**Правительство Российской Федерации**

**Федеральное государственное автономное образовательное учреждение высшего профессионального образования
"Национальный исследовательский университет
"Высшая школа экономики"**

Московский институт электроники и математики Национального

исследовательского университета "Высшая школа экономики"

Факультет Электроники и телекоммуникаций

**Программа дисциплины** «Интегрированные системы комплексной защиты информации в системах связи и средствах телекоммуникации и управления»

для направления 210100. «Электроника и наноэлектроника»

Авторы программы:

Захарова С.С. к.т.н. (szaharova@hse.ru)

Одобрена на заседании кафедры Радиоэлектроники и телекоммуникаций «\_\_»\_\_\_\_\_\_\_\_\_ 2014 г

Зав. кафедрой Увайсов С.У.

Рекомендована секцией УМС «Электроника» «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_ 2014 г

Председатель

Утверждена УС факультета Электроники и телекоммуникаций «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_2014 г.

Ученый секретарь \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Москва, 2014

*Настоящая программа не может быть использована другими подразделениями университета и другими вузами без разрешения кафедры-разработчика программы.*

Область применения и нормативные ссылки

Настоящая программа учебной дисциплины устанавливает минимальные требования к знаниям и умениям магистранта и определяет содержание и виды учебных занятий и отчетности.

Программа предназначена для преподавателей, ведущих данную дисциплину, учебных ассистентов и магистрантов, направления подготовки 210100.68 «Электроника и наноэлектроника», обучающихся по магистерской программе «Инжиниринг в электронике» (специализация «Радиоэлектронные средства космических аппаратов») изучающих дисциплину «Автоматизированные системы обеспечения надёжности и качества радиоэлектронных средств».

Программа разработана в соответствии с:

* Федеральным государственным образовательным стандартом высшего профессионального образования по направлению подготовки 210100 «Электроника и наноэлектроника» (квалификация (степень) «магистр»)
* Примерной основной образовательной программой по направлению подготовки 210100 «Электроника и наноэлектроника», (квалификация (степень) «магистр») Учебно-методического объединения в области радиотехники, электроники, биомедицинской техники и автоматизации
* Рабочим учебным планом университета по направлению подготовки 211000.68 «Электроника и наноэлектроника», магистерской программе «Инжиниринг в электронике», специализации «Радиоэлектронные средства космических аппаратов», утвержденным в 2013 г.

# Цели освоения дисциплины

Целями освоения дисциплины «Интегрированные системы комплексной защиты информации в системах связи и средствах телекоммуникации и управления» являются обучение магистрантов системному подходу к обеспечению защиты информации в комплексных системах связи и телекоммуникации.

# Компетенции обучающегося, формируемые в результате освоения дисциплины

В результате освоения дисциплины магистрант должен:

В результате освоения дисциплины студент должен:

Знать

* общие проблемы безопасности, роль и место информационной безопасности на современном этапе развития общества;
* основные методы инженерно-технической, программно-аппаратной и криптографической защиты информации;
* способы несанкционированного доступа к информации и средства инженерной защиты и технической охраны объектов

Уметь

* применять системный подход к обеспечению информационной безопасности систем связи и инфокоммуникационных систем;
* разрабатывать модели информационной безопасности телекоммуникационных систем, использовать стандартные методы инженерно-технической, программно-аппаратной и криптографической защиты информации;
* использовать типовые методы криптографического анализа;
* практически решать задачи защиты инженерно-технической, программно-аппаратной и криптографической защиты программ и данных;

Иметь навыки (приобрести опыт)

* анализа механизмов реализации методов защиты конкретных объектов и процессов для решения профессиональных задач;
* применения штатные средств защиты и специализированных продукты для решения типовых задач;
* квалифицированно оценивать область применения конкретных механизмов защиты;
* грамотно использовать аппаратные средства защиты при решении практических задач.

В результате освоения дисциплины магистрант осваивает следующие компетенции:

* Способен оценивать и модифицировать освоенные методы и способы профессиональной деятельности (СК-М1)
* Способен разрабатывать, апробировать и изобретать модели, способы, методы и инструменты профессиональной деятельности (СК-М2)
* Способен к самостоятельному освоению новых методов исследования, изменению научного и научно - производственного профиля своей деятельности и непрерывному повышению квалификации в течении всего периода профессиональной деятельности. (СК-М3)
* Способен анализировать, верифицировать, оценивать полноту информации в ходе профессиональной деятельности, при необходимости восполнять и синтезировать недостающую информацию и работать в условиях неопределенности (СК-М6)
* Способен определять, транслировать общие цели в профессиональной и социальной деятельности (ПК,1СЛК –М3)
* Способен создавать, описывать и ответственно контролировать выполнение технических и технологических требований и нормативов в профессиональной деятельности(ПК4,СЛК –М9)

# Место дисциплины в структуре образовательной программы

Настоящая дисциплина относится к профессиональному циклу дисциплин вариативной части, обеспечивающих профессиональную подготовку.

Для специализации «Радиоэлектронные средства космических аппаратов» магистерской программы «Инжиниринг в электронике» настоящая дисциплина является дисциплиной по выбору.

Изучение данной дисциплины базируется на дисциплинах базовых частей гуманитарного, социального и экономического цикла, математического и естественнонаучного цикла, а так же профессионального цикла дисциплин подготовки бакалавра по направлению 210100 «Электроника и наноэлектроника».

Для освоения учебной дисциплины магистранты должны владеть знаниями и компетенциями, предусмотренными Федеральным государственным образовательным стандартом высшего профессионального образования по направлению подготовки 210100 «Электроника и наноэлектроника» (квалификация (степень) «бакалавр»).

Основные положения дисциплины должны быть использованы в дальнейшем при изучении следующих дисциплин:

* Подготовка магистерской диссертации

# Тематический план учебной дисциплины

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № | Название раздела | Всего часов  | Аудиторные часы | Самостоятельная работа |
| Лекции | Семинары | Практические занятия |
| 1 | Функции и задачи защиты информации. Стратегии защиты информации | 18 | 4 |  | 4 | 10 |
| 2 | Основные направления инженерно-технической защиты информации  | 56 | 8 |  | 20 | 30 |
| 3 | Программно-аппаратная защита информации предмет и задачи программно-аппаратной защиты информации  | 50 | 8 |  | 14 | 30 |
| 4 | Криптографические методы защиты информации | 50 | 8 |  | 14 | 30 |

# Формы контроля знаний магистрантов

|  |  |  |  |
| --- | --- | --- | --- |
| Типконтроля | Формаконтроля | 1 год | Параметры |
| 2 | 3 | 4 |  |
| Текущий | Домашнеезадание | + | + | - | Решение задач по определению защищенности информации в инфокоммуникационных информационных системах |
| Лабораторные работы | + |  |  | Моделирование свойств криптографических систем ЗИ |
| Итоговый | Экзамен |  | + | + | Устные ответы на вопросы по материалам дисциплины в целом |

## Критерии оценки знаний, навыков

При текущем контроле используются следующие критерии:

* Посещение занятий
* Активность работы на аудиторных занятиях
* Своевременность выполнения домашних заданий
* Правильность выполнения домашних заданий
* Своевременность выполнения и защиты лабораторных работ

Оценки по всем формам текущего контроля выставляются по десятибалльной балльной шкале.

При итоговом контроле используются следующие критерии:

* Выполнение критериев оценки знаний на этапе промежуточного контроля
* Точность и полнота ответов на тестовые вопросы

Оценки по всем формам итогового контроля выставляются по десятибалльной шкале.

## Порядок формирования оценок по дисциплине

Преподаватель оценивает результаты практических работ, выполненных студетом по следующим позициям: правильность решения задач во время практических работ и качество выполненного по ним отчета. Оценки за эти работы преподаватель выставляет в рабочую ведомость. Накопленная оценка по 10-ти балльной шкале за работу на практических занятиях определяется перед итоговым контролем, каждого модуля – *Опр2, Опр3, Опр4,* соответственно*.*

Преподаватель оценивает правильность выполнения дополнительных задач и заданий (необязательных для решения всеми студентами, носящих нестандартный характер). Оценки за самостоятельную работу студента преподаватель выставляет в рабочую ведомость. Эти оценки могут только повысить накопленную оценку студентов или не изменить ее. Невыполнение дополнительных заданий и задач не может понизить оценку студентов за практические занятия.

Оценка за второй модуль является средней оценкой за лабораторные работы, проведенные в течении модуля.

Кроме того, в конце 3 модуля проводится устный зачет по практическим работам. Оценки за зачет *Опр3*

Накопленная оценка учитывает оценку за практические занятия, а также за аудиторную контрольную работу, коллоквиум и курсовую работу. Итоговые оценки формируется по следующему правилу:

За 2 модуль



за 3 модуль



за 4 модуль



накопленная оценка для итоговой аттестации



Результирующая оценка по 10-балльной шкале формируется как взвешенная сумма:



## где— оценка, полученная на экзамене

|  |  |
| --- | --- |
| Число баллов до округления | Округленная оценка |
| 0 | 0 |
| 0,1 – 1,4 | 1 |
| 1,5 – 2,4 | 2 |
| 2,5 – 3,9 | 3 |
| 4 – 4,4 | 4 |
| 4,5 – 5,4 | 5 |
| 5,5 – 6,4 | 6 |
| 6,5 – 7,4 | 7 |
| 7,5 – 8,4 | 8 |
| 8,5 – 9,4 | 9 |
| 9,5 – 10 | 10 |

# Содержание дисциплины

**Лекция 1. Информационная безопасность автоматизированных систем**

Общие положения. Информация как продукт. Информационные услуги. Источники конфиденциальной информации в информационных системах. Неправомерное овладение конфиденциальной информацией в информационных системах. Виды технических средств информационных систем.

Современная постановка задачи защиты информации. Организационно-правовое обеспечение информационной безопасности. Информация как объект юридической защиты. Основные принципы засекречивания информации. Государственная система правового обеспечения защиты информации в РФ.

**Лекция 2. Классификация и анализ угроз информационной безопасности.**

Классы каналов несанкционированного получения информации. Причины нарушения целостности информации. Виды угроз информационным системам. Виды потерь. Модель нарушителя информационных систем. Эмпирический подход к оценке уязвимости информации.

Система с полным перекрытием. Практическая реализация модели «угроза - защита».

Рекомендации по использованию моделей оценки уязвимости информации, позволяющих определить текущие и прогнозировать будущие значения всех показателей уязвимости информации для любых компонентов автоматизированной системы обработки данных, любой их комбинации и для любых условий жизнедеятельности автоматизированной системы обработки данных.

**Лекция 3. Методы и методики защиты информации**

Требования к защите информации, обусловленные спецификой автоматизированной обработки информации. Требования, связанные с размещением защищаемой информации. Требования, определяемые структурой автоматизированной системы. Требования, обусловленные видом защищаемой информации.

Требования к безопасности информационных систем в США. Требования к безопасности информационных систем в России. Анализ существующих методик определения требований к защите информации. Классы защищенности средств вычислительной техники от несанкционированного доступа. Оценка состояния безопасности ИС. Факторы, влияющие на требуемый уровень защиты информации. Критерии оценки безопасности информационных технологий.

**Лекция 4, 5.Основные направления. Инженерно - технической защиты информации**. Проблемы Информационной войны. Система защиты информации основные положения.Теории защиты информации. Общая характеристика радиоэлектронной разведки. Демаскирующие признаки объектов наблюдения и сигналов.пособы и средства инженерной защиты и технической охраны объектов. Скрытие объектов наблюдения. Энергетическое скрытие Акустических информативных сигналов. Способы Несанкционированного доступа к информации. Обнаружение и локализация закладных устройств, Подавление их сигналов. Обеспечение безопасности данных в сетях ЭВМ. Щиты информации. Обнаружение и локализация закладных устройств,подавление их сигналов. Противодействие утечке компьютерной И аудио видео информации. Мероприятия по защите коммерческой тайны. О государственном лицензировании деятельности в области защиты информации

**Лекция 6. Функции и задачи защиты информации. Стратегии защиты информации**

Общие положения. Методы формирования функций защиты. Классы задач защиты информации. Функции защиты. Состояния и функции системы защиты информации.

Организация защиты информации. Уровень структурно-организационного построения объекта обработки информации. Уровень технологических схем обработки. Виды стратегии защиты информации.

**Лекция 7 Программно-аппаратная защиты информации**

предмет и задачи программно-аппаратной защиты информации;основные понятия

уязвимость компьютерных систем; политика безопасности в компьютерных системах; оценка защищенности; механизмы защиты.

**Лекция 8**. Идентификация пользователей кс-субъектов доступа к данным

Основные понятия и концепции; Идентификация и аутентификация пользователя; Взаимная проверка подлинности пользователей; Протоколы идентификации с нулевой передачей знаний ; схема идентификации гиллоу-куискуотера.

**Лекция** 9. Средства и методы ограничения доступа к файлам

защита информации в кс от несанкционированного доступа

Система разграничения доступа к информации в кс

Концепция построения систем разграничения доступа

Организация доступа к ресурсам кс

обеспечение целостности и доступности информации в кс

**Лекция** 10. **Аппаратно-программные средства криптографической защиты информации**

полностью контролируемые компьютерные системы

Основные элементы и средства защиты от несанкционированного доступа

Системы защиты информации от несанкционированного доступа

Комплекс криптон-замок для ограничения доступа к компьютеру4.5 система защиты данных crypton sigma

**Лекция 11. Методы и средства ограничения доступа к компонентам эвм Защита программ от несанкционированного копирования**

защита информации в пэвм

защита информации, обрабатываемой пэвм и лвс, от утечки по сети электропитания

виды мероприятий по защите информации

современные системы защиты пэвм от несанкционированного доступа к информации5.5 контрольные вопросы

методы, затрудняющие считывание скопированной информации

методы, препятствующие использованию скопированной информации 6.3 основные функции средств защиты от копирования

основные методы защиты от копирования

методы противодействия динамическим способам снятия защиты программ от копирования

**Лекция** 12.. **Управление криптографическими ключами**

генерация ключей; хранение ключей; распределение ключей; протокол аутентификации и распределения ключей для симметричных криптосистем ; протокол для асимметричных криптосистем с использованием сертификатов открытых ключей

**Лекция 13. Криптографические методы защиты информации**

Важные моменты в истории развития теории защиты информации. «Наивная» криптография:

шифр Цезаря, шифр Пиблса; Формальная криптография: шифр Вижинера, роторные криптосистемы; математическая криптография: доказуемо криптостойкие системы; компьютерная криптография: криптосистемы с открытым ключом, автоматизированный криптоанализ.

Требования к криптосистемам. Основные алгоритмы шифрования. Цифровые подписи. Криптографические хеш-функции. Криптографические генераторы случайных чисел. Обеспечиваемая шифром степень защиты. Криптоанализ и атаки на криптосистемы.

**Лекция 14. Защита программных средств от исследования**

классификация средств исследования программ

методы защиты программ от исследования

общая характеристика и классификация компьютерных вирусов

общая характеристика средств нейтрализации компьютерных вирусов

классификация методов защиты от компьютерных вирусов

**Практические занятия**

1 Криптография с открытым ключом

Модель передачи сообщения в криптосистеме с открытым ключом. Основы теории чисел: функция Эйлера, обобщенный алгоритм Евклида, быстрый алгоритм возведения в степень справа налево и слева направо. Понятие односторонней функции. Примеры односторонних функций. Система защищенной передачи ключей Диффи и Хеллмана. Шифр Шамира. Шифр Эль-Гамаля. Шифр RSA. Электронная подпись на базе RSA.

2 Криптографические протоколы

Понятие криптографического протокола. Протокол «Ментальный покер». Протокол «Доказательство с нулевым знанием»: задача о раскраске, задача о гамильтоновом цикле. Электронные деньги. Задача о взаимной верификации.

3 Шифры с секретным ключом

Первый шифр с секретным ключом: шифр Цезаря. Понятие блокового шифра. Шифр ГОСТ 28147-89. Шифр RC-5. Шифр RC-6. Шифр AES (Rijndael). Режимы функционирования блоковых шифров: режим электронной кодовой книги (ECB), режим цепных блоков (CBC).

Понятие идеального шифра. Первый идеальный шифр – шифр Вернама.

Потоковые шифры. Генераторы псеводослучайных чисел. Режим OFB блокового шифра. Режим CTR блокового шифра. Шифр RC-4. Криптографические хеш-функции. Понятие хеш-функции. Требования к криптографическим хеш-функциям. Примеры криптографических хеш-функций.

4 Криптосистемы на эллиптическ их кривых.

Краткая информация об эллиптических кривых. Математические основы теории эллиптических кривых. Общий вид уравнения эллиптической кривой. Свойства эллиптических кривых. Арифметические операции на эллиптических кривых. Оценки количества точек на эллиптической кривой. Построение криптосистем на основе арифметики на эллиптических кривых.

5 Случайные числа в криптографии.

Физические генераторы случайных чисел. Генераторы псевдослучайных чисел: конгруэнтные генераторы, сдвиговые регистры, сдвиговый регистр с линейной обратной связью, сдвиговые регистры с нелинейной обратной связью.

6 Основы криптоанализа. Стеганография

Цели и задачи криптоанализа. Криптографическая устойчивость информационных систем. Линейный криптоанализ. Дифференциальный криптоанализ. Градиентная статистическая атака, принципы анализа криптографических систем; История стеганографии. Задачи стеганографии. Модель передачи скрытых сообщений. Первые стеганографические системы. Современная стеганография. Защита авторского права. Цифровые водяные знаки. Цифровые отпечатки пальцев. Обнаружение факта передачи скрытого сообщения. Понятие идеальной стеганографической системы.

7 Сжимающее кодирование

Основные определения теории сжимающего кодирования. Сжимающие коды: Код Фано, Код Хаффмана, Код Шенона, Адаптивный код Хаффмана, Арифметический код, Стопка книг, Код LZ77, Код LZ78.

8 Теория кодирования

Задачи теории кодирования. Примеры ошибок при передаче сообщений. Модель передачи

данных в зашумленном канале. Типы ошибок в канале связи. Основные определения теории

кодирования. Основные понятия теории групп. Группа автоморфизмов. Расстояние Хэмминга. Вес Хэмминга.

9 Линейные коды.

Проверочная и порождающая матрицы. Связь проверочной и порождающей матрицы. Границы объемов кодов: граница Хэмминга, граница Синглтона. Циклические коды. Теорема о столбцах проверочной матрицы. Код Хэмминга и его свойства. Примеры кода Хэмминга. Декодирование кода Хэмминга. Теорема Шеннона

В рамках практических работ запланировано для приобретения навыков разработки программных систем, реализующих рассматриваемые в течение курса алгоритмы по темам:

1) Криптография с открытым ключом.

2) Криптографические протоколы.

3) Шифры с секретным ключом.

4) Криптосистемы на эллиптических кривых.

5) Случайные числа в криптографии.

6) Сжимающее кодирование.

**5. Образовательные**

# Образовательные технологии

Помимо традиционных образовательных технологий будут использоваться следующие активные методы обучения: проблемные лекции, лекции-беседы и дискуссии, лабораторные работы в виде имитационного неигрового занятия, будут применяться следующие приемы: “мозговой штурм”, “анализ практических ситуаций”.

# Оценочные средства для текущего контроля и аттестации студента

Контроль качества подготовки осуществляется путем проверки

теоретических знаний и практических навыков путем

1) зачета в конце семестра.

2) проверки и приема текущих практических работ.

3) проверки и приема домашних заданий.

Практические работы направлены на самостоятельную работу по созданию криптографических алгоритмов и программ.

Практические работы должны выполняться на любом современном языке программирования.

Результатом выполнения практической работы должна являться работающая программа, реализующая требуемый алгоритм шифрования или же криптографический протокол.

Программа может быть реализована как в виде консольного приложения, так и с использованием графического интерфейса. Параметры работы алгоритма должны передаваться в командной строке (в случае консольного приложения), или же вводиться вручную (в случае использования графического интерфейса).

Каждое задание выполняется группой, состоящей из 3-4 студентов в течение одного занятия.

# Оценочные средства для текущего контроля и аттестации магистранта

## Тематика заданий текущего контроля

# Учебно-методическое и информационное обеспечение дисциплины

## Базовые учебники

## Основная литература

1. Герасименко В.А., Малюк А.А. Основы защиты информации. М.:

МОПО РФ, МИФИ, 1997, 537 с.

2. Петраков А.В. Утечка и защита информации в телефонных каналах.

М.: Энергоатомиздат. 1996. 320 с.

3. Демин В.П., Куприянов А.И., Сахаров А.В. Радиоэлектронная

разведка и радиомаскировка. М.: Изд-во МАИ, 1997, 156 с.

4. Поздняков Е.Н. Защита объектов. – М.: Концерн “Банковский

Деловой Центр”, 1997 г. – 224 с.

5. Лагутин В.С., Петраков А.В. Утечка и защита информации в

телефонных каналах. – М.: Энергоатомиздат, 1996 г. – 304 с.

6. Торокин А.А. Основы инженерно-технической защиты информации.

М: “Ось-89”, 1998, 334 с.

7. Хорев А.А. Защита информации от утечки по техническим каналам.

Часть 1. Технические каналы утечки информации. Учебное пособие.

М.: Гостехкомиссия России, 1998, 320 с.

8. Петраков А.В., Дорошенко П.С., Савлуков Н.В. Охрана и защита

современного предприятия. М: Энергоатомиздат, 1999, 568 с.

9. Каторин Ю.Ф. и др. Большая энциклопедия промышленного

шпионажа. – СПб.: ООО “Изд-во “Полигон”, 2000. – 896 с.

10. Домашев А.В., Грунтович М.М., Попов В.О. Программирование

алгоритмов защиты информации. – М.: Издательство “Нолидж”,

2002.

11. Соколов А.В., Шаньгин В.Ф. Защита информации в распределенных

корпоративных сетях и системах. – М.: ДМК Пресс, 2002.

12. Вильям Столлингс Криптографическая защита сетей. – М.:

Издательсткий дом “Вильямс”, 2001.

## Дополнительная литература

## Справочники, словари, энциклопедии

# Материально-техническое обеспечение дисциплины

Лекционные занятия проходят в мультимедийной аудитории, оснащенной компьютером и проектором. Каждая лекция сопровождается презентацией, содержащей краткий теоретический материал и иллюстративный материал.

Каждая презентация построена по следующему шаблону: название лекционного занятия, краткое содержание предыдущей, теоретический материал, примеры.

Практические занятия проходят в компьютерном классе.