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
17 февраля 2023 г.

подписано электронно-цифровой подписью

Программа дисциплины

Основы информационной безопасности

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: 2023

Содержание

Программу дисциплины разработал(а)(и): старший преподаватель, б/с Еникеев Р.Р. (кафедра системного анализа и информационных технологий, отделение фундаментальной информатики и информационных технологий), renikeev@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	Способен применять фундаментальные знания, полученные в области математических и (или) естественных наук, и использовать их в профессиональной деятельности
УК-2	Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

Обучающийся, освоивший дисциплину (модуль):

Должен знать:

- криптографические методы защиты информации;
- математические основы криптографии,
- криптографические алгоритмы и протоколы.

Должен уметь:

- применять имеющиеся знания для обеспечения информационной безопасности;
- разрабатывать системы, реализующие криптографические протоколы и алгоритмы.

Должен владеть:

- знаниями и навыками обеспечения информационной безопасности;
- знаниями и навыками разработки защищённых приложений.

Должен демонстрировать способность и готовность:

-применять полученные знания в своей профессиональной деятельности

2. Место дисциплины (модуля) в структуре ОПОП ВО

Данная дисциплина (модуль) включена в раздел "Б1.О.11 Дисциплины (модули)" основной профессиональной образовательной программы 02.03.02 "Фундаментальная информатика и информационные технологии (Фундаментальная информатика и информационные технологии)" и относится к обязательной части ОПОП ВО.

Осваивается на 3 курсе в 6 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 3 зачетных(ые) единиц(ы) на 108 часа(ов).

Контактная работа - 54 часа(ов), в том числе лекции - 36 часа(ов), практические занятия - 0 часа(ов), лабораторные работы - 18 часа(ов), контроль самостоятельной работы - 0 часа(ов).

Самостоятельная работа - 54 часа(ов).

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

Форма промежуточного контроля дисциплины: зачет в 6 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)						Самостоятельная работа
			Лекции, всего	Лекции в эл. форме	Практические занятия, всего	Практические в эл. форме	Лабораторные работы, всего	Лабораторные в эл. форме	
1.	Тема 1. Сущность, задачи информационной безопасности.	6	6	0	0	0	3	0	9
2.	Тема 2. Методы контроля доступа к информации.	6	6	0	0	0	3	0	9
3.	Тема 3. Организационно-правовые средства защиты.	6	6	0	0	0	3	0	9
4.	Тема 4. Криптографические средства защиты информации. Метод RSA.	6	6	0	0	0	3	0	9
5.	Тема 5. Сертификаты X.509. Аутентификация на основе сертификатов.	6	6	0	0	0	3	0	9
6.	Тема 6. Системы шифрования на основе эллиптических кривых.	6	6	0	0	0	3	0	9
	Итого		36	0	0	0	18	0	54

4.2 Содержание дисциплины (модуля)

Тема 1. Сущность, задачи информационной безопасности.

Введение в информационную безопасность и защиту информации. Современная постановка задачи защиты информации. Угрозы безопасности в современных информационных системах и их классификация. Меры противодействия угрозам безопасности информационных систем. Классификация основных угроз информационной безопасности.

Тема 2. Методы контроля доступа к информации.

Методы идентификации и аутентификации пользователей, технических средств обработки, программ и баз данных. Классификация информационных систем по степени защищенности. Общие критерии стран Европейского сообщества, их основные положения. Парольная идентификация и аутентификация в сетевых операционных системах.

Тема 3. Организационно-правовые средства защиты.

Законодательный уровень защиты информации. Основные положения закона "Об информации, информатизации и защите информации" от 20 февраля 1995 года, определение понятий информации, документированной информации (документа), информационных процессов, информационной системы, информационных ресурсов. Закон "О лицензировании отдельных видов деятельности" от 8 августа 2001 г

Тема 4. Криптографические средства защиты информации. Метод RSA.

Криптографические средства защиты информации. Криптосистемы с секретным ключом. Математические основы современной криптологии. Электронная цифровая подпись и ее применение. Понятие хэш-функции. Открытое распределение ключей. Алгоритм построения электронной цифровой подписи на основе российского ГОСТа 2012 года.

Тема 5. Сертификаты X.509. Аутентификация на основе сертификатов.

Математические основы построения эллиптических кривых. Прямые и обратные операции в конечных полях. Система шифрования Эль-Гамаля. Реализации системы Эль - Гамаля на эллиптических кривых. Алгоритм электронной подписи на эллиптических кривых с использованием схемы Эль-Гамаля. Российский ГОСТ электронной цифровой подписи.

Тема 6. Системы шифрования на основе эллиптических кривых.

Математические основы построения эллиптические кривых. Прямые и обратные операции в конечных полях. Проективные координаты. Вычисления координат в проективных координатах. Проблема факторизации натуральных чисел. Алгоритм Ленстры вычисления факторов натурального числа на основе эллиптических кривых.

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 образовательных ресурсов по ИТ - http://www.intuit.ru

Интернет-портал ресурсов по математике - http://www.mathnet.ru

Ишмухаметов Ш.Т. Математические основы защиты информации - http://kpfu.ru/docs/F366166681/mzi.pdf

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

электронное пособие - https://kpfu.ru//staff_files/F1107621258/Math_Osnovi_Zach_Inform.pdf

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.
самостоя-тельная 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.
зачет	Зачет проводится в письменной форме с последующим устным собеседованием. При подготовке к сдаче зачета весь объем работы рекомендуется распределять равномерно по дням, отведенным для подготовки к зачету, контролировать каждый день выполнения работы. Лучше, если можно перевыполнить план. Тогда всегда будет резерв времени. Следует по мере подготовки создавать краткие конспекты, словари терминов, карты знаний.

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.

Компьютерный класс.

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.О.11 Основы информационной безопасности

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: 2023

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: 25.01.2023). - 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: 25.01.2023). - Режим доступа: по подписке.

3. 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: 25.01.2023). - Режим доступа: по подписке.

4. Нестеров, С. А. Основы информационной безопасности : учебное пособие / С. А. Нестеров. - 5-е изд., стер. - Санкт-Петербург : Лань, 2022. - 324 с. - ISBN 978-5-8114-4067-2. - Текст : электронный // Лань : электронно-библиотечная система. - URL: https://e.lanbook.com/book/206279 (дата обращения: 25.01.2023). - Режим доступа: для авториз. пользователей.

5. Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 3-е изд. - Москва : РИОР : ИНФРА-М, 2021. - 400 с. - (Высшее образование). - DOI: https://doi.org/10.12737/1759-3. - ISBN 978-5-369-01759-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1210523 (дата обращения: 25.01.2023). - Режим доступа: по подписке.

Дополнительная литература:

1. Мартынов, Л. М. Алгебра и теория чисел для криптографии : учебное пособие для вузов / Л. М. Мартынов. - 2-е изд., стер. - Санкт-Петербург : Лань, 2022. - 456 с. - ISBN 978-5-8114-9346-3. - Текст : электронный // Лань : электронно-библиотечная система. - URL: https://e.lanbook.com/book/189446 (дата обращения: 25.01.2023). - Режим доступа: для авториз. пользователей.

2. Гришина, Н. В. Информационная безопасность предприятия : учебное пособие / Н.В. Гришина. - 2-е изд., доп. - Москва : ФОРУМ : ИНФРА-М, 2022. - 239 с. - (Среднее профессиональное образование). - ISBN 978-5-00091-545-5. - Текст : электронный. - URL: https://znanium.com/catalog/product/1846437 (дата обращения: 25.01.2023). - 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: 25.01.2023). - 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: 25.01.2023). - Режим доступа: по подписке.

Приложение 3
к рабочей программе дисциплины (модуля)
Б1.О.11 Основы информационной безопасности

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: 2023

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.