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 криптографического анализа

Направление подготовки: 10.04.01 - Информационная безопасность
Профиль подготовки: Математические методы и программные технологии защиты информации
Квалификация выпускника: магистр
Форма обучения: очное
Язык обучения: русский
Год начала обучения по образовательной программе: 2017

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) доцент, к.н. (доцент) Кугураков В.С. (кафедра теоретической кибернетики, отделение фундаментальной информатики и информационных технологий), Vladimir.Kugurakov@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-10	способность проводить аттестацию объектов информатизации по требованиям безопасности информации
ПК-14	способность организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России
ПК-16	способность разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности
ПК-2	способность разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности
ПК-3	способность проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов
ПК-4	способность разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности
ПК-5	способность анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества
ПК-6	способность осуществлять сбор, обработку, анализ и систематизацию научно-технической информации по теме исследования, выбор методов и средств решения задачи, разрабатывать планы и программы проведения научных исследований и технических разработок
ПК-8	способность обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи

Обучающийся, освоивший дисциплину (модуль):

Должен знать:

основные понятия криптологии;
- примеры секретных систем;
- алгебраическую структуру секретных систем;
- основные свойства чистых и смешанных шифров;
- понятия энтропии и ненадежности;
- понятия односторонней функции и функции с секретом;
- основные идеи криптосистем с открытым ключом

Должен уметь:

применять методы алгебры, теории вероятностей и теории чисел для описания и анализа криптосистем;
- применять методы криптоанализа для простейших шифров;

- использовать на практике простейшие криптографические протоколы

Должен владеть:

терминологией криптологии;

- методикой использования простейших методов криптоанализа.
- методикой использования простейших криптографических протоколов

Должен демонстрировать способность и готовность:

разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности

обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов

разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности

анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях станов-ления современного информационного общества

способность осуществлять сбор, обработку, анализ и система-тизацию научно-технической информации по теме исследова-ния, выбор методов и средств решения задачи, разрабатывать планы и программы проведения научных исследований и тех-нических разработок

обрабатывать результаты экспериментальных ис-следований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи

проводить аттестацию объектов информатизации по требованиям безопасности информации

организовать работу по созданию или модерни-зации систем, средств и технологий обеспечения информаци-онной безопасности в соответствии с правовыми нормативны-ми актами и нормативными методическими документами ФСБ России, ФСТЭК России

разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере про-фессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения ин-формационной безопасности

2. Место дисциплины (модуля) в структуре ОПОП ВО

Данная дисциплина (модуль) включена в раздел "Б1.В.ДВ.5 Дисциплины (модули)" основной профессиональной образовательной программы 10.04.01 "Информационная безопасность (Математические методы и программные технологии защиты информации)" и относится к дисциплинам по выбору.
Осваивается на 2 курсе в 3 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 - 0 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 3 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. Тема 1. Введение. Обзор современных направлений в криптографии и криптоанализе.	3	0	0	2	6

N	Разделы дисциплины / модуля	Семестр	Виды и часы контактной работы, их трудоемкость (в часах)			Самостоятельная работа
			Лекции	Практические занятия	Лабораторные работы	
2.	Тема 2. Тема 2. Булевы функции (б.ф.). Основные определения и теоремы. Алгебраическая нормальная форма б.ф. Линейные б.ф. Преобразование Уолша-Адамара. Аффинная эквивалентность б.ф. Представление б.ф. как функций над конечными полями. Классификация б.ф.	3	0	0	2	6
3.	Тема 3. Тема 3. Блочные шифры (б.ш.). Математическая модель б.ш. Б.ф. при конструировании б.ш. Сеть Фейстеля и SP-сеть. Стандарты шифрования. Примеры шифров: DES, ГОСТ 28147-89, AES, CAST и др.	3	0	0	2	6
4.	Тема 4. Тема 4. Поточные шифры (п.ш.). Математическая модель п.ш., принципы построения. Регистры сдвига с обратной связью. Линейные рекуррентные последовательности над полями Галуа. Определение их периода. Алгоритм Берлекэмпа-Месси. Нелинейные рекуррентные последовательности. Современные поточные шифры и методы их криптоанализа.	3	0	0	2	6
5.	Тема 5. Тема 5. Криптоанализ шифров. Статистические методы криптоанализа. Оценки свойств "лавинного эффекта". Проблема различения статистических гипотез. Надежность алгоритма как математическое ожидание вероятности его корректной работы. Линейный криптоанализ. Леммы Мацуи. Дифференциальный криптоанализ. Применение методов криптоанализа на конкретных шифрах.	3	0	0	4	12
6.	Тема 6. Тема 6. Булевы функции в криптографии. Математические задачи обеспечения высокой криптостойкости шифров.	3	0	0	2	6
7.	Тема 7. Тема 7. Хэш-функции. Принципы построения. Математические задачи, связанные с построением надёжных хэш-функций. Методы обнаружения коллизий. Хэш-функции MD5, SHA, ГОСТ Р 34.11-2013 и др. Применение хэш-функций.	3	0	0	2	6

N	Разделы дисциплины / модуля	Семестр	Виды и часы контактной работы, их трудоемкость (в часах)			Самостоятельная работа
			Лекции	Практические занятия	Лабораторные работы	
8.	Тема 8. Тема 8. Асимметричная криптография. Труднорешаемые задачи. Разновидности асимметричных криптосистем. Стандарт электронной подписи. Вопросы существования односторонних функций и псевдослучайных генераторов. Вероятностные тесты на простоту. Алгоритмы генерации простых чисел. Разложение числа на множители.	3	0	0	2	6
	Итого		0	0	18	54

4.2 Содержание дисциплины (модуля)

Тема 1. Тема 1. Введение. Обзор современных направлений в криптографии и криптоанализе.

ООбзор современных направлений в криптографии и криптоанализе.

Симметричная криптография.

Блочное и поточное шифрование.

Криптоанализ симметричных шифров.

Асимметричная криптография.

Разновидности асимметричных криптосистем.

Тема 2. Тема 2. Булевы функции (б.ф.). Основные определения и теоремы. Алгебраическая нормальная форма б.ф. Линейные б.ф. Преобразование Уолша-Адамара. Аффинная эквивалентность б.ф. Представление б.ф. как функций над конечными полями. Классификация б.ф.

Булевы функции.

Основные определения и теоремы.

Алгебраическая нормальная форма булевых функций.

Линейные булевы функции.

Преобразование Уолша-Адамара.

Аффинная эквивалентность булевых функций.

Представление булевых функций как функций над конечными полями. Классификация булевых функций.

Тема 3. Тема 3. Блочные шифры (б.ш.). Математическая модель б.ш. Б.ф. при конструировании б.ш. Сеть Фейстеля и SP-сеть. Стандарты шифрования. Примеры шифров: DES, ГОСТ 28147-89, AES, CAST и др.

Блочные шифры.

Математическая модель блочных шифров.

Сеть Фейстеля и SP-сети.

Стандарты шифрования.

Примеры шифров: DES, ГОСТ 28147-89, AES, CAST и др.

Тема 4. Тема 4. Поточные шифры (п.ш.). Математическая модель п.ш., принципы построения. Регистры сдвига с обратной связью. Линейные рекуррентные последовательности над полями Галуа. Определение их периода. Алгоритм Берлекэмпа-Месси. Нелинейные рекуррентные последовательности. Современные поточные шифры и методы их криптоанализа.

Поточные шифры.

Математическая модель поточных шифров. принципы построения. Регистры сдвига с обратной связью.

Линейные рекуррентные последовательности над полями Галуа. Определение их периода.

Алгоритм Берлекэмпа-Месси.

Нелинейные рекуррентные последовательности.

Современные поточные шифры и методы их криптоанализа.

Тема 5. Тема 5. Криптоанализ шифров. Статистические методы криптоанализа. Оценки свойств "лавинного эффекта". Проблема различения статистических гипотез. Надежность алгоритма как математическое ожидание вероятности его корректной работы. Линейный криптоанализ. Леммы Мацуи. Дифференциальный криптоанализ. Применение методов криптоанализа на конкретных шифрах.

Криптоанализ шифров.

Статистические методы криптоанализа.

Оценки свойств "лавинного эффекта".

Проблема различения статистических гипотез.

Надежность алгоритма как математическое ожидание вероятности его корректной работы.

Линейный криптоанализ.

Леммы Мацуи.

Дифференциальный криптоанализ.

Применение методов криптоанализа на конкретных шифрах.

Тема 6. Тема 6. Булевы функции в криптографии. Математические задачи обеспечения высокой криптостойкости шифров.

Булевы функции в криптографии.

Математические задачи обеспечения высокой криптостойкости шифров.

Анализ и построение стойких S-блоков.

Нелинейные булевы функции.

Бент-функции и их обобщения.

Гипербент-функции.

Бент-функции над конечными абелевыми группами.

Дифференциально равномерные булевы функции.

Корреляционная иммунность, устойчивость, алгебраическая иммунность булевых функций.

Связи между различными криптографическими характеристиками булевой функции.

Тема 7. Тема 7. Хэш-функции. Принципы построения. Математические задачи, связанные с построением надёжных хэш-функций. Методы обнаружения коллизий. Хэш-функции MD5, SHA, ГОСТ Р 34.11-2013 и др. Применение хэш-функций.

Хэш-функции. Принципы построения.

Математические задачи, связанные с построением надёжных хэш-функций.

Методы обнаружения коллизий.

Хэш-функции MD5, SHA, ГОСТ Р 34.11-2013 и др.

Применение хэш-функций.

Тема 8. Тема 8. Асимметричная криптография. Труднорешаемые задачи. Разновидности асимметричных криптосистем. Стандарт электронной подписи. Вопросы существования односторонних функций и псевдослучайных генераторов. Вероятностные тесты на простоту. Алгоритмы генерации простых чисел. Разложение числа на множители.

Асимметричная криптография.

Труднорешаемые задачи.

Разновидности асимметричных криптосистем.

Стандарт электронной подписи.

Вопросы существования односторонних функций и псевдослучайных генераторов.

Вероятностные тесты на простоту.

Алгоритмы генерации простых чисел.

Разложение числа на множители.

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)

М. Анохин, Блочные криптографические алгоритмы?. - Отличный краткий обзор современного состояния криптоанализа на русском языке. - http://www.cryptography.ru/db/msg.html?mid=1162999&uri=node4.html

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

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

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

Обучение происходит в форме лекционных и лабораторных занятий, а также самостоятельной работы студентов.

Изучение курса подразумевает овладение теоретическим материалом и получение практических навыков для более глубокого понимания разделов

дисциплины ″Основы криптографического анализа″ симметричных и асимметричных шифров на основе решения задач и упражнений, иллюстрирующих

доказываемые теоретические положения, а также развитие абстрактного мышления и способности самостоятельно доказывать частные утверждения.

Самостоятельная работа предполагает выполнение письменных домашних работ. Практические задания, выполняемые, как правило, вне аудитории,

предназначены для усвоения общих методов решения задач определенного типа. Работа заключается в самостоятельной проработка пройденных на занятиях тем. Закрепить навыки можно лишь в результате самостоятельной работы.

Следующий вид самостоятельной работы - написание компьютерных программ. Заключается в программной реализации заданных алгоритмов шифрования, хеширования и цифровой подписи.

Программа должна принимать входные данные и выдавать выходные. При написании программы необходимо досконально изучить алгоритм, можно просмотреть реализации на других языках.

И применить полученные знания при написании своего варианта приложения.

Заключительная часть самостоятельной работы - подготовка к зачету. При подготовке к сдаче зачета весь объем работы рекомендуется распределять равномерно

по дням, отведенным для подготовки к зачету, контролировать каждый день выполнения работы. При подготовки к зачёту нужно использовать конспекты лекций, литературу и источники из интернета, данные преподавателем. Лучше, если можно перевыполнить план. Тогда всегда будет резерв времени.

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 10.04.01 "Информационная безопасность" и магистерской программе "Математические методы и программные технологии защиты информации".

Приложение 2
к рабочей программе дисциплины (модуля)
Б1.В.ДВ.5 Основы криптографического анализа

Перечень литературы, необходимой для освоения дисциплины (модуля)

Направление подготовки: 10.04.01 - Информационная безопасность
Профиль подготовки: Математические методы и программные технологии защиты информации
Квалификация выпускника: магистр
Форма обучения: очное
Язык обучения: русский
Год начала обучения по образовательной программе: 2017

Основная литература:

1.Введение в криптографию. [Электронный ресурс] ? Электрон. дан. ? М.: МЦНМО, 2012. ? 348 с. ? Режим доступа: http://e.lanbook.com/book/71813

2. Червяков Н.И., Евдокимов А.А., Галушкин А.И. Применение искусственных нейронных сетей и системы остаточных классов в криптографии. - М.: Физматлит, 2012. URL: http://e.lanbook.com/books/element.php?pl1_id=5300.

3. Кнауб Л. В., Новиков Е. А., Шитов Ю. А. Теоретико-численные методы в криптографии [Электронный ресурс] : Учеб. пособие. - Красноярск : Сибирский федеральный университет, 2011. URL: http://znanium.com/bookread.php?book=441493.

4. Партыка Т.Л., Попов И И. Информационная безопасность: Учебное пособие. - М.: Форум: НИЦ ИНФРА-М, 2014. URL: http://znanium.com/bookread.php?book=420047.

Дополнительная литература:

1. Жук А.П., Жук Е.П., Лепешкин О.М., Тимошкин А.И. Защита информации: Учебное пособие. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - (Высшее образование: Бакалавриат; Магистратура). http://znanium.com/bookread2.php?book=474838

2. Каратунова Н. Г. Защита информации. Курс лекций [Электронный ресурс] : Учебное пособие / Н. Г. Каратунова. - Краснодар: КСЭИ, 2014. http://znanium.com/bookread.php?book=503511.

3.Марченков, С.С. Основы теории булевых функций. [Электронный ресурс] ? Электрон. дан. ? М. : Физматлит, 2014. ? 136 с. ? Режим доступа: http://e.lanbook.com/book/59714

Приложение 3
к рабочей программе дисциплины (модуля)
Б1.В.ДВ.5 Основы криптографического анализа

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

Направление подготовки: 10.04.01 - Информационная безопасность
Профиль подготовки: Математические методы и программные технологии защиты информации
Квалификация выпускника: магистр
Форма обучения: очное
Язык обучения: русский
Год начала обучения по образовательной программе: 2017

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.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе "Консультант студента", доступ к которой предоставлен обучающимся. Многопрофильный образовательный ресурс "Консультант студента" является электронной библиотечной системой (ЭБС), предоставляющей доступ через сеть Интернет к учебной литературе и дополнительным материалам, приобретенным на основании прямых договоров с правообладателями. Полностью соответствует требованиям федеральных государственных образовательных стандартов высшего образования к комплектованию библиотек, в том числе электронных, в части формирования фондов основной и дополнительной литературы.