МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВАСТОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Институт радиоэлектроники и информационной безопасности

«ЗАЩИТА ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ И ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ»

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

к изучению дисциплины
и выполнению контрольной работы
для студентов заочной формы обучения
специальности 11.05.01 «Радиоэлектронные системы и комплексы»

УДК 681.3.81
004.056

Рецензент:
профессор, д-р. техн. наук. **Афонин И. Л.**

Составитель: И.В. Лащенко

«Защита информации в информационно-телекоммуникационных системах»: методические рекомендации к изучению дисциплины и выполнению контрольной работы для студентов заочной формы обучения специальности 11.05.01 «Радиоэлектронные системы и комплексы» / СевГУ; сост. И.В. Лащенко. — Севастополь: Изд-во СевГУ, 2017. — 8 с.

Целью методических рекомендаций является оказание помощи студентам заочной формы обучения при самостоятельном изучении дисциплины «Защита информации в информационных и телекоммуникационных системах», а также при выполнении и оформлении контрольной работы. Изложен перечень основных тем дисциплины.

УДК 681.3.81
004.056

Методические рекомендации утверждены на заседании кафедры «Радиоэлектроника и телекоммуникации» 26 января 2017 года, протокол № 7.

Методические рекомендации рассмотрены и рекомендованы к изданию на заседании методической комиссии института радиоэлектроники и информационной безопасности 01 февраля 2017 года, протокол № 6.

Ответственный за выпуск: д-р техн. наук, профессор, заведующий кафедрой «Радиоэлектроника и телекоммуникации» **Афонин И. Л.**

Издательский номер 07/17

1. Цели и задачи освоения дисциплины

Целью преподавания дисциплины «Защита информации в информационных и телекоммуникационных системах» (ЗИвИТС) является формирование представления о современных методах и средствах защиты информации в информационных и телекоммуникационных системах. Приобретение знаний, умений и навыков.

Задачей преподавания дисциплины ЗИвИТС является формирование у студентов навыков и умений для правильного выбора и применения средств криптографической и технической защиты информации, предотвращения несанкционированного доступа, модификации либо блокирования информации в информационных и телекоммуникационных системах.

2. Формируемые компетенции: ОПК-1

Общекультурные компетенции (ОК):

— способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

3. Место дисциплины в структуре образовательной программы

Дисциплина ЗИвИТС относится к дисциплинам по выбору 7 вариативной части профессионального цикла основной образовательной программы подготовки по специальности 11.05.01 — Радиоэлектронные системы и комплексы.

Освоение данной дисциплины требует знания материалов предшествующих дисциплин: «Математика. Математический анализ», «Физика», «Радиотехнические цепи и сигналы», «Основы теории передачи информации», «Основы сетевых информационных технологий», «Технологии защиты информации в радиоэлектронных системах», «Телекоммуникационные технологии», «Телекоммуникационные сети с радиодоступом».

Знания, полученные при освоении данной дисциплины необходимы для выполнения выпускной квалификационной работы.

4. Содержание дисциплины

Тема 1. Основные направления государственной политики в области обеспечения информационной безопасности

Методология оценивания безопасности информационных технологий. Развитие стандартов безопасности. Государственная политика Российской Федерации в области обеспечения безопасности, в том числе

информационных и телекоммуникационных систем. Оценка защищенности критических инфраструктур.
Доктрина информационной безопасности Российской Федерации

Тема 2. Методы и средства криптографической защиты информации

Методы криптографической защиты информации.
Классификация криптографических и стеганографических методов защиты информации. Симметричное и несимметричное шифрование.
Блочное шифрование. Стандарты шифрования данных.
Сеть Фейстеля. Подстановочно-перестановочная сеть.
Шифры DES, AES. Шифр ГОСТ 28147-89. ГОСТ Р 34.12-2015.
Поточные шифры. Гаммирование.
Генераторы псевдослучайных чисел.
Асимметричная криптография.
Электронная цифровая подпись.
Хэш-функция.
Телекоммуникационные протоколы, использующие сеансовые ключи. Использование криптографических алгоритмов в радиоэлектронных средствах обеспечения безопасности.

Тема 3. Защита информации в каналах связи

Криптографические методы закрытия информации в каналах связи.
Защита информации в проводных каналах. Классификация систем закрытия речевых сигналов.
Защита информации в беспроводных каналах связи.
Безопасность беспроводных сетей: стандарт IEEE 802.11.
Обеспечение безопасности передачи информации в телекоммуникационных системах стандарта GSM. Алгоритмы аутентификации A3 и генерации ключа A8. Хеш-функция COMP128. Шифрование поточным шифром A5. Защита информации в телекоммуникационных системах стандартов UMTS и CDMA2000.

Тема 4. Обеспечение компьютерной безопасности

Защита информации на уровне операционной системы.
Риски информационной безопасности.
Типы уязвимостей систем и причины их появления.
Вредоносное программное обеспечение.
Особенности защиты в операционной системе Windows. Принципы организации системы разграничения доступа. Защита конфиденциальной информации.
Удостоверение подлинности. Формальный анализ протоколов проверки подлинности и обмена ключами.
Протоколы аутентификации.
Защита информации в распределенных системах. Угрозы безопасности информации в сетях. Безопасность сетевых протоколов интернета. Обеспечение безопасности прикладных служб интернета.

Средства обеспечения безопасности: противодействие подслушиванию трафика, сегментация сети, резервирование сетевого оборудования и каналов связи.
Технологии защиты облаков.
Межсетевые экраны. Возможности персональных брандмауэров.
Организация виртуальных частных сетей. Задачи, решаемые VPN.
Стандарт ISO/IEC 27002 «Практические правила управления безопасностью информации».

Тема 5. Эффективность систем безопасности

Стандарт ISO/IEC 15408 "Критерии оценки безопасности информационных технологий".
Политика безопасности.
Аудит. Методы оценки и повышения эффективности систем безопасности информационных и телекоммуникационных систем.

5. Содержание и распределение времени самостоятельной работы студентов

Общий объем дисциплины 108 часов.

Самостоятельная работа по дисциплине ЗИвИТС для ЗФО включает: подготовку к лабораторным занятиям, выполнение домашней контрольной работы (домашней контрольной работы) и подготовку к зачету.

Таблица 5.1 — Распределение СРС студента ЗФО

Вид работ	Объем, ч
Изучение теоретического материала	36
Подготовка к лабораторным и практическим занятиям	12
Выполнение индивидуального задания (ДКР)	10
Подготовка к промежуточной аттестации по дисциплине (зачет)	36
Всего	94

Кроме того, самостоятельная работа студентов по изучению отдельных тем дисциплины включает поиск и систематизацию учебных материалов по дисциплине, переработку и освоение материала, самоконтроль знаний по данной теме, проектную деятельность в рамках студенческой научно-исследовательской работы.

6. Контрольная работа и методические рекомендации по ее выполнению

Контрольная работа для студентов ЗФО выполняется в 11 семестре и состоит из трех заданий, соответствующих содержанию дисциплины. Объем контрольной работы 10…16 страниц.

Номер варианта выбирается в соответствии с последними цифрами номера зачетной книжки.

Требования к оформлению работы представлены в [1].

Задание 1.

Изложить основные направления государственной политики Российской Федерации в области обеспечения информационной безопасности.

Рекомендации:

Изучить Доктрину информационной безопасности Российской Федерации [12].

Указать действующие Федеральные Законы и основные стандарты информационной безопасности.

После изучения соответствующего раздела в [2, 6, 9] уточните актуальность нормативной базы, используя ресурс «Энциклопедия по информационной безопасности» http://wikisec.ru/MediaWiki/index.php .

Задание 2.

Описать указанные криптографические методы защиты информации.

Таблица 6.1 — Варианты к заданию 2

Последняя цифра зачетной книжки	Содержание задания
1	Асимметричная криптография. Метод RSA. Эллиптическая криптография
2	Стандарты шифрования данных. Шифры DES, AES
3	Стандарты шифрования данных. Шифр ГОСТ 28147-89. ГОСТ Р 34.12-2015
4	Асимметричная криптография. Процессы формирования и проверки электронной цифровой подписи
5	Асимметричная криптография. Метод RSA. Эллиптическая криптография
6	Стандарты шифрования данных. Шифр ГОСТ 28147-89. ГОСТ Р 34.12-2015
7	Стандарты шифрования данных. Шифры DES, AES
8	Асимметричная криптография. Процессы формирования и проверки электронной цифровой подписи
9	Стандарты шифрования данных. Шифр ГОСТ 28147-89. ГОСТ Р 34.12-2015
0	Асимметричная криптография. Метод RSA. Эллиптическая криптография

Рекомендации:

Привести примеры использования криптографических алгоритмов в радиоэлектронных средствах обеспечения безопасности, в каналах связи, в информационно-телекоммуникационных системах [10].

Задание 3.

Описать методы обеспечения компьютерной безопасности для раздела, соответствующего номеру варианта.

Таблица 6.2 — Варианты к заданию 3

Последняя цифра зачетной книжки	**Содержание задания**
1	Принципы организации системы разграничения доступа.
2	Протоколы аутентификации
3	Угрозы безопасности информации в сетях.
4	Защита информации на уровне операционной системы.
5	Организация VPN.
6	Межсетевые экраны.
7	Антивирусная защита
8	Защита информации в распределенных системах.
9	Типы уязвимостей систем и причины их появления.
0	Аудит систем безопасности

Рекомендации:

После изучения общих принципов защиты информации для соответствующего раздела в [3, 5, 6, 7] найдите и опишите примеры применения этих средств обеспечения безопасности, используя, например, [11].

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Оформление текстовых работ: методические указания / СевГУ; сост. В. Г. Слёзкин, П. П. Ермолов. — Севастополь: Изд-во СевГУ, 2015. — 19 с.
2. Стрельцов, А.А. Организационно-правовое обеспечение информационной безопасности / А.А.Стрельцов, В.С.Горбатов, Т.А. Полякова.— М.: Академия, 2008.
3. Гайворонский, М.В. Безопасность информационно-коммуникационных систем / М.В.Гайворонский, О.М.Новиков. — К.: BHV, 2009. — 608с.
4. Куприянов, А. И. Основы защиты информации: учеб. пособие для студ. вузов, обуч. по спец. "Радиоэлектронные системы", "Средства радиоэлектронной борьбы","Информационные системы и технологии" / А. И. Куприянов, А. В. Сахаров, В. А. Шевцов. —М. : ACADEMIA, 2006. — 256 с.
5. Васильков, А. В. Информационные системы и их безопасность: учеб. пособие / А. В. Васильков, А. А. Васильков, И. А. Васильков. — М. : Форум, 2010. — 528 с.
6. Шаньгин, В. Ф. Защита компьютерной информации: эффективные методы и средства.— М.: ДМК Пресс, 2010. (рус.)
7. Защита информации в телекоммуникационных системах / Г. Ф. Коханович, В. П. Климчук, С. М. Паук, В. Г. Потапов. — К. : МК - Пресс, 2005. — 288 с. (рус.)
8. Хорошко, В. А. Методы и средства защиты информации/ В. А. Хорошко, А. А. Чекатков; Под ред. Ю. С. Ковтанюк. — К.: ЮНИОР, 2003. — 505 с
9. Щербаков, А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты .— М.: Книжный мир, 2009.— 352 с.
10. Ветров, Ю.В. Криптографические методы защиты информации в телекоммуникационных системах / Ю.В. Ветров, С.Б.Макаров. — СПб.: Издательство политехн. ун-та, 2011. — 174 с.
11. Информационно-методический журнал «Защита информации. Инсайд» [Электронный ресурс]. — http://www.inside-zi.ru
12. Указ Президента РФ от 5 декабря 2016 г. № 646 “Об утверждении Доктрины информационной безопасности Российской Федерации [Электронный ресурс]. — http://www.garant.ru/products/ipo/prime/doc/71456224/#ixzz4WpzcSJmS