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

Введение в информационную безопасность

Направление подготовки: 02.03.02 - Фундаментальная информатика и информационные технологии
Профиль подготовки: Фундаментальная информатика и информационные технологии
Квалификация выпускника: бакалавр
Форма обучения: очное
Язык обучения: русский
Год начала обучения по образовательной программе: 2025

Содержание

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
ПК-11	Способен использовать действующее законодательство и другие правовые документы в своей профессиональной деятельности

Обучающийся, освоивший дисциплину (модуль):

Должен знать:

- значение информационной безопасности в структуре национальной безопасности.
- основы государственной политики в области информационной безопасности, понятийный аппарат информационной безопасности.
- принципы политики управления доступом подсистемы информационной безопасности объекта защиты.
- основы построения средств защиты информации прикладного и системного программного обеспечения.

Должен уметь:

- применять на практике основные общеметодологические принципы обеспечения информационной безопасности.
- находить необходимые нормативные правовые акты и информационно-правовые нормы в системе действующего законодательства.
- решать задачи для разработки и реализации политики управления доступом в компьютерных системах и подсистемах информационной безопасности объекта защиты.
- применять на практике методы и средства защиты информации.

Должен владеть:

- базовыми методами и средствами обеспечения информационной безопасности.
- навыками анализа данных для выбора способов решения задач в области информационной безопасности.
- навыками внедрения и развития политики управления доступом в компьютерных системах.
- навыками анализа, выбора и администрирования средств защиты информации.

Должен демонстрировать способность и готовность:

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

2. Место дисциплины (модуля) в структуре ОПОП ВО

Данная дисциплина (модуль) включена в раздел "Б1.В.13 Дисциплины (модули)" основной профессиональной образовательной программы 02.03.02 "Фундаментальная информатика и информационные технологии (Фундаментальная информатика и информационные технологии)" и относится к части ОПОП ВО, формируемой участниками образовательных отношений.

Осваивается на 1 курсе в 2 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 2 зачетных(ые) единиц(ы) на 72 часа(ов).

Контактная работа - 18 часа(ов), в том числе лекции - 18 часа(ов), практические занятия - 0 часа(ов), лабораторные работы - 0 часа(ов), контроль самостоятельной работы - 0 часа(ов).

Самостоятельная работа - 54 часа(ов).

Контроль (зачёт / экзамен) - 0 часа(ов).

Форма промежуточного контроля дисциплины: зачет во 2 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-местр	Виды и часы контактной работы, их трудоемкость (в часах)						Само-стоя-тель-ная ра-бота
			Лекции, всего	Лекции в эл. форме	Практи-ческие занятия, всего	Практи-ческие в эл. форме	Лабора-торные работы, всего	Лабора-торные в эл. форме	
1.	Тема 1. Сущность, задачи информационной безопасности.	2	2	2	0	0	0	0	6
2.	Тема 2. Методы контроля доступа к информации.	2	2	2	0	0	0	0	6
3.	Тема 3. Введение в математические основы защиты информации.	2	2	2	0	0	0	0	6
4.	Тема 4. Симметричные алгоритмы шифрования.	2	2	2	0	0	0	0	6
5.	Тема 5. Асимметричные методы шифрования. Алгоритм RSA.	2	2	2	0	0	0	0	6
6.	Тема 6. Асимметричные методы шифрования. Алгоритм Диффи-Хеллмана.	2	2	2	0	0	0	0	6
7.	Тема 7. Проблемы обеспечения безопасности операционных систем.	2	2	2	0	0	0	0	6
8.	Тема 8. Компьютерные вирусы и проблемы антивирусной защиты.	2	2	2	0	0	0	0	6
9.	Тема 9. Задачи управления системой сетевой безопасности.	2	2	2	0	0	0	0	6
	Итого		18	18	0	0	0	0	54

4.2 Содержание дисциплины (модуля)

Тема 1. Сущность, задачи информационной безопасности.

Рассматриваются основные задачи и проблемы информационной безопасности.

1.1. Введение в защиту информации.

1.2. Современная постановка задачи защиты информации.

1.3. Угрозы безопасности информационным системам и их классификация.

1.4. Меры противодействия угрозам безопасности ИС.

1.5. Сервисы информационной безопасности.

Тема 2. Методы контроля доступа к информации.

Рассматриваются основные методы контроля доступа к информации.

2.1. Классификация средств идентификации и аутентификации с точки зрения применяемых технологий.

2.2. Биометрия. Статические методы.

2.3. Биометрия.Динамические методы.

2.4. Технологии аутентификации.Варианты реализации систем аутентификации.

2.5. Протоколы аутентификации.

Тема 3. Введение в математические основы защиты информации.

Рассматриваются математические основы защиты информации.

3.1.Модулярная арифметика. Малая теорема Ферма. Функция Эйлера.

3.2. Квадратичные вычеты и невычеты. Символ Лежандра и его свойства.

3.3. Алгоритм вычисления символа Лежандра.

3.4. Символ Якоби и его свойства. Алгоритм вычисления символа Якоби.

3.5. Простые числа. Генерация простых чисел. Решето Эратосфена.

3.6. Вероятностные методы поиска простых чисел.

Тема 4. Симметричные алгоритмы шифрования.

Рассматриваются классические алгоритмы симметричного шифрования.

4.1. Основные криптографические термины и определения.

4.2. Блочные шифры и основы построения блочных шифров.

4.3. Примитивные операции.

4.4. Шифр Цезаря.

4.5. Система шифрования Вижинера. Криптоанализ.

4.6. Шифры простой замены.

4.7. Шифры сложной замены.

4.8. Блочные шифры.

Тема 5. Асимметричные методы шифрования. Алгоритм RSA.

Рассматриваются основные идеи построения асимметричных методов шифрования.

5.1. История алгоритма RSA.

5.2. Алгоритм RSA. Описание алгоритма. Методы генерации ключей.

5.3. Вспомогательные алгоритмы RSA.Алгоритм быстрого возведения числа в степень по модулю n. Расширенный алгоритм Евклида. Примеры.

Тема 6. Асимметричные методы шифрования. Алгоритм Диффи-Хеллмана.

Рассматриваются основные идеи построения асимметричных методов шифрования.

6.1.Основные требования к алгоритмам асимметричного шифрования.

6.2. Криптоанализ алгоритмов с открытым ключом.

6.3. Основные способы использования алгоритмов с открытым ключом.

6.4. Диффи-Хеллмана. Описание алгоритма. Методы атак на Алгоритм Диффи-Хеллмана. MITM атака. Применение алгоритма Диффи-Хеллмана.

Тема 7. Проблемы обеспечения безопасности операционных систем.

Рассматриваются основные проблемы обеспечения безопасности операционных систем.

7.1. Угрозы безопасности операционных систем и классификация по различным

аспектам их реализации

7.2. Понятие защищенной операционной системы.

7.3. Подходы к построению защищенных операционных систем.

7.4. Административные меры защиты.

Тема 8. Компьютерные вирусы и проблемы антивирусной защиты.

Рассматриваются основные виды компьютерных вирусов и проблемы антивирусной защиты.

8.1. Классификация компьютерных вирусов.

8.2. Жизненный цикл вирусов.

8.3. Вредоносные программы других типов

8.4. Основные каналы распространения вирусов и других вредоносных программ.

8.5. Антивирусные программы и комплексы.

Тема 9. Задачи управления системой сетевой безопасности.

Рассматриваются основные задачи и подходы управления системой сетевой безопасности.

9.1. Архитектура управления средствами сетевой безопасности.

9.2. Основные понятия.

9.3. Концепция глобального управления безопасностью.

9.4. Глобальная и локальная политики безопасности.

9.5. Функционирование системы управления средствами безопасности.

9.6. Аудит и мониторинг безопасности.

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 №14-55-996ин/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 с образовательными ресурсами по ИТ - http://www.intuit.ru/

Научная электронная библиотека - https://elibrary.ru/

Официальный сайт ФСТЭК России - http://www.fstec.ru/

Справочная система MSDN - http://msdn.com/

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

Вид работ	Методические рекомендации
лекции	Во время лекций студенты должны сосредоточить внимание на её содержании. Основные положения лекции, важные определения и теоретические положения необходимо записывать. Конспектирование предлагаемого преподавателем материала вырабатывает у студентов навыки самостоятельного отбора и анализа необходимой для них информации, умение более сжато и четко записывать услышанное. Лекции могут служить необходимым вспомогательным материалом в процессе подготовки к самостоятельной работе и зачету.
самостоя-тельная работа	Изучение основ информационной безопасности предусматривает систематическую самостоятельную работу студентов над дополнительными материалами; развитие навыков самоконтроля, способствующих интенсификации учебного процесса. Изучение лекционного материала по конспекту лекций должно сопровождаться изучением рекомендуемой литературы, основной и дополнительной. Основной целью организации самостоятельной работы студентов является систематизация и активизация знаний, полученных ими на лекциях. Студентам следует стремиться к активизации знаний на занятиях и по другим общематематическим дисциплинам. Самостоятельная работа по изучению курса предполагает внеаудиторную работу, которая включает: 1. Выполнение тестовых заданий. 2. Изучение вопросов, оставленных на самостоятельное изучение. 3. Подготовку к зачету.
зачет	Залогом успешной сдачи зачета является работа в течение всего семестра и выполнение тестового задания. Основным источником подготовки к зачету является конспект лекций. Правильно составленный конспект лекций содержит тот оптимальный объем информации, на основе которого студент сможет представить себе весь учебный материал. В ходе подготовки к зачету студентам необходимо обращать внимание не только на уровень запоминания, но и на степень понимания основных понятий.

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 02.03.02 "Фундаментальная информатика и информационные технологии" и профилю подготовки "Фундаментальная информатика и информационные технологии".

Приложение 2
к рабочей программе дисциплины (модуля)
Б1.В.13 Введение в информационную безопасность

Перечень литературы, необходимой для освоения дисциплины (модуля)

Направление подготовки: 02.03.02 - Фундаментальная информатика и информационные технологии
Профиль подготовки: Фундаментальная информатика и информационные технологии
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: 16.01.2025). - Режим доступа: по подписке.

2. Башлы, П. Н. Информационная безопасность и защита информации: учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - Москва : РИОР, 2013. - 222 с. - ISBN 978-5-369-01178-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/405000 (дата обращения: 16.01.2025). - Режим доступа: по подписке.

3. Нестеров, С. А. Основы информационной безопасности: учебник для вузов / С. А. Нестеров. - 3-е изд., стер. - Санкт-Петербург : Лань, 2024. - 324 с. - ISBN 978-5-507-49077-6. - Текст : электронный // Лань : электронно-библиотечная система. - URL: https://e.lanbook.com/book/370967 (дата обращения: 16.01.2025). - Режим доступа: для авториз. пользователей.

4. 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: 16.01.2025). - Режим доступа: по подписке.

5. Глинская, Е. В. Информационная безопасность конструкций ЭВМ и систем : учебное пособие / Е.В. Глинская, Н.В. Чичварин. - Москва : ИНФРА-М, 2021. - 118 с. - (Высшее образование: Бакалавриат). - DOI 10.12737/13571. - ISBN 978-5-16-010961-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1178152 (дата обращения: 16.01.2025). - Режим доступа: по подписке.

Дополнительная литература:

1. Мартынов, Л. М. Алгебра и теория чисел для криптографии: учебное пособие для вузов / 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: 16.01.2025). - Режим доступа: для авториз. пользователей.

2. Гришина, Н. В. Основы информационной безопасности предприятия : учебное пособие / Н.В. Гришина. - Москва : ИНФРА-М, 2024. - 216 с. - (Высшее образование: Специалитет). - ISBN 978-5-16-016534-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/2131865 (дата обращения: 16.01.2025). - Режим доступа: по подписке.

3. Хорев, П. Б. Программно-аппаратная защита информации : учебное пособие / П.Б. Хорев. - 3-е изд., испр. и доп. - Москва : ИНФРА-М, 2022. - 327 с. - (Высшее образование: Бакалавриат). - DOI 10.12737/1035570. - ISBN 978-5-16-015471-8. - Текст : электронный. - URL: https://znanium.com/catalog/product/1865598 (дата обращения: 16.01.2025). - Режим доступа: по подписке.

4. Васильков, А. В. Безопасность и управление доступом в информационных системах : учебное пособие / А.В. Васильков, И.А. Васильков. - Москва : ФОРУМ : ИНФРА-М, 2022. - 368 с. - (Среднее профессиональное образование). - ISBN 978-5-91134-360-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1836631 (дата обращения: 16.01.2025). - Режим доступа: по подписке.

Приложение 3
к рабочей программе дисциплины (модуля)
Б1.В.13 Введение в информационную безопасность

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

Направление подготовки: 02.03.02 - Фундаментальная информатика и информационные технологии

Профиль подготовки: Фундаментальная информатика и информационные технологии

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.