению вредоносных программ. Понятие о случайном и безусловном запуске. Внедрение и запуск программного кода на этапах самотестирования ПЭВМ и загрузки операционной системы. Способы подготовки вредоносных программ к автоматическому запуску. Типичные варианты обмана пользователей, провоцирующих их на запуск неизвестных программ. Внедрение и запуск опасных программ с применением «троянских» оболочек. Возможности программ-«джойнеров».
~~**2**~~	Средства и методы защиты	Виды и возможности антивирусных программ. Меры

	от вредоносных компьютерных программ	по реализации изолированной программной среды. Статический анализ потенциально опасных программ. Определение истинного типа файла. Просмотр текстовых строк в исполняемых и командных файлах. Рекомендации по дизассемблированию и исследованию программного кода. Динамический 6 анализ опасных программ. Запуск программ в виртуальной среде VMWare. Трассировка программ. Возможности программ типа ExeScope и OllyDebugger. Использование мониторов обращений к стеку сетевых драйверов, файлам и системному реестру. Оформление заключений по результатам исследования неизвестных и опасных программ. Способы выявления деструктивной активности вредоносных программ. Понятие о сигнатуре вредоносного программного кода. Принципы антивирусного сканирования памяти ЭВМ. Понятие о механизмах скрытности вредоносных программ. Демаскирующие признаки вредоносного программного кода. Полиморфизм программного кода. «Stealth»-технологии. Способы сокрытия файловых объектов и процессов на уровне ядра операционной системы. Возможности программ-«руткитов». Мониторинг подозрительной активности программ. Статический анализ потенциально опасных программ. Определение истинного типа файла. Просмотр текстовых строк в исполняемых и командных файлах. Рекомендации по дизассемблированию и исследованию программного кода. Динамический анализ опасных программ. Запуск программ в виртуальной среде VMWare. Трассировка программ. Возможности программ типа ExeScope и OllyDebugger. Использование мониторов обращений к стеку сетевых драйверов, файлам и системному реестру. Оформление заключений по результатам исследования неизвестных и опасных программ.

2.3. Программа дисциплины реализуется на государственном языке Российской Федерации

УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Управление проектами в области информационной безопасности

Электронные ресурсы (издания)

- *ЭБС, на которые есть подписка,*
- *elar.urfu.ru,*
- *study.urfu.ru,*
- *иные сайты в домене urfu.ru.*

1. *Московское отделение Института управления проектами - Project Management Institute PMI – www.pmi.ru*
2. *Национальная ассоциация управление проектами «СОВНЕТ» (корпоративный член международной организации управления проектами IPMA) – www.sovnet.ru*
3. *Технологии корпоративного управления. Проектное управление. – http://www.iteam.ru/publications/project/*

Печатные издания

Андрончик А.Н. и др. Защита информации в компьютерных сетях. Практический курс: учебное пособие / А.Н. Андрончик, В.В. Богданов, Н.А. Домуховский, А.С. Коллеров, Н.И. Синадский, Д.А. Хорьков, М.Ю. Щербаков; Под ред. Н.И.Синадского. – Екатеринбург: ГОУ ВПО УГТУ - УПИ, 2007. – 246 с. 90 экз. 2. Сетевая защита на базе технологий фирмы CiscoSystems. Практический курс: учебное пособие / А.Н. Андрончик, А.С. Коллеров, Н.И. Синадский, М.Ю. Щербаков; под ред. Н.И. Синадского. – Екатеринбург: УрФУ, 2011. – 160 с. URL:http://biblioclub.ru/index.php?page=book&id=275694>.

9.1.2. Дополнительная литература

1. Петренко, В.И. Теоретические основы защиты информации : учебное пособие / В.И. Петренко ; Министерство образования и науки Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный

10

университет». - Ставрополь : СКФУ, 2015. - 222 с. : ил. - Библиогр.: с. 214-215. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=458204 (20.03.2018). 2. 3. Сердюк, В.А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий : учебное пособие / В.А. Сердюк ; Высшая Школа Экономики Национальный Исследовательский Университет. - Москва : Издательский дом Государственного университета Высшей школы экономики, 2015. - 574 с. : ил. - Библиогр. в кн. - ISBN 978-5-7598-0698-1 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=440285 (20.03.2018). 4. Хаулет, Т. Защитные средства с открытыми исходными текстами: Практическое руководство по защитны м приложениям : учебное пособие / Т. Хаулет ; пер. с англ. В. Галатенко, О. Труфанова ; под ред. В. Галатенко ; Национальный Открытый Университет "ИНТУИТ". - Москва : Интернет-Университет Информационных Технологий, 2007. - 608 с. : ил., табл., схем. - (Основы информационных технологий). - ISBN 978-5-94774-629-7 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=233306 (20.03.2018). Касперски К. Компьютерные вирусы изнутри и снаружи / К. Касперски .— СПб. : Питер, 2006 .— 527 с.

9.2. Методические разработки

1. Бакланов, В. В. Противодействие созданию и распространению вредоносных программ / Бакланов В.В. — Ссылка .— 2008 .— Курс "Противодействие созданию и распространению вредоносных программ" является специальным курсом для специальности "Компьютерная безопасность". Излагается классификация вредоносных программ. Обсуждаются методы и средства противодействия созданию и распространению вредоносных программ. Включает учебное пособие, программу дисциплины, сборник лабораторных работ, методические указания, экзаменационные материалы, презентации. Предназначен для студентов специальности "Компьютерная безопасность". — в корпоративной сети УрФУ .— <URL:http://study.urfu.ru/view/Aid_view.aspx?AidId=11067>.

Профессиональные базы данных, информационно-справочные системы

http://lib.urfu.ru/mod/data/view.php?id=1379]

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
www.consultant.ru. - www.garant.ru. - Электронно- библиотечная **система** ZNANIUM.COM – режим доступа www.znanium.com.
- Научная электронная библиотека eLIBRARY.RU – режим доступа http://elibrary.ru.
- Электронная библиотека Grebennikon – режим доступа http://grebennikon.ru/.
- Универсальная справочно-информационная полнотекстовая **база данных** периодических изданий EastViewhttp://ebiblioteka.ru/.

2.4. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ 2

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. Реквизиты подтверждающего документа
	Лекции; Лабораторные занятия; Консультации; Самостоятельная работа студентов;	*1. Компьютерный класс.* *2. Персональный компьютер преподавателя с мультимедиа-проектором и экраном.* *3. Сертифицированный программно-аппаратный комплекс межсетевого экранирования.* *4. Общесистемное и прикладное программное обеспечение, средства защиты информации*	• *Компьютер, на котором установлено программное обеспечение: MS Excel, Project Expert 7, MS Project.*

ПРОГРАММА МОДУЛЯ

Методы и средства защиты информации в информационных системах персональных данных (ИСПДн), государственных информационных системах (ГИС) и значимых объектах критической информационной инфраструктуры (КИИ)

РАЗДЕЛ 2. СОДЕРЖАНИЕ И ОБЕСПЕЧЕНИЕ РЕАЛИЗАЦИИ ДИСЦИПЛИН МОДУЛЯ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ 1

Стандарты и методы оценки защищенности ИСПДн, ГИС и значимых объектов КИИ

Рабочая программа дисциплины составлена авторами:

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

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

2. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ 1

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

2.1. Технологии обучения, используемые при изучении дисциплины модуля

- Традиционная (репродуктивная) технология *(ориентирована на передачу знаний и умений, обеспечивающая усвоение обучающимися содержания обучения, проверку и оценку его качества на репродуктивном уровне);*

2.2. Содержание дисциплины 1

Таблица 1.3

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 телекоммуникационного оборудования	Средства разграничения доступа к телекоммуникационному оборудованию. Средства контроля доступа к среде передачи данных. Технология VLAN. Агрегирование каналов.
Р2, Т2	Средства терминального доступа	Принцип работы средств терминального доступа. Протоколы SSH, X11, RDP, VNC, SPICE.
Р2, Т3	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.
Р2, Т4	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.

2.3. Программа дисциплины реализуется на государственном языке Российской Федерации

2.4. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Управление информационной безопасностью ИСПДн, ГИС и значимых объектов КИИ

Электронные ресурсы (издания)

- *ЭБС, на которые есть подписка,*
- *elar.urfu.ru,*
- *study.urfu.ru,*
- *иные сайты в домене urfu.ru.*

Сведения берутся из электронного каталога библиотеки
http://lib.urfu.ru/course/view.php?id=76 и включаются в рабочую программу после

проверки их доступности (должен открываться полный текст, а не ознакомительный фрагмент).]

Печатные издания

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.*
13. *A Complete Guide to the Common Vulnerability Scoring System Version 3.0 [Электронный ресурс] http://www.first.org/cvss/cvss-guide.html.*
14. *Trusted Computer System Evaluation Criteria. US Department of Defense. CSC-STD-001-83, Aug. 1983.*
15. *Агафонов А.В., Андрончик А. Н., Иванов Ф.И. Защита информации в компьютерных сетях. Технологии межсетевого экранирования : учебное пособие / А.В. Агафонов, А. Н. Андрончик, Ф.И. Иванов — Иркутск : ИГУ, 2012. — 111с.*
16. *Андрончик А.Н., Коллеров А.С., Синадский Н.И., Щербаков М.Ю. 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 ред. Н.И. Синадского. – Екатеринбург: УрФУ, 2012. – 159 с.*
17. *Корольков Ю.Д., Синадский Н.И., Хорьков Д.А. Защита информации в компьютерных сетях. Технологии защищенной обработки информации : учебное пособие / Ю.Д. Корольков, Н.И. Синадский, Д.А. Хорьков. — Иркутск: ИГУ, 2012. — 117*

*c.***Профессиональные базы данных, информационно-справочные системы**

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

www.consultant.ru. - www.garant.ru. - Электронно- библиотечная **система** ZNANIUM.COM – режим доступа www.znanium.com.

- Научная электронная библиотека eLIBRARY.RU – режим доступа http://elibrary.ru.
- Электронная библиотека Grebennikon – режим доступа http://grebennikon.ru/.
- Универсальная справочно-информационная полнотекстовая **база данных** периодических изданий EastViewhttp://ebiblioteka.ru/.

2.5. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

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. Реквизиты подтверждающего документа
	Лекции; Практические занятия; Консультации; Самостоятельная работа студентов;	*1. Компьютерный класс.* *2. Персональный компьютер преподавателя с мультимедиа-проектором и экраном.* *3. Сертифицированный программно-аппаратный комплекс межсетевого экранирования.* *4. Общесистемное и прикладное программное обеспечение, средства защиты информации:*	1. Microsoft Windows 7 Enterprise SP1, Windows Server 2008 R2 Enterprise; 2. Microsoft Windows XP SP3, Microsoft Windows Server 2003 R2 Enterprise; 3. Microsoft Internet Information Services 6.0. 4. Программное обеспечение Microsoft Office версии не менее 2010.