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
Проф. Д.А. Таюрский
_____ «___»_____20__г.

подписано электронно-цифровой подписью

Программа дисциплины

Основы криптоанализа

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: 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) ассистент, к.н. Разинков Е.В. (кафедра системного анализа и информационных технологий, отделение фундаментальной информатики и информационных технологий), Evgenij.Razinkov@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-3	способность администрировать подсистемы информационной безопасности объекта защиты
ПК-4	способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты
ПК-5	способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации
ПК-6	способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации

Обучающийся, освоивший дисциплину (модуль):

Должен знать:

Студент должен знать:

- Математические принципы, лежащие в основе асимметричных криптографических алгоритмов.
- Существующие атаки на асимметричные криптосистемы.
- Значения параметров криптосистемы RSA, приводящие к возможности проведения криптоаналитической атаки.

Должен уметь:

Студент должен уметь:

- Проводить анализ стойкости криптографического алгоритма RSA при заданных параметрах.
- Идентифицировать причины снижения криптостойкости RSA.

Должен владеть:

Студент должен владеть:

- Криптографической терминологией.

Должен демонстрировать способность и готовность:

Студент должен демонстрировать способность и готовность:

- Анализировать стойкость асимметричной криптосистемы RSA.
- Вырабатывать рекомендации по повышению стойкости криптосистемы RSA.

2. Место дисциплины (модуля) в структуре ОПОП ВО

Данная дисциплина (модуль) включена в раздел "Б1.В.ДВ.7 Дисциплины (модули)" основной профессиональной образовательной программы 10.03.01 "Информационная безопасность (Безопасность компьютерных систем)" и относится к дисциплинам по выбору.
Осваивается на 4 курсе в 7 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 - 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) - 36 часа(ов).

Форма промежуточного контроля дисциплины: экзамен в 7 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. Математические основы асимметричной криптографии.	7	4	0	2	6
2.	Тема 2. Криптосистема RSA.	7	4	0	2	8
3.	Тема 3. Криптоаналитические атаки на алгоритм RSA.	7	4	0	2	8
4.	Тема 4. Решетки.	7	6	0	2	8
5.	Тема 5. Криптоанализ RSA с использованием решеток.	7	6	0	2	8
6.	Тема 6. Тесты на простоту.	7	6	0	4	8
7.	Тема 7. Методы факторизации.	7	6	0	4	8
	Итого		36	0	18	54

4.2 Содержание дисциплины (модуля)

Тема 1. Математические основы асимметричной криптографии.

Расширенный алгоритм Евклида. Китайская теорема об остатках. Кольца и группы. Кольцо вычетов по модулю. Существование обратного элемента по умножению по модулю. Функция Эйлера. Мультипликативная группа кольца вычетов по модулю n. Теорема Эйлера. Малая теорема Ферма. Алгоритм быстрого возведения в степень.

Тема 2. Криптосистема RSA.

Симметричное и асимметричное шифрование. Преимущества асимметричного шифрования. Алгоритм RSA. Открытый и закрытый ключ RSA, использование открытого ключа для шифрования сообщения и закрытого для расшифрования. Генерирование модуля RSA, выбор шифрующей экспоненты, вычисление расшифровывающей экспоненты. Реализация шифрования и расшифрования RSA.

Тема 3. Криптоаналитические атаки на алгоритм RSA.

Криптоанализ асимметричных систем шифрования. Элементарные атаки на алгоритм асимметричного шифрования RSA: разделенный модуль, малая шифрующая экспонента. Атака Винера на RSA. Частичное раскрытие ключа при использовании малой шифрующей экспоненты. Условия успешного проведения атаки Боне-Дерфи. Границы Вегера.

Тема 4. Решетки.

Понятие решетки. Базис решетки. Получение другой матрицы базиса решетки. Ортогонализация Грама-Шмидта. LLL-приведенный базис решетки и его свойства. Алгоритм построения LLL-приведенного базиса решетки и его свойства.

Применение LLL-приведенного базиса решетки в криптоанализе асимметричных систем шифрования.

Тема 5. Криптоанализ RSA с использованием решеток.

Теорема Копперсмита. Атака на RSA с использованием LLL-приведенного базиса решетки: известна половина старших битов простого числа p или q. Формулировка теоремы Копперсмита для двух переменных. Атака на RSA: известна половина младших битов простых чисел p или q. Анализ применимости рассмотренных атак.

Тема 6. Тесты на простоту.

Проблема проверки числа на простоту. Приложения проверки числа на простоту: генерация простых чисел p и q для алгоритма асимметричного шифрования RSA. Тест Ферма. Преимущества и недостатки теста Ферма. Тест Миллера-Рабина. Преимущества и недостатки теста Миллера-Рабина. Способы повышения эффективности теста Миллера-Рабина.

Тема 7. Методы факторизации.

Факторизация числа - разложение составного числа на простые множители. Сложность факторизации больших чисел. Приложения факторизации больших чисел - криптоанализ симметричной криптосистемы RSA. Метод факторизации Ферма, границы его применимости, вычислительная сложность. (p–1)-метод Полларда. ρ-метод Полларда.

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)

Материалы онлайн-курсов Массачусетского Технологического Института - http://ocw.mit.edu/index.htm

Онлайн-курсы лучших университетов мира - https://www.coursera.org

Онлайн-курсы лучших университетов мира - https://www.edx.org

Онлайн-курсы лучших университетов мира - https://www.udacity.com

Онлайн-курсы Стенфордского Университета - http://online.stanford.edu

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

Вид работ	Методические рекомендации
лекции	Студенту рекомендуется внимательно слушать лектора, следить за тем, что написано на доске или представлено на слайдах презентации, анализировать получаемую им информацию. В случае, если материал лекции непонятен, следует задать вопрос в отведенное для вопросов время. Студенту также рекомендуется конспектировать материал лекции в тетради, что улучшает запоминание.
лабораторные работы	При выполнении лабораторных работ студенту рекомендуется внимательно анализировать поставленную задачу, уделяя особенное внимание критериям оценки точности решения задачи. Программный код должен быть объектно-ориентированным, чистым, с поясняющими комментариями. Особенное внимание следует уделить методологическим аспектам решения задачи, на корректное разделение выборки на обучающую, валидационную и тестовую. Результаты работы программы должны быть оформлены в виде таблиц и графиков.
самостоя-тельная работа	При ведении самостоятельной работы студенту рекомендуется внимательно подходить к изучению научных статей, обращать внимание на значимость полученного результата, на требования к обучающей выборке, на скорость работы предлагаемых алгоритмов, на результаты их сравнения с существующими. В случае, если изучаемый материал понятен не до конца, рекомендуется обращение к дополнительной литературе.
экзамен	Студенту рекомендуется внимательно анализировать вопросы в экзаменационном билете. Ответ на экзаменационный билет должен быть подробным и четким, все релевантные формулы должны быть приведены и пояснены. При ответе на вопрос студент должен проявить не столь умение запомнить материал, сколь глубокое его понимание. Рекомендуется избегать приведения в ответе материала, не относящегося к билету.

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 компьютерных систем".

Приложение 2
к рабочей программе дисциплины (модуля)
Б1.В.ДВ.7 Основы криптоанализа

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: 2016

Основная литература:

1. Кельберт, М.Я. Вероятность и статистика в примерах и задачах. Т.3: Теория информации и кодирования [Электронный ресурс] / М.Я. Кельберт, Ю.М. Сухов. - Электрон. Дан. - Москва : МЦНМО, 2016. - 567 с.- Режим доступа: https://e.lanbook.com/book/80125

2. Штарьков, Ю.М. Универсальное кодирование. Теория и алгоритмы [Электронный ресурс] : учебное пособие / Ю.М. Штарьков. - Электрон. Дан. - Москва : Физматлит, 2013. - 288 с. - Режим доступа: https://e.lanbook.com/book/59667.

3. Основы теории кодирования: Учебное пособие / Кудряшов Б.Д. - СПб:БХВ-Петербург, 2016. - 400 с. - Режим доступа: http://znanium.com/catalog/product/944069

4. Криптографическая защита информации: учеб. Пособие / С.О. Крамаров, О.Ю. Митясова, С.В. Соколов [и др.]; под ред. Проф. С.О. Крамарова. - М. : РИОР : ИНФРА-М, 2018. - 321 с. Режим доступа: http://znanium.com/catalog/product/901659

5. Введение в криптографию. Курс лекций / В.А. Романьков. - 2-е изд., испр. И доп. - М. : ФОРУМ : ИНФРА-М, 2018. - 240 с. - Режим доступа: http://znanium.com/catalog/product/924700

Дополнительная литература:

1.Сидельников, В. М. Теория кодирования [Электронный ресурс] / В. М. Сидельников. - М.: ФИЗМАТЛИТ, 2008. - 324 с. - Режим доступа:
http://znanium.com/bookread2.php?book=544713

2. Масленников М. Е. Практическая криптография: Пособие / Масленников М.Е. СПб:БХВ-Петербург, 2015. - 465 с. - Режим доступа:
http://znanium.com/bookread2.php?book=944503

3. 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. - Режим доступа: http://znanium.com/bookread2.php?book=474838

4. Каратунова, Н. Г. Защита информации. Курс лекций [Электронный ресурс] : Учебное пособие / Н. Г. Каратунова. - Краснодар: КСЭИ, 2014. - 188 с. - Режим доступа: http://znanium.com/bookread2.php?book=503511

5.Искусство защиты и взлома информации: Пособие / Скляров Д.В. - СПб:БХВ-Петербург, 2014. - 289 с. - Режим доступа: http://znanium.com/bookread2.php?book=940261

6. Чечёта, С.И. Введение в дискретную теорию информации и кодирования [Электронный ресурс] : учеб. Пособие - Электрон. Дан. - Москва : МЦНМО, 2011. - 224 с. - Режим доступа: https://e.lanbook.com/book/9437

Приложение 3
к рабочей программе дисциплины (модуля)
Б1.В.ДВ.7 Основы криптоанализа

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: 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.

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.