МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ЮЖНО-РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ (НПИ) ИМЕНИ М.И. ПЛАТОВА»

УТВЕРЖДАЮ:
Проректор по ОД ЮРГПУ(НПИ)
_____ Е.М. Дьяконов
«__» _____ 2017 г.

РАБОЧАЯ ПРОГРАММА

ФТД.2 «Защита информации в системах беспроводной связи»
10.04.01 «Информационная безопасность»
направленность «Комплексная защита объектов информатизации»

Военный институт
Кафедра Информационная безопасность
Курс 2
Семестр 3

программа магистратуры
набор 2016 г.

ИТОГО по дисциплине 2 /72 (ЗЕ / ч.)
(с учетом ЗЕ/часов на экзамен)

2017 г.

Рабочая программа составлена на основании рабочего учебного плана, утвержденного Ученым советом ЮРГПУ (НПИ) протоколом №6 от 26.01.2017 г.

Рабочую программу составил доцент, доцент кафедры ИБ Максимов А.С.
ученое звание, степень, должность, фамилия, инициалы

Рабочая программа обсуждена на заседании кафедры ИБ
наименование кафедры

утверждена 02.03.2017 г. Протокол №9

Заведующий кафедрой ИБ Баранов В.В. /
(подпись, фамилия, инициалы)

СОДЕРЖАНИЕ

1. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Защита информации в системах беспроводной связи» относится к дисциплинам вариативной части блока ФТД рабочего учебного плана.

Логические и содержательно-методические взаимосвязи дисциплины с другими частями ОП (дисциплинами (модулями), практиками):

- связь с предыдущими дисциплинами (модулями), практиками, ВКР

№ п/п	Наименование предыдущей дисциплины (модуля), практик, ВКР	Семестр	Шифр компетенции предыдущей дисциплины (модуля), практик, ВКР
1.	Специальные разделы физики	1	ОК-1,2; ОПК-2; ПК-6,7,8
2.	Организационно-правовые механизмы обеспечения информационной безопасности	1	ОК-2; ПК-1,3,5,14,15,16
3.	Теоретические основы компьютерной безопасности	1	ОК-2; ПК-1,5
4.	Научно-исследовательская работа в семестре (НИР)	1	ОК-1,2; ОПК-1,2; ПК-1,5,8,16
5.	Защищенные информационные системы	1	ПК-1,2,3,15
6.	Методы и средства защиты информации в системах электронного документооборота	1	ОПК-1; ПК-2,3,5
7.	Специальные разделы математики	2	ОК-1,2; ОПК-2; ПК-1,7,8
8.	Теория защиты информации	3	ОК-2; ОПК-2; ПК-1,7
9.	Основы криптографии	3	ОК-2; ОПК-2; ПК-1,7

- связь с последующими дисциплинами (модулями), практиками, ВКР

№ п/п	Наименование последующей дисциплины (модуля), практик, ВКР	Семестр	Шифр компетенции последующей дисциплины (модуля), практик, ВКР
1.	Основы имитационного модерирования автоматизированных систем	3	ОК-1,2; ПК-1,3
2.	Технология обеспечения информационной безопасности объектов	3	ПК-1,2,3,4,5,7,15
3.	Научно-исследовательская работа (НИР)	3	ОК-1,2; ОПК-1,2; ПК-3,5,6,7,8,16
4.	Производственная практика (практика по получению профессиональных умений и опыта профессиональной деятельности)	4	ОПК-1,2; ПК-1,2,5,12,13,14,15,16
5.	Преддипломная практика (преддипломная практика)	4	ОК-1,2; ОПК-1,2; ПК-1,2,3,4,5,6, 7,8,13,14,16
6.	Государственная итоговая аттестация–защита выпускной квалификационной работы, включая подготовку к защите и процедуру защиты	4	ОК-1,2; ОПК-1,2; ПК-1,2,3,4,5,6, 7,8,12,13,14,15,16

Дисциплина «Защита информации в системах беспроводной связи» обеспечивает успешное усвоение всех дисциплин и практик, требующих знания и практического применения средств, способов и методов защиты информации в системах беспроводной связи.

2. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Процесс изучения дисциплины направлен на формирование у обучаемого следующих компетенций:

способность самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения (ОК-2);

способность разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности (ПК-2).

В результате изучения дисциплины студент должен

знать:

основные нормативные документы по защите информации в системах беспроводной связи;

основные методы и алгоритмы обеспечения информационной безопасности в сетях подвижной связи;

основные механизмы обеспечения информационной безопасности в системах беспроводной широкополосной связи;

основы построения систем защиты информации в беспроводных сетях связи;

методы обнаружения и предотвращения мошенничества (фрода) в сетях беспроводной связи;

основы организации информационной безопасности в компании - операторе сети СПС;

основы построения систем и сетей беспроводной связи;

основные угрозы и уязвимости информации в системах беспроводной связи;

основные методы и алгоритмы защиты информации в системах беспроводной связи;

основы обеспечения защиты от НСД средств и сооружений связи в сетях СПС;

уметь:

приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения;

разрабатывать и проектировать защищенные системы беспроводной связи.

3. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ) С РАСПРЕДЕЛЕНИЕМ ПО СЕМЕСТРАМ

№ семестра	Виды учебных занятий	Всего часов по учебному плану	Контактная работа		Самостоятельная работа
			аудиторная	внеаудиторная	
3	лекции	18	18	х	х
	лабораторные работы	х	х	х	х
	практические/ семинарские занятия	18	18	х	х
	СРС	36	х	1,8	34,2
	СРС экз.	х	х	х	х
ИТОГО по дисциплине		**72**	**36**	**1,8**	**34,2**

Промежуточная аттестация – зачет в 3-м семестре.

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ).

4.1. Контактная аудиторная работа

4.1.1. Наименование тем лекций, их содержание и объём в часах

Тема №1. Введение. 2 ч. (ОК-2)

Важность и актуальность дисциплины. Содержание дисциплины. Основные термины и определения. Понятие о системах беспроводной связи и их защите. Обзор основных технологий и протоколов беспроводных сетей. Нормативно-правовая база по защите информации в системах беспроводной связи.

Литература: раздел 7 [1-16].

Тема №2. Структурные компоненты сети GSM/GPRS как объекты защиты от НСД. 2 ч. (ОК-2, ПК-2)

Сетевая инфраструктура GSM/GPRS. Эволюция сетей СПС ОП к сетям 3G. Абонентские терминалы и абонентский радиоинтерфейс. Биллинговая система. Цифровая транспортная сеть. WAP-платформа. Стек протоколов WAP. Спецификация приложений беспроводного доступа (WAE). SMS-платформа. MMS-платформа. Pre-paid-платформа. WEB-платформы. Гибридная сеть GPRS/WLAN (Wi-Fi). Сеть FMC (Fixed-Mobile Convergence). Корпоративные телекоммуникационные сети и информационные ресурсы предприятия-оператора.

Литература: раздел 7 [1-16].

Тема №3. Методы и алгоритмы обеспечения информационной безопасности в сетях СПС ОП стандарта GSM/GPRS. 6 ч. (ОК-2, ПК-2)

Механизмы защиты от НСД, предусмотренные стандартом GSM/GPRS. Эволюция механизмов защиты от НСД, реализованных в сетях СПС стандарта GSM. Анализ уязвимости механизмов защиты от НСД, предусмотренных стандартом GSM. Угрозы информационной безопасности сети СПС стандарта GSM/GPRS.

Обеспечение защиты от НСД средств и сооружений связи в сетях СПС стандарта GSM. Общие принципы построения систем защиты объектов связи. Специфика защиты сетей и сооружений связи. Классификация методик для построения систем защиты объектов связи от НСД. Подсистемы, входящие в систему комплексной защиты объектов связи. Методика применения интегрального подхода к построению системы защиты объектов связи от НСД. Взаимосвязь системы защиты объектов связи от НСД с действиями внутренних нарушителей.

Использование алгоритмов шифрования и аутентификации в сетях СПС стандарта GSM. Общее описание характеристик безопасности в стандарте GSM. Рекомендации Международной ассоциации GSM. Перечень алгоритмов защиты, используемых в сетях СПС стандарта GSM. Перспективные алгоритмы: алгоритм A5/3, алгоритмы спецификации G-Milenage. Атаки на алгоритмы со стороны злоумышленника.

Литература: раздел 7 [1-16].

Тема №4. Механизмы информационной безопасности в системах широкополосной связи WI-MAX и WI-FI. 4 ч. (ОК-2, ПК-2)

Общие сведения о Wi-MAX. Физический уровень IEEE 802.16 (Wi-MAX). Сетевой уровень безопасности IEEE 802.16 (Wi-MAX). Шифрование пакетов данных. Протокол управления ключами. Ассоциация безопасности (Security Associations). Назначение соответствия соединений SA.

Криптографический инструментарий. Аутентификация СП и обмен авторизованным ключом. Передача ключей шифрования пакетов с данными. Выбор средств безопасности. Механизм управления авторизацией. Механизм управления КШД. Безопасность беспроводных локальных сетей стандарта 802.11.

Литература: раздел 7 [1-16].

Тема №5. Модель защиты сети GSM от НСД с учетом методов борьбы с мошенничеством. 2 ч. (ОК-2)

Определение и классификация мошенничества (фрода) в сетях СПС. Методы обнаружения и предотвращения мошенничества (фрода) в сетях СПС стандарта GSM. Методы предотвращения мошенничества. Формальные модели защиты от НСД. Модель защиты сети GSM от НСД с учетом методов борьбы с мошенничеством

Литература: раздел 7 [1,6-16].

Тема №6. Организация информационной безопасности в компании - операторе сети СПС. 2 ч. (ОК-2)

Перечень, содержание и порядок разработки основных организационно-режимных процессов по обеспечению информационной безопасности. Разработка организационно-режимных процессов защиты информации в компаниях - операторах услуг подвижной связи на сетях СПС стандарта GSM. Типовой состав нормативной документации по обес-

печению информационной безопасности и порядок ее разработки. Типовые процессы, специфические для компании - оператора сети СПС, требующие нормативного обеспечения.

Литература: раздел 7 [1,6-16].

4.1.2. Практические (семинарские) занятия, их наименование и объем в часах

№	Наименование тем занятий	Кол-во часов	Форма контроля	Сроки контроля	Номер компетенции	Литература
1.	Проектирование защищенной системы мобильной связи стандарта GSM	6	Отчет	15-20.11	ОК-2, ПК-2	7 [17]
2.	Проектирование защищенной системы мобильной связи стандарта IEEE 802.11 (WiFi)	4	Отчет	15-20.12	ОК-2, ПК-2	7 [17]
3.	Проектирование защищенной системы мобильной связи стандарта IEEE 802.16 (WiMAX)	4	Отчет	15-20.12	ОК-2, ПК-2	7 [17]
4.	Проектирование защищенной системы мобильной связи стандарта IEEE 802. 20 (LTE)	4	Отчет	15-20.12	ОК-2, ПК-2	7 [17]

4.2. Самостоятельная работа

СРС – темы и (или) разделы тем для самостоятельного изучения, в том числе конспектирование – 34,2 ч.

№	Наименование тем (разделов)	Кол-во часов	Номер компетенции	Литература
1.	Тема №1. Введение	1,2	ОК-2	7 [1-16]
2.	Тема №2. Структурные компоненты сети GSM/GPRS как объекты защиты от НСД	2	ОК-2, ПК-2	7 [1-16]
3.	Тема №3. Методы и алгоритмы обеспечения информационной безопасности в сетях СПС ОП стандарта GSM/GPRS	2	ОК-2, ПК-2	7 [1-16]
4.	Тема №4. Механизмы информационной безопасности в системах широкополосной связи WI-MAX и WI-FI	2	ОК-2, ПК-2	7 [1-16]
5.	Тема №5. Модель защиты СЕТИ GSM от НСД с учетом методов борьбы с мошенничеством	2	ОК-2	7 [1,6-16]
6.	Тема №6. Организация информационной безопасности в компании - операторе сети СПС	2	ОК-2	7 [1,6-16]
7.	Проектирование защищенной системы мобильной связи стандарта GSM	6	ОК-2, ПК-2	7 [17]
8.	Проектирование защищенной системы мобильной связи стандарта IEEE 802.11 (WiFi)	5	ОК-2, ПК-2	7 [17]
9.	Проектирование защищенной системы мобильной связи стандарта IEEE 802.16 (WiMAX)	5	ОК-2, ПК-2	7 [17]
10.	Проектирование защищенной системы мобильной связи стандарта IEEE 802. 20 (LTE)	5	ОК-2, ПК-2	7 [17]

4.3. Контактная внеаудиторная работа

СРС: – групповые консультации с преподавателем в течение семестра – 1,8 ч.

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ, ТЕКУЩЕЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

5.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Номер компетенции «ОК-2»	Формулировка компетенции «способность самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения»	
Дисциплины, формирующие компетенцию в процессе освоения образовательной программы		Этап формирования (семестр)
Индекс	Наименование	
Б1.Б.02	Специальные разделы физики	1
Б1.В.03	Организационно-правовые механизмы обеспечения информационной безопасности	1
Б1.В.05	Теоретические основы компьютерной безопасности	1
Б2.В.01(П)	Научно-исследовательская работа в семестре (НИР)	1
Б1.В.07	Специальные разделы математики	2
Б1.В.ДВ.01.01	Теория защиты информации	3
Б1.В.ДВ.01.02	Основы криптографии	3
Б1.В.ДВ.02.02	Основы имитационного модерирования автоматизированных систем	3
Б2.В.02(П)	Научно-исследовательская работа (НИР)	3
ФТД.В.01	Программно-аппаратные средства обеспечения информационной безопасности	3
ФТД.В.02	Защита информации в системах беспроводной связи	3
Б2.В.04(П)	Преддипломная практика (преддипломная практика)	4
Б3.Б.01	Государственная итоговая аттестация–защита выпускной квалификационной работы, включая подготовку к защите и процедуру защиты	4

Номер компетенции «ПК-2»	Формулировка компетенции «способность разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности»	
Дисциплины, формирующие компетенцию в процессе освоения образовательной программы		Этап формирования (семестр)
Индекс	Наименование	
Б1.Б.03	Защищенные информационные системы	1
Б1.В.04	Методы и средства защиты информации в системах электронного документооборота	1
Б1.Б.04	Технология обеспечения информационной безопасности объектов	3
ФТД.В.02	Защита информации в системах беспроводной связи	3
Б2.В.03(П)	Производственная практика (практика по получению профессиональных умений и опыта профессиональной деятельности)	4
Б2.В.04(П)	Преддипломная практика (преддипломная практика)	4
Б3.Б.01	Государственная итоговая аттестация–защита выпускной квалификационной работы, включая подготовку к защите и проце-	4

	дуру защиты	

5.2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

Оценка сформированности компетенций в рамках промежуточной аттестации проводится по билетам зачета.

Билеты зачета должны включать в себя вопросы для оценки знаний, умений и навыков. Количество вопросов в билетах зачета должно составлять 3-10 (в случае проведения промежуточной аттестации в форме тестов количество вопросов в билетах должно составлять 10-20).

При текущей аттестации обучающихся оценка сформированности компетенций осуществляется на занятиях:

- лекционного типа посредством собеседования с обучаемыми (опрос обучающихся), в том числе по темам и (или) разделам тем, вынесенным для самостоятельного изучения обучаемыми, доклада (сообщения);
- семинарского типа посредством тестирования обучающихся, собеседования, расчетных работ в ходе практического занятия и т.п.

Номер компетенции	Показатели оценивания компетенций (знания и (или) умения и (или) навыки и (или) опыт деятельности, формируемые данной компетенцией)	Критерии оценивания компетенций на различных этапах их формирования		
		1-й уровень «УЗНАВАНИЕ»	2-й уровень «ВОСПРОИЗВЕДЕНИЕ»	3-й уровень «ПРИМЕНЕНИЕ»
1	2	3	4	5
ОК-2	**Знать:** основные нормативные документы по защите информации в системах беспроводной связи; основные методы и алгоритмы обеспечения информационной безопасности в сетях подвижной связи; основные механизмы обеспечения информационной безопасности в системах беспроводной широкополосной связи; основы построения систем защиты информации в беспроводных сетях связи; методы обнаружения и предотвращения мошенничества (фрода) в сетях беспроводной связи; основы организации информационной безопасности в компании - операторе сети СПС; **уметь** приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения	+	+	
ПК-2	**Знать:** **уметь** разрабатывать и проектировать защищенные системы беспроводной связи	+	+	

Шкала оценивания компетенций:

«отлично» - обучающийся правильно, четко, аргументировано и в полном объёме изложил содержание теоретических зачетных вопросов, успешно выполнил практические задания, убедительно ответил на все дополнительные вопросы, показал высокий уровень сформированных компетенций;

«хорошо» - обучающийся правильно, но недостаточно полно изложил содержание теоретических зачетных вопросов, успешно выполнил практические задания, испытывал затруднения при ответе на дополнительные вопросы, показал продвинутый уровень сформированных компетенций;

«удовлетворительно» - обучающийся изложил основные положения теоретических зачетных вопросов, правильно выполнил практическое задание, испытывал серьезные затруднения при ответах на дополнительные вопросы, показал пороговый уровень сформированных компетенций;

«неудовлетворительно» - обучающийся не справился с большинством теоретических зачетных вопросов и (или) не справился с выполнением практических заданий.

5.3. Типовые контрольные задания или иные материалы, необходимые для оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы.

Материалы для оценивания знаний:

Тема №1. Введение.

1. Перечислите и кратко охарактеризуйте основные технологии беспроводных сетей.
2. Назовите основные протоколы беспроводных сетей.
3. Назовите и кратко охарактеризуйте основные топологии беспроводных сетей.
4. Назовите и кратко охарактеризуйте основные методы разделения доступа к радиоканалу.
5. Назовите и кратко охарактеризуйте стандарты беспроводных сетей.
6. Назовите основные нормативные документы по защите беспроводных сетей.

Тема №2. Структурные компоненты сети GSM/GPRS как объекты защиты от НСД.

1. Структура сети сотовой подвижной связи стандарта GSM.
2. Назовите и кратко охарактеризуйте основные внутренние интерфейсы сетей GSM/GPRS
3. Назовите и кратко охарактеризуйте основные интерфейсы сетей GSM/GPRS с внешними сетями.
4. Назовите и кратко охарактеризуйте основные интерфейсы, реализуемые в подсистеме GPRS.
5. Назовите и кратко охарактеризуйте основные способы канального кодирования в сетях связи стандарта GSM.
6. типы абонентских устройств в сетях связи стандарта GSM.
7. Порядок функционирования биллинговой системы.
8. Стек протоколов беспроводного доступа WAP.
9. Архитектура службы SMS в сетях GSM.
10. Архитектура службы MMS в сетях GSM.
11. Охарактеризуйте сеть FMC (Fixed-Mobile Convergence).
12. Охарактеризуйте корпоративную телекоммуникационную сеть и информационные ресурсы предприятия-оператора.

Тема №3. Методы и алгоритмы обеспечения информационной безопасности в сетях СПС ОП стандарта GSM/GPRS.

1. Назовите и кратко охарактеризуйте основные механизмы защиты от НСД в сетях GSM/GPRS.
2. Охарактеризуйте основные механизмы аутентификации в сетях GSM/GPRS..
3. Состав секретной информации и ее распределение в аппаратных средствах GSM.
4. Порядок обеспечения секретности в сетях GSM/GPRS.
5. Порядок обеспечения подлинности абонента в сетях GSM/GPRS.
6. Назовите и кратко охарактеризуйте основные механизмы защиты от НСД в сети передачи данных GPRS.
7. Назовите и кратко охарактеризуйте основные уязвимости механизмов защиты от НСД в сетях GSM/GPRS.
8. Уязвимости механизма аутентификации абонента в сетях GSM.
9. Уязвимости алгоритмов шифрования информации в сетях GSM.
10. Уязвимости механизма использования TMSI.
11. Уязвимости технологии GPRS.
12. Угрозы информационной безопасности сетей стандарта GSM/GPRS.
13. Общие принципы построения систем защиты объектов связи.
14. В чем специфика защиты сетей и сооружений связи?
15. Классификация методик для построения систем защиты объектов связи от НСД.
16. Назовите и кратко охарактеризуйте подсистемы, входящие в систему комплексной защиты объектов связи.
17. Сущность методики применения интегрального подхода к построению системы защиты объектов связи от НСД.
18. Какова взаимосвязь системы защиты объектов связи от НСД с действиями внутренних нарушителей?
19. Назовите основные характеристики безопасности в стандарте GSM.
20. Каковы возможные последствия использования ненадежных алгоритмов шифрования?
21. Рекомендации Международной ассоциации GSM по использованию алгоритмов шифрования и аутентификации.
22. Охарактеризуйте алгоритм A5/3.
23. Охарактеризуйте алгоритмы спецификации G-Milenage.
24. Возможные атаки на алгоритмы со стороны злоумышленника.
25. Каковы рекомендации Международной ассоциации GSM по использованию встроенных алгоритмов шифрования и аутентификации?

Тема №4. Механизмы информационной безопасности в системах широкополосной связи WI-MAX и WI-FI.

1. Назовите и кратко охарактеризуйте основные механизмы защиты в системах широкополосной связи WI-MAX.
2. Назовите и кратко охарактеризуйте основные механизмы защиты в системах широкополосной связи WI-FI.
3. Охарактеризуйте физический уровень IEEE 802.16 (Wi-MAX).
4. Охарактеризуйте Сетевой уровень безопасности IEEE 802.16 (Wi-MAX).
5. Порядок функционирования ассоциаций безопасности (Security Associations).
6. Порядок аутентификации абонентских станций и обмена авторизованным ключом в сетях Wi-MAX.
7. Порядок передачи ключей шифрования пакетов с данными в сетях Wi-MAX.
8. Охарактеризуйте механизм управления авторизацией в сетях Wi-MAX.
9. Охарактеризуйте механизм управления ключами шифрования пакетов с данными в сетях Wi-MAX.

10. Порядок и средства обеспечения безопасности беспроводных локальных сетей стандарта 802.11.

Тема №5. Модель защиты СЕТИ GSM от НСД с учетом методов борьбы с мошенничеством.

1. Определение и классификация мошенничества (фрода) в сетях систем подвижной связи.
2. Методы обнаружения мошенничества (фрода) в сетях стандарта GSM.
3. Методы предотвращения мошенничества (фрода) в сетях стандарта GSM.
4. Формальные модели защиты от НСД в сетях стандарта GSM.
5. Модель защиты сети GSM от НСД с учетом методов борьбы с мошенничеством.

Тема №6. Организация информационной безопасности в компании - операторе сети СПС.

1. Классификация концепций информационной безопасности.
2. Составные части концепции информационной безопасности.
3. Порядок разработки концепции информационной безопасности компании - оператора сети СПС ГТС.
4. Жизненный цикл концепции информационной безопасности.
5. Каковы основные организационно-режимные процессы защиты информации в компаниях - операторах услуг подвижной связи?
6. Требования к разработке процессов защиты информации.
7. Содержание основных организационно-режимных процессов по обеспечению информационной безопасности.
8. Порядок разработки основных организационно-режимных процессов по обеспечению информационной безопасности.
9. Типовой состав нормативной документации по обеспечению информационной безопасности.
10. Порядок разработки нормативной документации по обеспечению информационной безопасности.
11. Типовые процессы, специфические для компании - оператора сети СПС, требующие нормативного обеспечения.

Материалы для оценивания умений.

- варианты заданий к практическим (семинарским) занятиям.

Практическое занятие №1. Проектирование защищенной системы мобильной связи стандарта GSM.

Задание в соответствии с Л. 17.

Практическое занятие №2. Проектирование защищенной системы мобильной связи стандарта IEEE 802.11 (WiFi).

Задание в соответствии с Л. 17.

Практическое занятие №3. Проектирование защищенной системы мобильной связи стандарта IEEE 802.16 (WiMAX).

Задание в соответствии с Л. 17.

Практическое занятие №4. Проектирование защищенной системы мобильной связи стандарта IEEE 802. 20 (LTE).

Задание в соответствии с Л. 17.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Практические занятия по дисциплине проводятся в учебной аудитории 322 военного института, укомплектованной специализированной мебелью и техническими средства-

ми обучения, служащими для представления учебной информации. Аудитория оснащена персональными компьютерами, объединенными в локальную сеть с выходом в Интернет. В процессе обучения используются современные программно-методические комплексы для решения задач в области информационной безопасности.

При использовании электронных изданий каждый обучающийся во время самостоятельной подготовки обеспечен рабочим местом в компьютерном классе с выходом в Интернет в соответствии с объемом изучаемой дисциплины. Время доступа в Интернет с рабочих мест вуза для внеаудиторной работы составляет для каждого студента не менее двух часов в неделю.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Основная учебная литература

1. Максименко В. Н., Афанасьев В. В., Волков Н. В. Защита информации в сетях сотовой подвижной связи/Под ред. доктора техн. наук, профессора О. Б. Макаревича. – М.: Горячая линия–Телеком, 2007. – 360 с.

Дополнительная учебная литература

Учебные издания

2. А.Н. Берлин. Сотовые системы связи [Электронный ресурс]: учебное пособие. – М.: Интернет-Университет Информационных Технологий, БИНОМ. Лаборатория знаний, 2016. – 360 с. – Режим доступа: http://www.knigafund.ru/books/178790. – Загл. с экрана.

Официальные издания

3. Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи» [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/901867280. – Загл. с экрана.
4. ГОСТ Р 53801-2010 Связь федеральная. Термины и определения. [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/1200083097. – Загл. с экрана.
5. ГОСТ 33707-2016 (ISO/IEC 2382:2015) Информационные технологии (ИТ). Словарь. [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/1200139532. – Загл. с экрана.
6. ГОСТ Р 52448-2005. Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения. [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/1200044726. – Загл. с экрана.
7. ГОСТ Р 53110-2008 Система обеспечения информационной безопасности сети связи общего пользования. Общие положения [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/1200073586. – Загл. с экрана.
8. ГОСТ Р ИСО/МЭК 13335-1-2006. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/gost-r-iso-mek-13335-1-2006. – Загл. с экрана.
9. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/1200101777. – Загл. с экрана.
10. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности. [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/1200105710. – Загл. с экрана.

11. ГОСТ Р ИСО/МЭК 15408-3-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности. [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/1200105711. – Загл. с экрана.
12. ГОСТ Р ИСО/МЭК 27011-2012 Информационная технология. Методы и средства обеспечения безопасности. Руководства по менеджменту информационной безопасности для телекоммуникационных организаций на основе ИСО/МЭК 27002. [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/1200103621. – Загл. с экрана.
13. ГОСТ Р ИСО/МЭК 27033-1-2011 Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции. [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/gost-r-iso-mek-27033-1-2011. – Загл. с экрана.
14. ГОСТ Р ИСО/МЭК 27033-3-2014 Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления. [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/1200113374. – Загл. с экрана.
15. РД 45.201-2001 Шлюзы протокола беспроводных приложений (WAP) для систем подвижной радиосвязи. Общие технические требования (с Дополнением №1). [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/1200036278. – Загл. с экрана.
16. Дополнение №1 РД 45.201-2001 Шлюзы протокола беспроводных приложений (WAP) для систем подвижной радиосвязи. Общие технические требования. [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/1200036280. – Загл. с экрана.

Методические указания к практическим занятиям

17. Голиков, А.М. Основы проектирования защищенных телекоммуникационных систем. [Электронный ресурс]: учеб. пособие – Электрон. дан. – М. : ТУСУР, 2008. – 27 с. – Режим доступа: http://e.lanbook.com/book/10865. – Загл. с экрана.

Перечень информационных технологий

1. Microsoft Windows 7, 8, 10 Enterprise, лицензия V4640039.
2. Microsoft Office 2010, 2013, 2016 Professional, лицензия V4640039.
3. MathLab, лицензия №1110632.