

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
"Казанский (Приволжский) федеральный университет"
Институт вычислительной математики и информационных технологий



УТВЕРЖДАЮ

Проректор по образовательной деятельности КФУ

Е.А. Турилова

28 февраля 2025 г.

подписано электронно-цифровой подписью

Программа дисциплины

Методы и средства криптографической защиты информации

Направление подготовки: 10.03.01 - Информационная безопасность

Профиль подготовки: Безопасность компьютерных систем

Квалификация выпускника: бакалавр

Форма обучения: очное

Язык обучения: русский

Год начала обучения по образовательной программе: 2025

Содержание

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения ОПОП ВО
2. Место дисциплины (модуля) в структуре ОПОП ВО
3. Объем дисциплины (модуля) в зачетных единицах с указанием количества часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся
4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий
 - 4.1. Структура и тематический план контактной и самостоятельной работы по дисциплине (модулю)
 - 4.2. Содержание дисциплины (модуля)
5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)
6. Фонд оценочных средств по дисциплине (модулю)
7. Перечень литературы, необходимой для освоения дисциплины (модуля)
8. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)
9. Методические указания для обучающихся по освоению дисциплины (модуля)
10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости)
11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)
12. Средства адаптации преподавания дисциплины (модуля) к потребностям обучающихся инвалидов и лиц с ограниченными возможностями здоровья
13. Приложение №1. Фонд оценочных средств
14. Приложение №2. Перечень литературы, необходимой для освоения дисциплины (модуля)
15. Приложение №3. Перечень информационных технологий, используемых для освоения дисциплины (модуля), включая перечень программного обеспечения и информационных справочных систем

Программу дисциплины разработал(а)(и): доцент, к.н. Мубараков Б.Г. (кафедра системного анализа и информационных технологий, отделение фундаментальной информатики и информационных технологий), BGMubarakov@kpfu.ru

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения ОПОП ВО

Обучающийся, освоивший дисциплину (модуль), должен обладать следующими компетенциями:

Шифр компетенции	Расшифровка приобретаемой компетенции
ОПК-1.1	Способен разрабатывать и реализовывать политики управления доступом в компьютерных системах
ОПК-9	Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности

Обучающийся, освоивший дисциплину (модуль):

Должен знать:

- основы и различные виды криптографических протоколов.
- стандартные криптографические протоколы.

Должен уметь:

- применять криптографические протоколы для решения задачи конфиденциальной обработки и передачи информации.
- на практике применять криптографические алгоритмы и протоколы для защиты информации.

Должен владеть:

- теоретическими знаниями о базовых разделах теории криптографических протоколов.
- навыками реализации криптографических протоколов

Должен демонстрировать способность и готовность:

- применять полученные знания и навыки в своей дальнейшей профессиональной деятельности.

2. Место дисциплины (модуля) в структуре ОПОП ВО

Данная дисциплина (модуль) включена в раздел "Б1.О.06.08 Дисциплины (модули)" основной профессиональной образовательной программы 10.03.01 "Информационная безопасность (Безопасность компьютерных систем)" и относится к обязательной части ОПОП ВО.

Осваивается на 4 курсе в 8 семестре.

3. Объем дисциплины (модуля) в зачетных единицах с указанием количества часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины составляет 5 зачетных(ые) единиц(ы) на 180 часа(ов).

Контактная работа - 80 часа(ов), в том числе лекции - 40 часа(ов), практические занятия - 0 часа(ов), лабораторные работы - 40 часа(ов), контроль самостоятельной работы - 0 часа(ов).

Самостоятельная работа - 46 часа(ов).

Контроль (зачёт / экзамен) - 54 часа(ов).

Форма промежуточного контроля дисциплины: экзамен в 8 семестре.

4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1 Структура и тематический план контактной и самостоятельной работы по дисциплине (модулю)

N	Разделы дисциплины / модуля	Се- мestr	Виды и часы контактной работы, их трудоемкость (в часах)						Само- стое- тель- ная ра- бота
			Лекции, всего	Лекции в эл. форме	Практические занятия, всего	Практические в эл. форме	Лабора-торные работы, всего	Лабора-торные в эл. форме	
1.	Тема 1. Введение в криптографические протоколы.	8	6	0	0	0	6	0	7
2.	Тема 2. Модель интерактивной системы доказательства.	8	8	0	0	0	8	0	7
3.	Тема 3. Протоколы совместных вычислений.	8	6	0	0	0	6	0	7
4.	Тема 4. Протоколы разделения секрета.	8	6	0	0	0	6	0	7
5.	Тема 5. Протоколы анонимности.	8	6	0	0	0	6	0	7
6.	Тема 6. Протоколы консенсуса.	8	8	0	0	0	8	0	11
	Итого		40	0	0	0	40	0	46

4.2 Содержание дисциплины (модуля)

Тема 1. Введение в криптографические протоколы.

История возникновения криптографических протоколов. Односторонние функции и гипотеза о существовании односторонних функций. Идеи Диффи-Хеллмана. Криптографический протокол формирования ключей Диффи-Хеллмана. Атака "man-in-the-middle". Идея криптографического протокола цифровой подписи Диффи-Хеллмана.

Тема 2. Модель интерактивной системы доказательства.

Определение интерактивной системы доказательства. Пример интерактивной системы доказательства, основанный на теории чисел. Свойства интерактивной системы доказательства. Доказательства с нулевым разглашением. Задача "пещера Али-Бабы". Структура доказательств с нулевым разглашением. Вероятностные доказательства.

Тема 3. Протоколы совместных вычислений.

Формализованная постановка задачи многосторонних вычислений. Требования к безопасности многосторонних вычислений. Пример решения задачи миллионеров. Проблемы реализации. Пример протокола - удаленное подбрасывание монеты. Реализация криптографического протокола подбрасывания монеты. Практическое применение.

Тема 4. Протоколы разделения секрета.

Постановка проблемы разделения секрета. Примеры: кодовый замок и проекции геометрических фигур. Криптографический протокол разделения секрета. Пороговые системы. Схема Блекли. Схема Шамира. Схема на основе китайской теоремы об остатках. Совершенные и идеальные схемы разделения секрета. Приложения.

Тема 5. Протоколы анонимности.

Формализованная постановка задачи обеспечения анонимности. Задача о трех обедающих криптографах. Вариант решения задачи об обедающих криптографах. Идеи Дэвида Чаума обеспечения анонимности в сети. Протокол тайного цифрового голосования. Формальные требования к системам цифрового голосования. Пример простого протокола. Протокол Фудзиока-Окамото-Охта.

Тема 6. Протоколы консенсуса.

Формализованная постановка задачи обеспечения консенсуса в сети. Обычные ошибки и византийские ошибки. Задача византийских генералов. Протокол Delegated Byzantine Fault Tolerance. Протокол Practical Byzantine Fault Tolerance. Протокол Federated Byzantine Agreement. Протоколы криптовалют: Proof-of-Work, Proof-of-Stake, Delegated Proof-of-Stake. Протоколы не для блокчейна.

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

Самостоятельная работа обучающихся выполняется по заданию и при методическом руководстве преподавателя, но без его непосредственного участия. Самостоятельная работа подразделяется на самостоятельную работу на аудиторных занятиях и на внеаудиторную самостоятельную работу. Самостоятельная работа обучающихся включает как полностью самостоятельное освоение отдельных тем (разделов) дисциплины, так и проработку тем (разделов), осваиваемых во время аудиторной работы. Во время самостоятельной работы обучающиеся читают и конспектируют учебную, научную и справочную литературу, выполняют задания, направленные на закрепление знаний и отработку умений и навыков, готовятся к текущему и промежуточному контролю по дисциплине.

Организация самостоятельной работы обучающихся регламентируется нормативными документами, учебно-методической литературой и электронными образовательными ресурсами, включая:

Порядок организации и осуществления образовательной деятельности по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры (утвержден приказом Министерства науки и высшего образования Российской Федерации от 6 апреля 2021 года №245)

Письмо Министерства образования Российской Федерации №14-55-996бин/15 от 27 ноября 2002 г. "Об активизации самостоятельной работы студентов высших учебных заведений"

Устав федерального государственного автономного образовательного учреждения "Казанский (Приволжский) федеральный университет"

Правила внутреннего распорядка федерального государственного автономного образовательного учреждения высшего профессионального образования "Казанский (Приволжский) федеральный университет"

Локальные нормативные акты Казанского (Приволжского) федерального университета

6. Фонд оценочных средств по дисциплине (модулю)

Фонд оценочных средств по дисциплине (модулю) включает оценочные материалы, направленные на проверку освоения компетенций, в том числе знаний, умений и навыков. Фонд оценочных средств включает оценочные средства текущего контроля и оценочные средства промежуточной аттестации.

В фонде оценочных средств содержится следующая информация:

- соответствие компетенций планируемым результатам обучения по дисциплине (модулю);
- критерии оценивания сформированности компетенций;
- механизм формирования оценки по дисциплине (модулю);
- описание порядка применения и процедуры оценивания для каждого оценочного средства;
- критерии оценивания для каждого оценочного средства;
- содержание оценочных средств, включая требования, предъявляемые к действиям обучающихся, демонстрируемым результатам, задания различных типов.

Фонд оценочных средств по дисциплине находится в Приложении 1 к программе дисциплины (модулю).

7. Перечень литературы, необходимой для освоения дисциплины (модуля)

Освоение дисциплины (модуля) предполагает изучение основной и дополнительной учебной литературы. Литература может быть доступна обучающимся в одном из двух вариантов (либо в обоих из них):

- в электронном виде - через электронные библиотечные системы на основании заключенных КФУ договоров с правообладателями;
- в печатном виде - в Научной библиотеке им. Н.И. Лобачевского. Обучающиеся получают учебную литературу на абонементе по читательским билетам в соответствии с правилами пользования Научной библиотекой.

Электронные издания доступны дистанционно из любой точки при введении обучающимся своего логина и пароля от личного кабинета в системе "Электронный университет". При использовании печатных изданий библиотечный фонд должен быть укомплектован ими из расчета не менее 0,5 экземпляра (для обучающихся по ФГОС 3++ - не менее 0,25 экземпляра) каждого из изданий основной литературы и не менее 0,25 экземпляра дополнительной литературы на каждого обучающегося из числа лиц, одновременно осваивающих данную дисциплину.

Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля), находится в Приложении 2 к рабочей программе дисциплины. Он подлежит обновлению при изменении условий договоров КФУ с правообладателями электронных изданий и при изменении комплектования фондов Научной библиотеки КФУ.

8. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)

Интернет-портал образовательных ресурсов по ИТ - <http://www.intuit.ru/>

Интернет-портал образовательных ресурсов по ИТЦифровой образовательный ресурс "Введение в кибербезопасность", Дальневосточный федеральный университет - <https://stepik.org/course/61595>

Информационный портал по защите информации - <http://all-ib.ru/>

Цифровой образовательный ресурс "Введение в современную криптографию", МИФИ - https://openedu.ru/course/mephi/mephi_011_crypto/

Цифровой образовательный ресурс "Защита информации", ВШЭ - <https://openedu.ru/course/hse/DATPRO/>

Цифровой образовательный ресурс "Основы обеспечения информационной безопасности" - https://openedu.ru/course/bmstu/MGTU_6/

9. Методические указания для обучающихся по освоению дисциплины (модуля)

Вид работ	Методические рекомендации
лекции	Теоретический курса материал излагается на лекциях. Причем конспект лекций, который остается у студента в результате прослушивания лекции не может заменить учебник. Его цель-формулировка основных утверждений и определений. Прослушав лекцию, полезно ознакомиться с более подробным изложением материала в учебнике. Список литературы разделен на две категории: необходимый для сдачи экзамена минимум и дополнительная литература.
лабораторные работы	Лабораторные занятия призваны дать такой практический навык, а также навыки программирования криптографических алгоритмов и их внедрения в информационные системы. В ходе выполнения работ происходит отработка знаний студентов по программированию криптографических алгоритмов, изучение специальных разделов программирования алгоритмов сетевого взаимодействия.
самостоятельная работа	Самостоятельная работа предполагает выполнение домашних работ при подготовке к контрольной работе и выполнении компьютерной программы. Самостоятельная работа выполняется в несколько этапов. Сначала предполагается изучение теоретического материала. Также рекомендуется каждый раздел программы сопровождать практической работой, выполняя лабораторные занятия
экзамен	Рекомендуется разбивать материал на смысловые блоки и изучать его, выписывая краткое содержание блока. По каждому блоку надо составить контрольные вопросы и самостоятельно составить краткие ответы по вопросам. Прочитав лекции, полезно ознакомиться с более подробным изложением материала в учебнике. Список литературы разделен на две категории: необходимый для сдачи экзамена минимум и дополнительная литература.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости)

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем, представлен в Приложении 3 к рабочей программе дисциплины (модуля).

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

Материально-техническое обеспечение образовательного процесса по дисциплине (модулю) включает в себя следующие компоненты:

Помещения для самостоятельной работы обучающихся, укомплектованные специализированной мебелью (столы и стулья) и оснащенные компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду КФУ.

Учебные аудитории для контактной работы с преподавателем, укомплектованные специализированной мебелью (столы и стулья).

Компьютер и принтер для распечатки раздаточных материалов.

Мультимедийная аудитория.

12. Средства адаптации преподавания дисциплины к потребностям обучающихся инвалидов и лиц с ограниченными возможностями здоровья

При необходимости в образовательном процессе применяются следующие методы и технологии, облегчающие восприятие информации обучающимися инвалидами и лицами с ограниченными возможностями здоровья:

- создание текстовой версии любого нетекстового контента для его возможного преобразования в альтернативные формы, удобные для различных пользователей;

- создание контента, который можно представить в различных видах без потери данных или структуры, предусмотреть возможность масштабирования текста и изображений без потери качества, предусмотреть доступность управления контентом с клавиатуры;
- создание возможностей для обучающихся воспринимать одну и ту же информацию из разных источников - например, так, чтобы лица с нарушениями слуха получали информацию визуально, с нарушениями зрения - аудиально;
- применение программных средств, обеспечивающих возможность освоения навыков и умений, формируемых дисциплиной, за счёт альтернативных способов, в том числе виртуальных лабораторий и симуляционных технологий;
- применение дистанционных образовательных технологий для передачи информации, организации различных форм интерактивной контактной работы обучающегося с преподавателем, в том числе вебинаров, которые могут быть использованы для проведения виртуальных лекций с возможностью взаимодействия всех участников дистанционного обучения, проведения семинаров, выступления с докладами и защиты выполненных работ, проведения тренингов, организации коллективной работы;
- применение дистанционных образовательных технологий для организации форм текущего и промежуточного контроля;
- увеличение продолжительности сдачи обучающимся инвалидом или лицом с ограниченными возможностями здоровья форм промежуточной аттестации по отношению к установленной продолжительности их сдачи:

 - продолжительности сдачи зачёта или экзамена, проводимого в письменной форме, - не более чем на 90 минут;
 - продолжительности подготовки обучающегося к ответу на зачёте или экзамене, проводимом в устной форме, - не более чем на 20 минут;
 - продолжительности выступления обучающегося при защите курсовой работы - не более чем на 15 минут.

Программа составлена в соответствии с требованиями ФГОС ВО и учебным планом по направлению 10.03.01 "Информационная безопасность" и профилю подготовки "Безопасность компьютерных систем".

Приложение 2
к рабочей программе дисциплины (модуля)
Б1.0.06.08 Методы и средства криптографической защиты информации

Перечень литературы, необходимой для освоения дисциплины (модуля)

Направление подготовки: 10.03.01 - Информационная безопасность

Профиль подготовки: Безопасность компьютерных систем

Квалификация выпускника: бакалавр

Форма обучения: очное

Язык обучения: русский

Год начала обучения по образовательной программе: 2025

Основная литература:

1. Мельников, Д.А. Информационная безопасность открытых систем : учебник / Д.А. Мельников. - 3-е изд., стер. - Москва : ФЛИНТА, 2019. - 444 с. - ISBN 978-5-9765-1613-7. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1042499> (дата обращения: 14.01.2025). - Режим доступа: по подписке.
2. Криптографическая защита информации : учебное пособие / С.О. Крамаров, О.Ю. Митясова, С.В. Соколов [и др.] ; под ред. С.О. Крамарова. - Москва : РИОР : ИНФРА-М, 2025. - 321 с. - (Высшее образование). - DOI: <https://doi.org/10.12737/1716-6>. - ISBN 978-5-369-01716-6. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/2169480> (дата обращения: 14.01.2025). - Режим доступа: по подписке.
3. Романьков, В. А. Введение в криптографию : курс лекций / В.А. Романьков. - 2-е изд., испр. и доп. - Москва : ФОРУМ : ИНФРА-М, 2025. - 240 с. - (Высшее образование). - ISBN 978-5-00091-493-9. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/2178770> (дата обращения: 14.01.2025). - Режим доступа: по подписке.
4. Пилиди, В. С. Математические основы защиты информации : учебное пособие / В. С. Пилиди ; Южный федеральный университет. - Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2019. - 308 с. - ISBN 978-5-9275-3363-3. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1088209> (дата обращения: 14.01.2025). - Режим доступа: по подписке.
5. Штарьков, Ю. М. Универсальное кодирование. Теория и алгоритмы : учебное пособие / Ю. М. Штарьков. - Москва : ФИЗМАТЛИТ, 2013. - 288 с. - ISBN 978-5-9221-1517-9. - Текст : электронный // Лань : электронно-библиотечная система. - URL: <https://e.lanbook.com/book/59667> (дата обращения: 14.01.2025). - Режим доступа: для авториз. пользователей.

Дополнительная литература:

1. Сидельников, В. М. Теория кодирования / В. М. Сидельников. - Москва : ФИЗМАТЛИТ, 2008. - 324 с. - ISBN 978-5-9221-0943-7. - Текст : электронный. - URL: <https://znanium.com/catalog/product/544713> (дата обращения: 14.01.2025). - Режим доступа: по подписке.
2. Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 3-е изд. - Москва : РИОР : ИНФРА-М, 2024. - 400 с. - (Высшее образование). - DOI: <https://doi.org/10.12737/1759-3>. - ISBN 978-5-369-01759-3. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/2140566> (дата обращения: 14.01.2025). - Режим доступа: по подписке.
3. Мартынов, Л. М. Алгебра и теория чисел для криптографии / Л. М. Мартынов. - 3-е изд., стер. - Санкт-Петербург : Лань, 2024. - 456 с. - ISBN 978-5-507-48774-5. - Текст : электронный // Лань : электронно-библиотечная система. - URL: <https://e.lanbook.com/book/362942> (дата обращения: 14.01.2025). - Режим доступа: для авториз. пользователей.
4. Информационный мир XXI века. Криптография - основа информационной безопасности : научно-популярное издание / под ред. Э. А. Болелова ; Московский государственный технический университет гражданской авиации. - 6-е изд. - Москва : Издательско-торговая корпорация 'Дашков и К', 2022. - 126 с. - ISBN 978-5-394-04804-3. - Текст : электронный. - URL: <https://znanium.com/catalog/product/2082694> (дата обращения: 14.01.2025). - Режим доступа: по подписке.

Приложение 3
к рабочей программе дисциплины (модуля)
Б1.0.06.08 Методы и средства криптографической защиты информации

**Перечень информационных технологий, используемых для освоения дисциплины (модуля), включая
перечень программного обеспечения и информационных справочных систем**

Направление подготовки: 10.03.01 - Информационная безопасность

Профиль подготовки: Безопасность компьютерных систем

Квалификация выпускника: бакалавр

Форма обучения: очное

Язык обучения: русский

Год начала обучения по образовательной программе: 2025

Освоение дисциплины (модуля) предполагает использование следующего программного обеспечения и информационно-справочных систем:

Операционная система Microsoft Windows 7 Профессиональная или Windows XP (Volume License)

Пакет офисного программного обеспечения Microsoft Office 365 или Microsoft Office Professional plus 2010

Браузер Mozilla Firefox

Браузер Google Chrome

Adobe Reader XI или Adobe Acrobat Reader DC

Kaspersky Endpoint Security для Windows

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе "ZNANIUM.COM", доступ к которой предоставлен обучающимся. ЭБС "ZNANIUM.COM" содержит произведения крупнейших российских учёных, руководителей государственных органов, преподавателей ведущих вузов страны, высококвалифицированных специалистов в различных сферах бизнеса. Фонд библиотеки сформирован с учетом всех изменений образовательных стандартов и включает учебники, учебные пособия, учебно-методические комплексы, монографии, авторефераты, диссертации, энциклопедии, словари и справочники, законодательно-нормативные документы, специальные периодические издания и издания, выпускаемые издательствами вузов. В настоящее время ЭБС ZNANIUM.COM соответствует всем требованиям федеральных государственных образовательных стандартов высшего образования (ФГОС ВО) нового поколения.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе Издательства "Лань", доступ к которой предоставлен обучающимся. ЭБС Издательства "Лань" включает в себя электронные версии книг издательства "Лань" и других ведущих издательств учебной литературы, а также электронные версии периодических изданий по естественным, техническим и гуманитарным наукам. ЭБС Издательства "Лань" обеспечивает доступ к научной, учебной литературе и научным периодическим изданиям по максимальному количеству профильных направлений с соблюдением всех авторских и смежных прав.