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
27 апреля 2021 г.

РАБОЧАЯ ПРОГРАММА МОДУЛЯ

Код модуля
1156882

Модуль
Проектирование защищенных телекоммуникационных систем

Екатеринбург, 2021

Перечень сведений о рабочей программе модуля	Учетные данные
Образовательная программа *Информационная безопасность телекоммуникационных систем*	**Код ОП 10.05.02/22.01**
Направление подготовки Информационная безопасность	**Код направления и уровня подготовки** *10.05.02*

Области образования, в рамках которых реализуется модуль образовательной программы по ФГОС ВО 3++ *специалитет*

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

Программа модуля составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Поршнев Сергей Владимирович	д.т.н., профессор	Директор УНЦ ИБ	*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 Проектирование защищенных телекоммуникационных систем

1.1. Аннотация содержания модуля

Модуль «**Проектирование защищенных телекоммуникационных систем**» направлен на изучение вопросов обеспечения безопасности систем и каналов связи, режимных объектов, выделенных помещений и хранилищ, формирование качеств, необходимых для понимания, распознавания и реагирования на разнообразные умышленные угрозы, характерные для компьютерной преступности. Изучаются физические основы образования утечки информации по техническим каналам, принципы и устройства технической разведки. Противодействие опасному человеческому фактору реализуется в виде взаимосвязанного набора активных и пассивных действий.

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.	Проектирование защищенных телекоммуникационных систем	*4/144*
	ИТОГО по модулю:	*4/144*

1.3. Последовательность освоения модуля в образовательной программе

Пререквизиты модуля	Методы анализа сигналов систем Технические средства и методы защиты информации
Постреквизиты и кореквизиты модуля	-

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

Код и наименование компетенции	Планируемые результаты обучения (индикаторы)				**Модули и дисциплины**
	Знания:	**Умения:**	**Практический опыт, владение**	**Другие результаты** *(указываются при необходимости, к примеру,* ***личностные качества*** *)*	
ОПК-9. Способен использовать программные, программно-аппаратные и технические средства защиты информации при решении задач профессиональной деятельности	"РО1-З ОПК9 Знает основные информационные технологии, используемые в телекоммуникационных системах, их состояние и тенденции развития" "РО2-З ОПК9 Знает текущее состояние и тенденции развития методов и средств защиты информации от утечки по техническим каналам" "РО3-З ОПК9 Знает текущее состояние и тенденции развития сетей и систем передачи информации"	"РО1-У ОПК9 Умеет проводить анализ архитектуры и структуры ЭВМ и систем, оценивать эффективность архитектурно-технических решений, реализованных при построении ЭВМ и систем" "РО2-У ОПК9 Умеет применять средства защиты от утечки по техническим каналам при решении задач профессиональной деятельности" "РО3-У ОПК9 Умеет определять требования по защите коммуникационн	"РО1-В ОПК9 Имеет навыки реализации вычислительных процедур на микропрограммном уровне при решении задач профессиональной деятельности" "РО2-В ОПК9 Владеет методами проектирования и навыками эксплуатации систем и сетей передачи информации при решении задач профессиональной деятельности" "РО3-В ОПК9 Имеет навыки имеет навыки проектирования распределенных информационных		Проектирование защищенных телекоммуникационных систем

	"РО4-З ОПК9 Знает технические каналы утечки информации,организацию защиты информации от утечки по техническим каналам, основные характеристики и принципы построения средств защиты информации от утечки по техническим каналам" "РО5-З ОПК9 Знает особенности построения, функционирования и защиты современных распределённых информационных систем и их коммуникационной среды"	ой среды распределенной информационной системы"	систем, в том числе разработки приложений, реализующих параллельные вычисления"		

1.5. Форма обучения

Обучение по дисциплинам модуля может осуществляться в очной форме

2. СОДЕРЖАНИЕ И ОБЕСПЕЧЕНИЕ РЕАЛИЗАЦИИ ДИСЦИПЛИН МОДУЛЯ

ПРОГРАММА МОДУЛЯ

Проектирование защищенных телекоммуникационных систем

РАЗДЕЛ 2. СОДЕРЖАНИЕ И ОБЕСПЕЧЕНИЕ РЕАЛИЗАЦИИ ДИСЦИПЛИН МОДУЛЯ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ 1

Проектирование защищенных телекоммуникационных систем

Рабочая 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 1

Проектирование защищенных телекоммуникационных 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 1

Таблица 1.3

Код раздела, темы	Раздел, тема дисциплины*	Содержание
1	Управление инцидентами информационной безопасности	Понятие инцидентов ИБ. Нормативная база в сфере управления инцидентами ИБ. Система управления инцидентами ИБ. Обработка событий и инцидентов ИБ. Реагирование на инциденты ИБ. Организация процесса обработки технических данных в рамках реагирования на инциденты ИБ.
2	Сбор и анализ технических данных при реагировании на инциденты	Организация процесса обработки технических данных в рамках реагирования на инциденты ИБ: – сбор технических данных с компонентов информационной инфраструктуры; – поиск (выделение) из собранных технических данных содержательной (семантической) информации, ее анализ и оформлению; – распространение (передача) выделенной и оформленной содержательной (семантической) информации; – обеспечение наличия технических данных на этапах создания и эксплуатации информационной инфраструктуры. Сбор и фиксация информации об инцидентах ИБ: способ выявления инцидента ИБ; источник информации об инциденте ИБ; содержание информации об инциденте ИБ, полученной от источника; сценарий реализации инцидента ИБ; дата и время выявления инцидента ИБ; состав информационной инфраструктуры, задействованной в реализации инцидента ИБ, в том числе пострадавшей от инцидента ИБ, уровень ее критичности; способы подключения информационной инфраструктуры, задействованной в реализации инцидента ИБ, к сети Интернет или сетям общего пользования; информация об операторе связи и провайдере сети Интернет. Проверка целостности (неизменности) собранных данных, маркирование носителей собранных данных. Криминалистическое копирование (создания образов) энергонезависимых технических данных запоминающих устройств СВТ методом побитового копирования. Копирование содержимого оперативной памяти СВТ и получение данных операционных

		систем. Копирование протоколов (журналов) регистрации. Копирование сетевого трафика. Поиск (выделение) содержательной (семантической) информации, ее анализ и оформление. Структура протокола обработки технических данных. Технические средства и инструменты для сбора и обработки технических данных: 6 технические средства выполнения криминалистической копии (создания образа) запоминающих устройств и содержимого оперативной памяти СВТ; технические средства получения данных операционных систем о сетевых конфигурациях, о сетевых соединениях, об открытых файлах, о запущенных процессах, об открытых сессиях доступа.»
3	Обеспечение режима защиты информации персональных данных (ПДн), и безопасности ПДн в организации	Меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных ФЗ «О персональных данных». Меры, по обеспечению безопасности ПДн при их обработке. Понятие угроз безопасности ПДн. Определение уровня защищенности ПДн

2.3. Программа дисциплины реализуется на государственном языке Российской Федерации

2.4. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Проектирование защищенных телекоммуникационных систем

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. Бакланов В.В. Введение в информационную безопасность. Направления информационной защиты : курс лекций : учеб. пособие для вузов / В. В. Бакланов .— Екатеринбург : Изд-во Уральского университета, 2007 .— 232 с. — (Приоритетный национальный проект "Образование") (Математика. Компьютерные науки) .— Библиогр.: с. 229-232 .— ISBN 5-7996-0259-5.

2. Галатенко, В. А. Основы информационной безопасности : Курс лекций: Учеб. пособие для вузов / В. А. Галатенко ; Под ред. В. Б. Бетелина .— 2-е изд., испр. — М. : Интернет-Ун-т Информ. Технологий, 2004 .— 264 с. — (Основы информационных технологий). — Рек. Учеб.-метод. об-нием в обл. прикладной информатики .— Библиогр.: с. 256-260. — ISBN 5-9556-0015-9 : 200-00.

3. Основы информационной безопасности : учеб. пособие для вузов / Е. Б. Белов [и др.]. — М. : Горячая линия-Телеком, 2006 .— 544 с. : ил. — Допущено М-вом образования и науки РФ .— ISBN 5-93517-292-5.

Дополнительная литература:

3. Расторгуев С.П. Основы информационной безопасности : учеб. пособие для студентов вузов, обучающихся по специальностям "Компьютер. безопасность", "Комплекс. обеспечение информ. безопасности автоматизир. систем" и "Информ. безопасность телекоммуникац. систем" / С. П. Расторгуев .— Москва : Академия, 2007 .— 188 с. ; 22 см .— (Высшее профессиональное образование, Информационная безопасность) .—Слов. терминов: с. 182-185. —Библиогр.: с. 180- 181 (39 назв.). — Допущено в качестве учебного пособия. — ISBN 978-5-7695-3098-2.

б) нормативные правовые акты и стандарты

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

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

*[Библиографические описания бумажных ресурсов из электронного каталога библиотеки http://lib.urfu.ru/course/view.php?id=76 с указанием имеющегося количества экземпляров (в ЗНБ и/или на кафедре или ином подразделении УрФУ) – суммарное количество экземпляров должно быть **не менее 0,25 экземпляра** каждого из изданий, на одного обучающегося из числа лиц, одновременно осваивающих соответствующую дисциплину (модуль), проходящих соответствующую практику]*

Профессиональные базы данных, информационно-справочные системы

Материалы для лиц с ОВЗ

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

Базы данных, информационно-справочные и поисковые системы

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

2.5. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Проектирование защищенных телекоммуникационных систем

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием и программным обеспечением

Таблица 3.1

№ п/п	Виды занятий	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения. 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*	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

		прикладное программное обеспечение, средства защиты информации:	версии не менее 2010.