МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
"Казанский (Приволжский) федеральный университет"
Институт физики

УТВЕРЖДАЮ
Проректор по образовательной деятельности КФУ
Проф. Д.А. Таюрский
_____ «___»_____20__г.

подписано электронно-цифровой подписью

Программа дисциплины

Основы информационной безопасности

Направление подготовки: 03.04.03 - Радиофизика
Профиль подготовки: Информационные процессы и системы
Квалификация выпускника: магистр
Форма обучения: очное
Язык обучения: русский
Год начала обучения по образовательной программе: 2018

Содержание

Программу дисциплины разработал(а)(и) профессор, д.н. (профессор) Карпов А.В. (Кафедра радиофизики, Высшая школа киберфизических систем и прикладной электроники), Arkadi.Karpov@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-4	Способность к свободному владению профессионально-профилированными знаниями в области информационных технологий, использованию современных компьютерных сетей, программных продуктов и ресурсов Интернет для решения задач профессиональной деятельности, в том числе находящихся за пределами профильной подготовки
ПК-3	Способность применять на практике навыки составления и оформления научно-технической документации, научных отчетов, обзоров, докладов и статей (в соответствии с профилем подготовки)

Обучающийся, освоивший дисциплину (модуль):

Должен знать:

-место криптографии в задаче информационной безопасности и построения защищенных информационных систем ;

-основные понятия теории криптографии:

- криптографические протоколы электронной подписи;

- типичные слабости реализации криптографических систем;

-математические основы криптографии (неприводимые многочлены, теория чисел, псевдо-случайные последовательности,

Должен уметь:

- правильно выбирать тип шифра в соответствии с поставленной задачей ;

- качественно реализовать алгоритм шифрования;

- реализовывать атаку на классические шифры (исторические и современные) , в частности реализовать простейшие алгоритмы подбора паролей ;

Должен владеть:

Математическими методами криптографии

Должен демонстрировать способность и готовность:

Развитать современные физические методы криптографии

2. Место дисциплины (модуля) в структуре ОПОП ВО

Данная дисциплина (модуль) включена в раздел "Б1.В.02 Дисциплины (модули)" основной профессиональной образовательной программы 03.04.03 "Радиофизика (Информационные процессы и системы)" и относится к вариативной части.
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 - 28 часа(ов), в том числе лекции - 14 часа(ов), практические занятия - 14 часа(ов), лабораторные работы - 0 часа(ов), контроль самостоятельной работы - 0 часа(ов).

Самостоятельная работа - 44 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	Семестр	Виды и часы контактной работы, их трудоемкость (в часах)			Самостоятельная работа
			Лекции	Практические занятия	Лабораторные работы	
1.	Тема 1. Введение в информационную безопасность.	2	2	0	0	4
2.	Тема 2. Криптография с секретным ключом	2	4	4	0	16
3.	Тема 3. Криптография с открытым ключом. Электронная цифровая подпись	2	6	8	0	16
4.	Тема 4. Криптографические системы, основанные на использовании уникальных свойств физических каналов связи	2	2	2	0	8
	Итого		14	14	0	44

4.2 Содержание дисциплины (модуля)

Тема 1. Введение в информационную безопасность.

Введение в информационную безопасность. Предмет защиты. Угрозы безопасности. Причины искажения информации. Виды атак. Каналы доступа. Методы противодействия. (Методы защиты информации). Политика безопасности. История криптографии. Шифр сдвига. Шифр замены. Шифр Вернама. Шифр Виженера. Криптоанализ, основные виды криптоатак.

Тема 2. Криптография с секретным ключом

Вычислительно защищенная криптосистема. Абсолютно стойкая криптосистема. Теорема Шеннона об абсолютно стойкой криптосистеме. Теория вероятности и криптография. Симметричные шифры. Причины ненадежности криптосистем. Принцип Керкхоффа для криптосистемы. Поточные шифры. Генераторы псевдослучайных чисел. Важность подбора параметров. Слабости реализаций Распределение симметричных ключей. Статичный ключ. Эфемерный ключ. Разработка ПО шифра замены. Дешифрация шифротекста.

Тема 3. Криптография с открытым ключом. Электронная цифровая подпись

Односторонние функции. Примеры односторонних функций. Факторизация. Целочисленное извлечение квадратных корней. Дискретное логарифмирование. Алгоритм RSA. Криптосистема Эль-Гамаль. Криптосистема Рабина. Компрометация ключа. Реализация процедуры распределения ключей. Время жизни ключа. Разделение секрета. Энтропия. Неопределенность ключа. Расстояние единственности. Ложный ключ. Фиктивный ключ.

Программная реализация алгоритма RSA.

Тема 4. Криптографические системы, основанные на использовании уникальных свойств физических каналов связи

Криптографические системы, основанные на физических принципах защиты информации. Квантовая криптография, Криптографические системы основанные на свойствах многолучевого распространения радиоволн. Метеорная криптография. Разработка ПО шифратора на основе генератора псевдослучайных чисел, основанного на свойствах ?М-последовательности.

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 образования и науки Российской Федерации от 5 апреля 2017 года №301)

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)

Глоссарий по криптографии - https://hpc.name/text/get/82/p1.html

Сайт по криптографии - http://kek.ksu.ru/Student/Crypto/Main.htm

Электронные книги по криптографии - http://www.knigka.info/kr

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

Вид работ	Методические рекомендации
лекции	После каждой лекции студенту следует внимательно прочитать и разобрать конспект, при этом: - Понять и запомнить все новые определения. - Понять все математические выкладки и лежащие в их основе физические положения и допущения; воспроизвести все выкладки самостоятельно, не глядя в конспект. - Выполнить или доделать выкладки, которые лектор предписал сделать самостоятельно (если таковые имеются). - Если лектор предписал разобрать часть материала более подробно самостоятельно по доступным письменным или электронным источникам, то необходимо своевременно это сделать. - При возникновении каких-либо трудностей с пониманием материала рекомендуется попросить помощи у своих одногруппников или сокурсников. Также можно обратиться за помощью к лектору. Для этого можно лично подойти к преподавателю, либо написать ему электронное письмо, сформулировав в нём возникающие вопросы. К письму можно прикрепить какие-либо электронные материалы, связанные с возникшими вопросами, например, отсканированные или сфотографированные листочки с рукописными комментариями, пометками, выкладками и т.п.
практические занятия	При подготовке к практическим занятиям необходимо внимательно прочитать задание, предложенное преподавателем. Изучить список предлагаемых источников информации. Прочитать теоретический материал к занятию. Рекомендуется начинать выполнять задания с более легких упражнений. После выполнения в задания, нужно провести работу над ошибками.
самостоя-тельная работа	При подготовке к практическим занятиям необходимо внимательно прочитать задание, предложенное преподавателем. Изучить список предлагаемых источников информации. Прочитать теоретический материал к занятию. Рекомендуется начинать выполнять задания с более легких упражнений. После выполнения в задания, нужно провести работу над ошибками.
зачет	При подготовке к зачету следует ориентироваться на вопросы, имеющиеся в РПД и розданные преподавателем по данному курсу. Как правило, требуется ответить на один теоретический вопрос, решить две задачи и ответить на дополнительные вопросы преподавателя по курсу. Перед зачетом будет проведена консультация. При подготовке к зачету необходимо внимательно изучить требования преподавателя к подготовке к зачету. Рассмотреть список тем и заданий, выносимых на зачет. Изучить список предлагаемой литературы по подготовке к зачету. Повторить изученные темы. Сделать краткие конспекты тем, которые были упущены в течение семестра. Обратиться к преподавателю. если возникли затруднения при усвоении темы.

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.

Специализированная лаборатория.

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 03.04.03 "Радиофизика" и магистерской программе "Информационные процессы и системы".

Приложение 2
к рабочей программе дисциплины (модуля)
Б1.В.02 Основы информационной безопасности

Перечень литературы, необходимой для освоения дисциплины (модуля)

Направление подготовки: 03.04.03 - Радиофизика
Профиль подготовки: Информационные процессы и системы
Квалификация выпускника: магистр
Форма обучения: очное
Язык обучения: русский
Год начала обучения по образовательной программе: 2018

Основная литература:

1. Зашита информаци: учеб. пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 3-е изд. - М.: РИОР: ИНФРА-М, 2019. - 400 с. - (Высшее образование). - Режим доступа: http://znanium.com/catalog/product/1018901

2. Масленников М.Е. Практическая криптография: Пособие / Масленников М.Е. - СПб:БХВ-Петербург, 2015. - 465 с. - Режим доступа: http://znanium.com/catalog/product/94450

3. Введение в криптографию. Курс лекций / В.А. Романьков. - 2-е изд., испр. и доп. - М.: ФОРУМ: ИНФРА-М, 2019.- 240 с. - (Высшее образование: Бакалавриат). - Режим доступа: http://znanium.com/catalog/product/1018899

4. Теоретический минимум и алгоритмы цифровой подписи: Учебное пособие / Молдовян Н.А. - СПб:БХВ-Петербург, 2010. - 293 с. - Режим доступа: http://znanium.com/catalog/product/351283

Дополнительная литература:

1. Моделирование системы защиты информации. Практикум: учеб. пособие / Е.К. Баранова, А.В. Бабаш. - 2-е изд., перераб. и доп. - М.: РИОР: ИНФРА-М, 2018.- 224 с. + Доп. материалы [Электронный ресурс; Режим доступа http: //www.znanium.com]. - (Высшее образование: Бакалавриат). - DOI: https://doi.org/10.12737/18877 - Режим доступа: http://znanium.com/catalog/product/916068

2. Кнауб, Л. В. Теоретико-численные методы в криптографии [Электронный ресурс]: Учеб. пособие / Л. В. Кнауб, Е. А. Новиков, Ю. А. Шитов. - Красноярск: Сибирский федеральный университет, 2011. - 160 с. - Режим доступа: http://znanium.com/catalog/product/441493

Приложение 3
к рабочей программе дисциплины (модуля)
Б1.В.02 Основы информационной безопасности

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

Направление подготовки: 03.04.03 - Радиофизика
Профиль подготовки: Информационные процессы и системы
Квалификация выпускника: магистр
Форма обучения: очное
Язык обучения: русский
Год начала обучения по образовательной программе: 2018

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.