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
1156042

Модуль
Криптографические методы защиты информации

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 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
Криптографические алгоритмы и протоколы Криптографические методы и средства защиты в ИСПДн, ГИС и значимых объектах КИИ	ПК 2. Способен проводить анализ безопасности компьютерных систем.	З-1 Принципы построения компьютерных систем и сетей З-2 Уязвимости компьютерных систем и сетей З-3 Криптографические методы защиты информации З-4 Принципы построения систем управления базами данных З-5 Средства анализа конфигураций З-6 Национальные, межгосударственные и международные стандарты в области защиты информации З-7 Нормативные правовые акты в области защиты информации З-8

		Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации З-9 Организационные меры по защите информации У-1 Анализировать компьютерную систему с целью определения уровня защищенности и доверия У-2 Прогнозировать возможные пути развития действий нарушителя информационной безопасности У-3 Производить анализ политики безопасности на предмет адекватности У-4 Проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в операционных системах У-5 Составлять и оформлять аналитический отчет по результатам проведенного анализа У-6 Разрабатывать предложения по устранению выявленных уязвимостей П-1 Определение уровня защищенности и доверия в компьютерных системах П-2 Оценка рисков, связанных с осуществлением угроз безопасности в отношении компьютерных систем П-3

		Оценка соответствия механизмов безопасности компьютерной системы требованиям существующих нормативных документов, а также их адекватности существующим рискам П-4 Подготовка аналитического отчета по результатам проведенного анализа П-5 Формулирование предложений по устранению выявленных уязвимостей

1.5. Форма обучения

Обучение по дисциплинам модуля может осуществляться в очной форме

2. СОДЕРЖАНИЕ И ОБЕСПЕЧЕНИЕ РЕАЛИЗАЦИИ ДИСЦИПЛИН МОДУЛЯ

ПРОГРАММА МОДУЛЯ
Криптографические методы защиты информации

РАЗДЕЛ 2. СОДЕРЖАНИЕ И ОБЕСПЕЧЕНИЕ РЕАЛИЗАЦИИ ДИСЦИПЛИН МОДУЛЯ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ 1

Криптографические алгоритмы и протоколы

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Чадов Антон Юрьевич,		старший преподаватель кафедры защиты информации	МИФИ

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

2. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ 1

Криптографические алгоритмы и протоколы

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	**Криптографические алгоритмы**	Способы криптографической защиты информации. Криптосистемы с секретным ключом. Инфраструктура открытых ключей Поточные и блочные алгоритмы
~~**2**~~	**Введение в криптографические протоколы**	Криптографические протоколы и основные требования к ним Протоколы обмена ключами Протоколы идентификации/аутентификации
~~**3**~~	**Криптографические протоколы**	Протоколы защиты данных в сети Internet Протоколы генерации и распределения ключей Протоколы разделения секретов. Протоколы с нулевым разглашением и доказательство нулевого разглашения

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

Основная литература

1. Криптографические методы защиты информации [Текст]: учеб. пособие для вузов / С. М. Владимиров [и др.]; М-во образования и науки РФ, Моск. физ.-техн. ин-т (гос. ун-т), Каф. радиотехники и систем управления. — 2-е изд., перераб. и доп. — М.: МФТИ,

2016. — 266 с. - Библиогр.: с. 215. - Предм. указ.: с. 262-265. - 200 экз. - ISBN 978-5-7417-0615-2.

Дополнительная литература

1. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си [Текст]: [монография] / Б. Шнайер; [науч.-техн. ред. пер. П. В. Семьянов]. — [Научное изд.]. —М.: ТРИУМФ, 2003. — 816 с. - Библиогр.: с. 741-796. - 4000 экз. - ISBN 5-89392-055-4 (в пер.).

7. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины

1. *Электронный научный архив УрФУ: URL: http://elar.urfu.ru.*
2. *Электронная библиотека МФТИ: URL: http://lib.mipt.ru.*
3. *Система дистанционного обучения МФТИ: URL: http://moodle.phystech.edu.*
4. *Криптографические протоколы: основные свойства и уязвимости: URL: https://cyberleninka.ru/article/n/kriptograficheskie-protokoly-osnovnye-svoystva-i-uyazvimosti*
5. *Криптографические методы защиты информации. Учебное пособие: URL: https://github.com/vlsergey/infosec/releases/*

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

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. 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*	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.

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

ПРОГРАММА МОДУЛЯ

Криптографические методы защиты информации

РАЗДЕЛ 2. СОДЕРЖАНИЕ И ОБЕСПЕЧЕНИЕ РЕАЛИЗАЦИИ ДИСЦИПЛИН МОДУЛЯ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ 2

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	Каннер Татьяна Михайловна,		ведущий инженер лаборатории прикладных исследований	МФТИ-Сбербанк

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

2. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ 2
Криптографические методы и средства защиты 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

Таблица 1.3

Код раздела, темы	Раздел, тема дисциплины*	Содержание
1	Меры защиты информации от НСД	Общая характеристика и классификация мер защиты информации от НСД Требования к мерам защиты информации от НСД Текущий контроль знаний1
~~**2**~~	Средства защиты информации от НСД	Резидентный компонент безопасности Концепция корректного старта и ее развитие в истории эволюции СВТ и СЗИ Ключевые характеристики и применение Доверенная загрузка операционных систем. СЗИ НСД «Аккорд-АМДЗ» Общие сведения о комплексе Установка и настройка комплекса Настройка комплекса (продолжение). Режимы доступа к аппаратным ресурсам платы контроллера Разграничение доступа пользователей в ОС Windows. ПАК СЗИ НСД «Аккорд-Win64» (TSE) Общие сведения о комплексе Построение системы защиты информации на основе комплекса Установка комплекса Учетные записи пользователей комплекса Права доступа пользователей комплекса Права доступа пользователей комплекса (продолжение) Контроль целостности объектов Дискреционный механизм управления доступом Дискреционный механизм управления доступом. Установка ПРД к сетевым ресурсам, съемным и стационарным устройствам Мандатный механизм управления доступом Контроль процессов с использованием дискреционного и/или мандатного механизмов разграничения доступа Особенности защиты систем терминального доступа с использованием ПАК СЗИ НСД «Аккорд-Win64» (TSE) Установка комплекса на терминальном сервере Установка и настройка клиентского ПО комплекса на удаленном терминале Сетевое администрирование комплексов СЗИ НСД семейства «Аккорд» Общие сведения о СУЦУ

		Установка и настройка СУЦУ Разграничение доступа пользователей в ОС Linux. ПАК СЗИ НСД «Аккорд-X» Общие сведения о комплексе Обзор и настройка комплекса Настройка и использование комплекса Защита инфраструктуры виртуализации с помощью ПАК «Аккорд-В.» и «Сегмент-В.» Общие сведения о ПАК «Аккорд-В.» Начало работы с ПАК «Аккорд-В.» Установка ПАК «Аккорд-В.» Установка агентов и сервиса регистрации событий. Настройка СПО «Аккорд-В.» Настройка и функционирование СПО «Аккорд-В.» Настройка и функционирование СПО «Аккорд-В.» (продолжение) Общие сведения о ПАК «Сегмент-В.» Межсетевые экраны Средства антивирусной защиты Текущий контроль знаний1

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

1. Конявский В. А. Доверенные информационные технологии: от архитектуры к системам и средствам / В. А. Конявский, С. В. Конявская. – М.: ЛЕНАНД, 2019 . – 264с. – (Основы защиты информации. №19). – Библиогр.: с. 256-261. – ISBN 978-5-9710-6514-2 .

2. Программно-аппаратная защита информации: Учебное пособие/П.Б. Хорев. – М.: Форум, 2012. – 352 с. – ISBN 978-5-91134-353-8

Дополнительная литература

1. Конявский В. А. Основы понимания феномена электронного обмена информацией [Текст] / В. А. Конявский, В. А. Гадасин. – [Научное изд.] . – Минск : Беллтфонд, 2004 . – 282 с. – (Библиотека журнала "УЗИ" ; кн. 2). - Библиогр.: с. 275-281. – ISBN 985-6546-37-7.

2. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах: учеб. пособие для вузов / В. Ф. Шаньгин. – М. : ФОРУМ : ИНФРА-М, 2010 . – 592 с. : ил. – (Высшее образование). – Библиогр.: с. 568-573. – Предм. указ.: с. 574-584. – ISBN 978-5-8199-0411-4 (в пер.)

3. Доктрина информационной безопасности Российской Федерации. Утверждена

Президентом Российской Федерации 5 декабря 2016 г. № 646.
4. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины
1. Электронная библиотека МФТИ: http://lib.mipt.ru/
2. Банк данных угроз безопасности информации: https://bdu.fstec.ru/
3. Официальный интернет-портал правовой информации: http://www.pravo.gov.ru
4. Сайт ФСТЭК России: https://fstec.ru/
5. Информационно-правовой портал «Гарант»: https://www.garant.ru/
6. Справочная правовая система «Консультант Плюс»: https://www.consultant.ru/
7. Сайт производителя программно-аппаратных комплексов СЗИ: https://www.okbsapr.ru/ **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.*