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

УТВЕРЖДАЮ
Директор по образовательной
деятельности

_____ С.Т. Князев
«___» _____

РАБОЧАЯ ПРОГРАММА МОДУЛЯ

Код модуля	Модуль
1156042	Криптографические методы защиты информации

Екатеринбург

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

Программа модуля составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Пономарева Ольга Алексеевна	-, -	старший преподаватель	УНЦ ИБ
2	Поршнев Сергей Владимирович	д.т.н, профессор	директор Учебно-научного центра "Информационная безопасность"	УНЦ ИБ

Согласовано:

Управление образовательных программ Р.Х. Токарева

1. ОБЩАЯ ХАРАКТЕРИСТИКА МОДУЛЯ Криптографические методы защиты информации

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
1	Криптографические алгоритмы и протоколы	3
2	Криптографические методы и средства защиты в ИСПДн, ГИС и значимых объектах КИИ	3
	ИТОГО по модулю:	6

1.3.Последовательность освоения модуля в образовательной программе

Пререквизиты модуля	1. Математические методы информационной безопасности
Постреквизиты и кореквизиты модуля	1. Методы и средства защиты информации в информационных системах персональных данных (ИСПДн), государственных информационных системах (ГИС) и значимых объектах критической информационной инфраструктуры (КИИ) 2. Обнаружение и предупреждение компьютерных атак на объектах критической информационной инфраструктуры (КИИ)

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

Таблица 2

Перечень дисциплин модуля	Код и наименование компетенции	Планируемые результаты обучения (индикаторы)
1	2	3
Криптографические алгоритмы и протоколы	ПК-4 - Способен разрабатывать программные и программно-аппаратные средства для систем защиты информации автоматизированных систем	З-4 - Применять основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах У-1 - Оценивать сложность алгоритмов и вычислений У-4 - Проводить комплексное тестирование аппаратных и программных средств П-2 - Разрабатывать программное обеспечение, технических средств, баз данных и компьютерных сетей с учетом требований по обеспечению защиты информации
Криптографические методы и средства защиты в ИСПДн, ГИС и значимых объектах КИИ	ПК-2 - Способен проводить анализ безопасности компьютерных систем	З-3 - Идентифицировать криптографические методы защиты информации У-1 - Анализировать компьютерную систему с целью определения уровня защищенности и доверия П-1 - Определять уровни защищенности и доверия в компьютерных системах П-3 - Оценивать соответствие механизмов безопасности компьютерной системы требованиям существующих нормативных документов, а также их адекватности существующим рискам
	ПК-4 - Способен разрабатывать программные и программно-аппаратные средства для систем защиты информации автоматизированных систем	З-1 - Пользоваться профессиональной и криптографической терминологией в области безопасности информации З-2 - Применять основные информационные технологии, используемые в автоматизированных системах З-6 - Различать принципы работы элементов и функциональных узлов электронной аппаратуры, типовые схемотехнические решения основных узлов и блоков электронной аппаратуры

		П-1 - Разрабатывать техническую документацию в соответствии с требованиями Единой системы конструкторской документации (ЕСКД) и Единой системы программной документации (ЕСПД) на компоненты автоматизированных систем П-3 - Оптимизировать работу электронных схем с учетом требований по защите информации

1.5. Форма обучения

Обучение по дисциплинам модуля может осуществляться в очной формах.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Криптографические алгоритмы и протоколы

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Каннер Татьяна Михайловна		старший преподаватель	МФТИ
2	Пономарева Ольга Алексеевна	кандидат технических наук, без ученого звания	Старший преподаватель	

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

Протокол № _9_ от _05.04.2022_ г.

1. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

Авторы:

1.1. Технологии реализации, используемые при изучении дисциплины модуля

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

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

1.2. Содержание дисциплины

Таблица 1.1

Код раздела, темы	Раздел, тема дисциплины*	Содержание
Р1	Криптографические алгоритмы	Способы криптографической защиты информации. Криптосистемы с секретным ключом. Инфраструктура открытых ключей Поточные и блочные алгоритмы
Р2	Введение в криптографические протоколы	Криптографические протоколы и основные требования к ним Протоколы обмена ключами Протоколы идентификации/аутентификации
Р3	Криптографические протоколы	Протоколы защиты данных в сети Internet Протоколы генерации и распределенияключей Протоколы разделения секретов.Протоколыснулевымразглашениемидоказательство нулевого разглашения

1.3. Направление, виды воспитательной деятельности и используемые технологии

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

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации .

2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Криптографические алгоритмы и протоколы

Электронные ресурсы (издания)

1. ; Онтология и аксиология права : тезисы докладов и сообщений седьмой международной научной конференции (20-21 октября 2015 г.).; Омская академия МВД России, Омск; 2015; http://www.iprbookshop.ru/61779.html (Электронное издание)

Печатные издания

1. Молдовян, А. А., Молдовян, Н. А., Советов, Б. Я.; Криптография; Лань, Санкт-Петербург; 2001 (15 экз.)

2. Атцик, А. А., Гольдштейн, А. Б., Саморезов, В. В.; IP-коммуникации в NGN : учеб. пособие по специальности 210406 "Сети связи и системы коммутации".; СПбГУТ, Санкт-Петербург; 2007 (1 экз.)

3. Столлингс, Столлингс В., Никифоров, Никифоров А.; Компьютерные сети, протоколы и технологии Интернета; БХВ-Петербург, Санкт-Петербург; 2005 (11 экз.)

4. Гольдштейн, А. Б., Гольдштейн, Б. С.; Технология и протоколы MPLS; БХВ-Санкт-Петербург, Санкт-Петербург; 2005 (2 экз.)

5. Иди, Тихонов, О. М., Ежов, В. Б.; Сетевой и межсетевой обмен данными с микроконтроллерами; Додэка-XXI, Москва; 2007 (1 экз.)

6. Стивенс, Ричард У., Р. У., Глебовский, А. Ю.; Протоколы TCP/IP. Практическое руководство : [монография].; Невский Диалект : БХВ-Петербург, Санкт-Петербург; 2003 (1 экз.)

7. Стивенс, Ричард У., Р. У., Глебовский, А. Ю.; Протоколы TCP/IP. Практическое руководство : [монография].; Невский Диалект : БХВ-Петербург, Санкт-Петербург; 2003 (1 экз.)

8. Стивенс, Ричард У., Р. У., Глебовский, А. Ю.; Протоколы TCP/IP. Практическое руководство : [монография].; Невский Диалект : БХВ-Петербург, Санкт-Петербург; 2003 (1 экз.)

Профессиональные базы данных, информационно-справочные системы

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

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

Материалы для лиц с ОВЗ

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

Базы данных, информационно-справочные и поисковые системы

Министерство образования и науки Российской Федерации (http:__минобрнауки.рф_).

Федеральный портал _Российское образование_ (http:__www.edu.ru_).

ООО Научная электронная библиотека (http:__elibrary.ru_defaultx.asp).

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

Электронный научный архив УрФУ (https:__elar.urfu.ru).

3. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Криптографические алгоритмы и протоколы

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием и программным обеспечением

Таблица 3.1

№ п/п	Виды занятий	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения
1	Лекции	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Периферийное устройство Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами Подключение к сети Интернет	Office 365 ProPlusEdu ShrdSvr ALNG SubsVL MVL PerUsr STUUseBnft Student EES
2	Практические занятия	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Периферийное устройство	CISSteDCCore ALNG LicSAPk MVL 2Lic CoreLic EES

		Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами Подключение к сети Интернет	

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Криптографические методы и средства защиты в ИСПДн, ГИС и значимых объектах КИИ

Рабочая программа дисциплины составлена авторами:

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

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

Протокол № _9_ от _05.04.2022_ г.

1. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

Авторы:

1.1. Технологии реализации, используемые при изучении дисциплины модуля

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

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

1.2. Содержание дисциплины

Таблица 1.1

Код раздела, темы	Раздел, тема дисциплины*	Содержание
Р1	Математические криптографические методы	Алгоритмы тестирования на простоту и факторизации; Свойствах группы точек эллиптической кривой над конечным полем
Р2	Методы и средства криптографической защиты компьютерной информации	Основные термины криптографической защиты информации и их определения; Общая характеристика программно-аппаратных средств криптографической защиты информации; Криптосредства; Электронная цифровая подпись; Контроль целостности; Уничтожение остаточной информации; Организация виртуальных частных сетей
Р3	Нормативно-правовое регулирование в сфере применения средств криптографической защиты информации	Нормативные документы в области применения средств криптографической защиты информации; Стандартизация, лицензирование и сертификация в области проектирования средств защиты информации; Использование криптографических средств для обеспечения безопасности персональных данных
Р4	Применение средств криптографической защиты информации	Классы защиты; Средства криптографической защиты информации: StrongDisk, Secret Disk, «Верба», «КриптоПро CSP», StrongNet, «Игла-П», VipNet.

1.3. Направление, виды воспитательной деятельности и используемые технологии

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

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации .

2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Криптографические методы и средства защиты в ИСПДн, ГИС и значимых объектах КИИ

Электронные ресурсы (издания)

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

Печатные издания

1. Духан, Е. И., Синадский, Н. И., Хорьков, Д. А., Гайдамакин, Н. А.; Применение программно-аппаратных средств защиты компьютерной информации : учебное пособие для студентов вузов, обучающихся по специальностям 090102, 090105, 090106.; УГТУ-УПИ, Екатеринбург; 2008 (30 экз.)

2. Духан, Е. И., Синадский, Н. И., Хорьков, Д. А., Гайдамакин, Н. А.; Применение программно-аппаратных средств защиты компьютерной информации : учебное пособие для студентов вузов, обучающихся по специальностям 090102 - "Компьютерная безопасность", 090105 - "Комплексное обеспечение информационной безопасности автоматизированных систем"....; УГТУ-УПИ, Екатеринбург; 2007 (15 экз.)

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

Профессиональные базы данных, информационно-справочные системы

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

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

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

Материалы для лиц с ОВЗ

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

Базы данных, информационно-справочные и поисковые системы

Министерство образования и науки Российской Федерации (http:__минобрнауки.рф_).

Федеральный портал _Российское образование_ (http:__www.edu.ru_).

ООО Научная электронная библиотека (http:__elibrary.ru_defaultx.asp).

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

Электронный научный архив УрФУ (https:__elar.urfu.ru).

3. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Криптографические методы и средства защиты в ИСПДн, ГИС и значимых объектах КИИ

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием и программным обеспечением

Таблица 3.1

№ п/п	Виды занятий	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения
1	Лекции	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Периферийное устройство Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами Подключение к сети Интернет	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES
2	Лабораторные занятия	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Периферийное устройство Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами Подключение к сети Интернет	Citrix NetScaler Cisco C3750X-24 LAN Base to IP Base E-License (L-C3750X-24-L-S) Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES