

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

Криптографические методы защиты информации

Направление подготовки: 10.03.01 - Информационная безопасность

Профиль подготовки: Безопасность автоматизированных систем

Квалификация выпускника: бакалавр

Форма обучения: очное

Язык обучения: русский

Год начала обучения по образовательной программе: 2016

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) 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-2	способностью применять соответствующий математический аппарат для решения профессиональных задач
ОПК-7	способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты
ПК-1	способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации
ПК-9	способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности

Обучающийся, освоивший дисциплину (модуль):

Должен знать:

- место криптографии в задаче информационной безопасности и построения защищенных информационных систем ;
- основные понятия теории криптографии:
- классические исторические шифры и методы атак на эти шифры, современные шифры - криптографические протоколы и электронную подпись;
- типичные слабости реализации криптографических систем (PGP, RC4, Windows и др.);
- теоретические основы "хорошего" шифра по Шеннону;
- теоретические основы "хорошей" криптосистемы (правила Кирхгоффа)

Должен уметь:

- правильно выбирать тип шифра в соответствии с поставленной задачей ;
- качественно реализовать алгоритм шифрования;
- реализовывать атаку на классические шифры (исторические и современные) , ;

Должен владеть:

- математические основы криптографии (неприводимые многочлены, теория чисел, псевдо-случайные последовательности,
- быстрые алгоритмы в дискретной математике) применительно к криптографии;

Должен демонстрировать способность и готовность:

Использовать криптографические методы при организации работ по защите информации. Реализовать современные криптографические подходы, основанные на использовании уникальных свойств физических каналов связи.

2. Место дисциплины (модуля) в структуре ОПОП ВО

Данная дисциплина (модуль) включена в раздел "Б1.Б.10 Дисциплины (модули)" основной профессиональной образовательной программы 10.03.01 "Информационная безопасность (Безопасность автоматизированных систем)" и относится к базовой (общепрофессиональной) части. 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 4 зачетных(ые) единиц(ы) на 144 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 - 19 часа(ов).

Контроль (зачёт / экзамен) - 45 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	Семестр	Виды и часы контактной работы, их трудоемкость (в часах)			Самостоятельная работа
			Лекции	Практические занятия	Лабораторные работы	
1.	Тема 1. Введение в криптографию.	8	6	8	0	4
2.	Тема 2. Симметричные криптосистемы.	8	12	10	0	8
3.	Тема 3. Криптографические системы с открытым ключом..	8	14	18	0	11
4.	Тема 4. Криптографические системы, основанные на физических механизмах защиты информации.	8	4	0	0	4
	Итого		36	36	0	27

4.2 Содержание дисциплины (модуля)

Тема 1. Введение в криптографию. .

Введение в криптографию

История криптографии.

Криптостойкость.

Теория вероятности и криптография.

Тема 2. Симметричные криптосистемы.

Симметричные шифры.

Поточные шифры.

Блочные шифры. Изучение криптосистемы DES.

Распределение симметричных ключей.

Разделение секрета.

Тема 3. Криптографические системы с открытым ключом..

Арифметика остатков.

Односторонние функции.

Алгоритм RSA.

Криптосистема Эль-Гамаль.

Криптосистема Рабина.

Схемы цифровой подписи: 1) RSA, 2) DSA,

Хэш-функция

Тема 4. Криптографические системы, основанные на физических механизмах защиты информации.

Криптографические системы, основанные на физических принципах защиты информации.

Квантовая криптография,

Метеорная криптография.

Криптографические системы основанные на свойствах многолучевого распространения радиоволн.

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

<http://radiosys.ksu.ru> - Карпов А.В. Введение в криптографию. 1. Симметричные криптосистемы (учебно-методическое пособие), (учебно-методическое пособие), <http://radiosys.ksu.ru/?p=415> 25с. 2009. ?

<http://radiosys.ksu.ru> - Карпов А.В., Туктарова И. Р., Смоляков А.Д., Имитационная компьютерная модель криптографической системы, основанная на генераторах М-последовательности <http://radiosys.ksu.ru/?p=963>

<http://radiosys.ksu.ru> - Карпов А.В., Любимов Д.В., Сулимов А.И. Введение в криптографию. Учебно-методическое пособие для выполнения лабораторных работ. Казань, 2013. 37 с. <http://radiosys.ksu.ru/?p=320>

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>

литература по криптографии - <http://www.proklondike.com/books/crypto.html>

сайт лаборатории радиосистем (кафедра радиофизики) - <http://radiosys.ksu.ru>

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

электронные книги по криптографии - <http://www.knigka.info/kriptograf/>

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

Основными видами самостоятельной работы являются:

- 1) предварительная подготовка к аудиторным занятиям. Такая подготовка предполагает изучение учебной программы, установление связи с ранее полученными знаниями, выделение наиболее значимых и актуальных проблем, на изучении которых следует обратить особое внимание и др.;
- 2) самостоятельная работа при осмыслении учебной информации, сообщаемой преподавателем, ее обобщение и краткая запись, а также своевременная доработка конспектов лекций;
- 3) подбор, изучение, анализ и при необходимости - конспектирование рекомендованных источников по учебным дисциплинам;
- 4) выяснение наиболее сложных, непонятных вопросов и их уточнение во время консультаций;
- 5) подготовка к контрольным занятиям, зачетам и экзаменам;
- 6) выполнение специальных учебных заданий, предусмотренных учебной программой;
- 7) написание рефератов, контрольных, квалификационных работ и их защита;

Все виды самостоятельной работы могут быть разделены на основные и дополнительные. Основные виды самостоятельной работы выполняются в обязательном порядке с последующим контролем результатов преподавателем, который проводит занятия. Дополнительные виды самостоятельной работы рекомендуются тем студентам, которые наиболее заинтересованы в изучении конкретной дисциплины и в последующем планируют поступление в аспирантуру.

Источниками для самостоятельного изучения выступают:

- учебники по предмету;
- курсы лекций по предмету;
- учебные пособия по отдельным темам
- научные статьи в периодической печати и рекомендованных сборниках;
- научные монографии.

Задания и задачи для самостоятельной работы преимущественно содержатся в учебно-методическом комплексе дисциплины (методических указаниях к семинарским занятиям). Кроме того, задания и задачи могут предлагаться преподавателями кафедры, ведущими семинарские занятия. На лекциях преподаватели также дают задания для самостоятельной работы.

Самостоятельная работа курируется преподавателем, ведущим эту учебную дисциплину. Часы оказания консультации преподавателями приведены в кафедральных расписаниях.

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 10.03.01 "Информационная безопасность" и профилю подготовки "Безопасность автоматизированных систем".

Приложение 2
к рабочей программе дисциплины (модуля)
Б1.Б.10 Криптографические методы защиты информации

Перечень литературы, необходимой для освоения дисциплины (модуля)

Направление подготовки: 10.03.01 - Информационная безопасность

Профиль подготовки: Безопасность автоматизированных систем

Квалификация выпускника: бакалавр

Форма обучения: очное

Язык обучения: русский

Год начала обучения по образовательной программе: 2016

Основная литература:

1. Жук А. П. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с.: <http://znanium.com/bookread.php?book=474838>
2. Практическая криптография: Пособие / Масленников М.Е. - СПб:БХВ-Петербург, 2015. - 465 с. ISBN 978-5-9775-1884-0 <http://znanium.com/bookread2.php?book=944503>
3. Введение в криптографию. Курс лекций / В.А. Романьков. ? 2-е изд., испр. и доп. ? М. : ФОРУМ : ИНФРА-М, 2017. ? 240 с. ? (Высшее образование). <http://znanium.com/bookread2.php?book=914480>
4. Молдовян Н. А. Молдовян Н.А. Теоретический минимум и алгоритмы цифровой подписи. - СПб.: БХВ-Петербург, 2010. - 293 с. - (Учебное пособие) <http://znanium.com/bookread.php?book=351283>

Дополнительная литература:

1. Баранова Е. К. Моделирование системы защиты информации: Практикум: Учебное пособие / Е.К.Баранова, А.В.Бабаш - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015 - 120 с. <http://znanium.com/bookread.php?book=476047>
2. Партыка Т. Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - 5-е изд., перераб. и доп. - М.: Форум: НИЦ ИНФРА-М, 2014. - 432 с. <http://znanium.com/bookread2.php?book=420047>
3. Кнауб Л. В. Новиков Е. А. Шитов Ю. А. Наименование: Теоретико-численные методы в криптографии Учебное пособие. ? Красноярск: СФУ, 2011. ? 161 с. ? ISBN 978-5-7638-2113-7. <http://znanium.com/bookread2.php?book=441493>.

Приложение 3
к рабочей программе дисциплины (модуля)
Б1.Б.10 Криптографические методы 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 автоматизированных систем

Квалификация выпускника: бакалавр

Форма обучения: очное

Язык обучения: русский

Год начала обучения по образовательной программе: 2016

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.