Частное образовательное учреждение высшего образования
«САНКТ-ПЕТЕРБУРГСКИЙ УНИВЕРСИТЕТ ТЕХНОЛОГИЙ УПРАВЛЕНИЯ И ЭКОНОМИКИ»

РАССМОТРЕНО И ОДОБРЕНО

На заседании кафедры информационных технологий и математики
Протокол № 9 от 25.05.2023 г.

УТВЕРЖДАЮ

Первый проректор
С.В. Авдашкевич
28.06.2023

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина:	Б1.В.01 Безопасность в корпоративных информационных системах
Направление подготовки:	09.04.03 Прикладная информатика
Направленность (профиль):	Корпоративные информационные системы
Уровень высшего образования:	Магистратура
Форма обучения:	очная, заочная
Разработчики:	Кандидат технических наук, доцент Курлов В.В.

Санкт-Петербург
2023

1. Цели и задачи дисциплины:

Цель освоения дисциплины:

Формирование углубленных знаний в области информационной безопасности корпоративных информационных систем и сетей на основе современных операционных систем и специализированного технического и программного обеспечения.

Задачи дисциплины:

Изучение программно-аппаратных средств обеспечения информационной безопасности корпоративных информационных систем (КИС), Освоение средств защиты сетевых служб КИС, Формирование методов анализа и планирования информационной безопасности КИС.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы высшего образования

Планируемые результаты освоения ОП ВО (код и содержание компетенций)	**Планируемые результаты обучения по ОП ВО (индикаторы достижения компетенций)**	**Примечание**
ПК-9 Управление проектами с учетом требований ИБ	ПК-9.1 Знает международные и отечественные стандарты, лучшие практики и фреймворки по управлению информационной безопасностью и программами проектов (в т.ч. ИТ-проектов); методы и средства обеспечения безопасности ИТ, критерии оценки безопасности ИТ; методы контроля безопасности ИТ; методы мониторинга и контроля управления программами ИТ-проектов;методы непрерывного улучшения управления информационной безопасностью и программами ИТ-проектов.	06.014 Профессиональный стандарт «Менеджер по информационным технологиям»
	ПК-9.2 Использует методы и средства обеспечения безопасности ИТ, соответствующие критериям оценки безопасности ИТ; умеет организовывать деятельность по непрерывному улучшению управления информационной безопасностью и программами ИТ-проектов; умеет осуществлять руководство программами ИТ-проектов; умеет осуществлять мониторинг и контроль управления информационной безопасностью и программами ИТ-проектов; формировать и декомпозировать цели управления информационной безопасностью; готов сформировать команду и организовывать персонал и стейкхолдеров для управления информационной безопасностью и программами ИТ-проектов.	
	ПК-9.3 Способен осуществлять организацию управления информационной безопасностью и программами ИТ-проектов с помощью персонала и стейкхолдеров; формировать и согласовывать принципы управления программами ИТ-проектов и информационной безопасностью; определять состав методов и средств обеспечения безопасности ИТ, соответствующих критериям оценки безопасности ИТ; осуществлять контроль качества и управление улучшением управления информационной безопасностью и программами ИТ-проектов.	

Планируемые результаты обучения по ОП ВО (индикаторы достижения компетенций)	Планируемые результаты обучения по дисциплине
ПК-9.1. Знает международные и отечественные стандарты, лучшие практики и фреймворки по управлению информационной безопасностью и программами проектов (в т.ч. ИТ-проектов); методы и средства обеспечения безопасности ИТ, критерии оценки безопасности ИТ; методы контроля безопасности ИТ; методы мониторинга и контроля управления программами ИТ-проектов;методы непрерывного улучшения управления информационной безопасностью и программами ИТ-проектов.	Знает требования и потребности в информационной безопасности, стандарты и методики управления информационной безопасностью.
ПК-9.2. Использует методы и средства обеспечения безопасности ИТ, соответствующие критериям оценки безопасности ИТ; умеет организовывать деятельность по непрерывному улучшению управления информационной безопасностью и программами ИТ-проектов; умеет осуществлять руководство программами ИТ-проектов; умеет осуществлять мониторинг и контроль управления информационной безопасностью и программами ИТ-проектов; формировать и декомпозировать цели управления информационной безопасностью; готов сформировать команду и организовывать персонал и стейкхолдеров для управления информационной безопасностью и программами ИТ-проектов.	Уметь оценивать и контролировать качество процесса управления информационной безопасностью.
ПК-9.3. Способен осуществлять организацию управления информационной безопасностью и программами ИТ-проектов с помощью персонала и стейкхолдеров; формировать и согласовывать принципы управления программами ИТ-проектов и информационной безопасностью; определять состав методов и средств обеспечения безопасности ИТ, соответствующих критериям оценки безопасности ИТ; осуществлять контроль качества и управление улучшением управления информационной безопасностью и программами ИТ-проектов.	Владеет навыками организации и контроля за изменениями в области информационной безопасности в корпоративных информационных системах.

3. Содержание, объем дисциплины и формы проведения занятий

№ п/п	Наименование темы дисциплины	Компетенции	Оценочные средства текущего контроля		
			ЗНАТЬ	УМЕТЬ	ВЛАДЕТЬ
			ПК-9.1	ПК-9.2	ПК-9.3
1	Сетевая безопасность	ПК-9	Собеседование, опрос/ Контрольная работа №1 (10)	Коллоквиум/ Проект (групповой проект) №1 (20)	Расчетно-графическая работа №1 (20)
2	Инструментарий Хакера	ПК-9	Собеседование, опрос/ Контрольная работа №1 (10)	Коллоквиум/ Проект (групповой проект) №1 (20)	Расчетно-графическая работа №2 (20)
3	Классификация типов программно-аппаратных средств защиты информации	ПК-9	Собеседование, опрос/ Контрольная работа №2 (10)	Коллоквиум/ Проект (групповой проект) №1 (20)	Деловая и (или) ролевая игра/Кейс-задача №1 (20)

№ п/п	Наименование темы дисциплины	Компетенции	Оценочные средства текущего контроля		
			ЗНАТЬ	УМЕТЬ	ВЛАДЕТЬ
			ПК-9.1	ПК-9.2	ПК-9.3
4	Методы построения программно-аппаратных средств защиты информации	ПК-9	Собеседование, опрос/ Контрольная работа №2 (10)	Коллоквиум/ Проект (групповой проект) №1 (20)	Деловая и (или) ролевая игра/Кейс-задача №1 (20)
Количество баллов (100 баллов):			100		

Содержание учебного материала, лабораторные работы и практические занятия, курсовая работа
Тема 1: Сетевая безопасность Классификация сетевых угроз, Файерволлы, Антивирусы, Обновление и настройка операционной системы, Шифрование и пароли, Архивирование и резервное копирование, Социальная инженерия. **Практические занятия/самостоятельная работа:** Защита от захвата пароля с применением атаки ARP-spoofing **Лабораторная работа:** -
Тема 2: Инструментарий Хакера Захват пароля с применением атаки ARP-spoofing, Следы пребывания Хакера, Подмена Mac-адресов, Мониторинг и анализ защищенности компьютера. **Практические занятия/самостоятельная работа:** Сокрытие своего IP и Mac-адресов, исследование атак ARP-spoofing и Man-in-the-Middle **Лабораторная работа:** -
Тема 3: Классификация типов программно-аппаратных средств защиты информации Идентификация и аутентификация, управление доступом, протоколирование и аудит, криптография, экранирование. **Практические занятия/самостоятельная работа:** Обзор методов построения: 1. Средств, разработанных для защиты информации от НСД в информационных сетях, но допускающие применение и в персональных компьютерах; 2. Средств, принципиально применимых только в компьютерных сетях и предназначенные для разделения информационных потоков, — так называемые межсетевые экраны; 3. Средств, принципиально предназначенных для защиты информации от НСД в персональных компьютерах **Лабораторная работа:** -
Тема 4: Методы построения программно-аппаратных средств защиты информации Обзор методов построения: 1. Средств, разработанных для защиты информации от НСД в информационных сетях, но допускающие применение и в персональных компьютерах; 2. Средств, принципиально применимых только в компьютерных сетях и предназначенные для разделения информационных потоков, — так называемые межсетевые экраны; 3. Средств, принципиально предназначенных для защиты информации от НСД в персональных компьютерах. **Практические занятия/самостоятельная работа:** Идентификация и аутентификация, управление доступом, протоколирование и аудит, криптография, экранирование. **Лабораторная работа:** -
Курсовая работа: не предусмотрено учебным планом

Очная форма обучения

Вид учебной работы	Всего часов	Семестр 3
Аудиторные занятия (АЗ):	36	36
Лекционные занятия (Лек)	18	18
Лабораторные занятия (Лаб)	0	0
Практические занятия (Пр)	18	18
Самостоятельная работа студента (СР)	33	33
Курсовая работа	0	0
Другие виды самостоятельной работы*	33	33
Контроль самостоятельной работы (КСР)	3	3
Контактная работа (КоР)	39	39
Форма промежуточной аттестации	0	Экзамен
Подготовка к экзамену и сдача экзамена (СР, КоР)	36	36

Вид учебной работы	Всего часов	Семестр 3
Общая трудоемкость дисциплины, часы/ЗЕТ	108/3	108/3

* Подготовка к аудиторным занятиям, подготовка к зачету (при наличии)

№	Наименование темы дисциплины	Семестр/ Курс	Количество учебных часов				Практическая подготовка
			В том числе по видам аудиторных занятий			СР	
			Лек	Пр	Лаб		
1	Сетевая безопасность	3	6	6	0	9	6
2	Инструментарий Хакера	3	4	4	0	8	4
3	Классификация типов программно-аппаратных средств защиты информации	3	4	4	0	8	4
4	Методы построения программно-аппаратных средств защиты информации	3	4	4	0	8	4
	Итого:		18	18	0	33	18

* Практическая подготовка при реализации дисциплин организована путем проведения практических занятий и (или) выполнения лабораторных и (или) курсовых работ и предусматривает выполнение работ, связанных с будущей профессиональной деятельностью.

Заочная форма обучения

Вид учебной работы	Всего часов	Семестр 3
Аудиторные занятия (АЗ):	10	10
Лекционные занятия (Лек)	4	4
Лабораторные занятия (Лаб)	0	0
Практические занятия (Пр)	6	6
Самостоятельная работа студента (СР)	85	85
Курсовая работа	0	0
Другие виды самостоятельной работы*	85	85
Контроль самостоятельной работы (КСР)	4	4
Контактная работа (КоР)	14	14
Форма промежуточной аттестации	0	Экзамен
Подготовка к экзамену/зачету и сдача экзамена/зачета (СР, КоР)	9	9
Общая трудоемкость дисциплины, часы/ЗЕТ	108/3	108/3

* Подготовка к аудиторным занятиям

№	Наименование темы дисциплины	Семестр/ Курс	Количество учебных часов				Практическая подготовка
			В том числе по видам аудиторных занятий			СР	
			Лек	Пр	Лаб		
1	Сетевая безопасность	3	2	0	0	22	6
2	Инструментарий Хакера	3	2	2	0	21	4
3	Классификация типов программно-аппаратных средств защиты информации	3	0	2	0	21	4
4	Методы построения программно-аппаратных средств защиты информации	3	0	2	0	21	4
	Итого:		4	6	0	85	18

* Практическая подготовка при реализации дисциплин организована путем проведения практических занятий и (или) выполнения лабораторных и (или) курсовых работ и (или) путем выделения часов из часов, отведенных на самостоятельную работу, и предусматривает выполнение работ, связанных с будущей профессиональной деятельностью.

4. Способ реализации дисциплины

Без использования онлайн-курса.

5. Учебно-методическое обеспечение дисциплины:

Основная литература:

1. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ. Учебное пособие для вузов / Зенков А. В., 2022 г. - 104 с. - ISBN 978-5-534-14590-8 – Режим доступа: https://urait.ru/book/informacionnaya-bezopasnost-i-zaschita-informacii-497002

2. КОРПОРАТИВНЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ: ТРЕБОВАНИЯ ПРИ ПРОЕКТИРОВАНИИ 2-е изд., испр. и доп. Учебное пособие для вузов / Астапчук В. А., Терещенко П. В. - Новосибирский государственный технический университет (г. Новосибирск)., 2022 г. - 113 с. - ISBN 978-5-534-08546-4 – Режим доступа: https://urait.ru/book/korporativnye-informacionnye-sistemy-trebovaniya-pri-proektirovanii-492141

3. БАЗЫ ДАННЫХ: ТЕХНОЛОГИИ ДОСТУПА 2-е изд., испр. и доп. Учебное пособие для вузов / Стасышин В. М., Стасышина Т. Л. - Новосибирский государственный технический университет (г. Новосибирск)., 2022 г. - 164 с. - ISBN 978-5-534-08687-4 – Режим доступа: https://urait.ru/book/bazy-dannyh-tehnologii-dostupa-492177

Дополнительная литература:

1. ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ. ЗАЩИТА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ. Учебник и практикум для вузов / Казарин О. В., Забабурин А. С. - Российский государственный гуманитарный университет (г. Москва).; Московский государственный университет имени М.В. Ломоносова (г. Москва)., 2022 г. - 312 с. - ISBN 978-5-9916-9043-0 – Режим доступа: https://urait.ru/book/programmno-apparatnye-sredstva-zaschity-informacii-zaschita-programmnogo-obespecheniya-491249

2. НАДЕЖНОСТЬ И БЕЗОПАСНОСТЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ. Учебное пособие для вузов / Казарин О. В., Шубинский И. Б. - Российский государственный гуманитарный университет (г. Москва).; Московский государственный университет имени М.В. Ломоносова (г. Москва)., 2022 г. - 342 с. - ISBN 978-5-534-05142-1 – Режим доступа: https://urait.ru/book/nadezhnost-i-bezopasnost-programmnogo-obespecheniya-493262

3. ПРОЕКТИРОВАНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ. Учебник и практикум для вузов / Под общ. ред. Чистова Д.В. - Финансовый университет при Правительстве РФ (г. Москва)., 2022 г. - 258 с. - ISBN 978-5-534-00492-2 – Режим доступа: https://urait.ru/book/proektirovanie-informacionnyh-sistem-489307

6. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения

1. Операционная система
2. Пакет прикладных офисных программ
3. Антивирусное программное обеспечение
4. LMS Moodle
5. Вебинарная платформа
6. Oracle VM Virtualbox

7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», информационных справочных систем и профессиональных баз данных, необходимых для освоения дисциплины

1. ibooks.ru : электронно-библиотечная система [Электронный ресурс] : профессиональная база данных. - Режим доступа: https://ibooks.ru. - Текст: электронный

2. Электронно-библиотечная система СПбУТУиЭ : электронно-библиотечная система [Электронный ресурс] : профессиональная база данных. - Режим доступа: http://libume.ru. - Текст: электронный

3. Юрайт : электронно-библиотечная система [Электронный ресурс] : профессиональная база данных. - Режим доступа: https://urait.ru. - Текст: электронный

4. eLibrary.ru : научная электронная библиотека [Электронный ресурс] : профессиональная база данных. - Режим доступа: http://elibrary.ru. - Текст: электронный

5. Архив научных журналов НЭИКОН [Электронный ресурс] : профессиональная база данных. - Режим доступа: arch.neicon.ru. - Текст: электронный

6. КиберЛенинка : научная электронная библиотека [Электронный ресурс] : информационная справочная система. - Режим доступа: http://cyberleninka.ru. - Текст: электронный

7. Лань : электронно-библиотечная система [Электронный ресурс] : профессиональная база данных. - Режим доступа: https://e.lanbook.com. - Текст: электронный

8. it-world.ru [Электронный ресурс] : информационная справочная система . - Режим доступа: https://www.it-world.ru. - Текст: электронный

9. Виртуальный компьютерный музей [Электронный ресурс] : информационная справочная система . - Режим доступа: https://www.computer-museum.ru. - Текст: электронный

10. Компьютерра : информационная справочная система . - Режим доступа: https://www.computerra.ru/. - Текст: электронный

11. Connect: IT-технологии : информационная справочная система. - Режим доступа: https://www.connect-wit.ru/. - Текст: электронный

12. Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации: профессиональная база данных. - Режим доступа: https://digital.gov.ru. - Текст: электронный

13. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций: профессиональная база данных . - Режим доступа: https://rkn.gov.ru. - Текст: электронный

14. Math-Net.Ru: профессиональная база данных . - Режим доступа: https://www.mathnet.ru/. - Текст: электронный

8. Материально-техническое обеспечение дисциплины

1. Учебная аудитория для проведения занятий лекционного типа, семинарского типа - практических занятий, для групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оборудованная: рабочими местами для обучающихся, оснащенными специальной мебелью; рабочим местом преподавателя, оснащенным специальной мебелью, персональным компьютером с возможностью подключения к сети «Интернет» и доступом к электронной информационно-образовательной среде Университета; техническими средствами обучения - мультимедийным оборудованием (проектор, экран, колонки) и маркерной доской; лицензионным программным обеспечением

2. Учебная аудитория для проведения занятий семинарского типа - практических занятий – компьютерный класс, оборудованный рабочими местами для обучающихся, оснащенными специальной мебелью, персональными компьютерами с возможностью подключения к сети «Интернет» и доступом к электронной информационно-образовательной среде Университета; рабочим местом преподавателя, оснащенным специальной мебелью, персональным компьютером с возможностью подключения к сети «Интернет» и доступом к электронной информационно-образовательной среде Университета; техническими средствами обучения - мультимедийным оборудованием (проектор, экран, колонки) и маркерной доской; лицензионным программным обеспечением

3. При применении электронного обучения, дистанционных образовательных технологий используются: виртуальные аналоги учебных аудиторий - вебинарные комнаты на вебинарных платформах, рабочее место преподавателя, оснащенное персональным компьютером (планшет, мобильное устройство) с возможностью подключения к сети «Интернет», доступом к электронной информационно-образовательной среде Университета и к информационно-образовательному порталу Университета umeos.ru, веб-камерой, микрофоном и гарнитурой (в т.ч. интегрированными в устройствами), программным обеспечением; рабочее место обучающегося оснащено персональным компьютером (планшет, мобильное устройство) с возможностью подключения к сети «Интернет», доступом к электронной информационно-

образовательной среде Университета и к информационно-образовательному порталу Университета umeos.ru, веб-камерой, микрофоном и гарнитурой (в т.ч. интегрированными в устройства). Авторизация на информационно-образовательном портале Университета umeos.ru и начало работы осуществляются с использованием персональной учетной записи (логина и пароля). Лицензионное программное обеспечение

4. Помещение для самостоятельной работы, оборудованное специальной мебелью, персональными компьютерами с возможностью подключения к сети «Интернет» и доступом к электронной информационно-образовательной среде Университета, лицензионным программным обеспечением

9. Оценочные материалы по дисциплине

Описание оценочных средств (показатели и критерии оценивания, шкалы оценивания) представлено в приложении к основной профессиональной образовательной программе «Каталог оценочных средств текущего контроля и промежуточной аттестации».

Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности приводятся в соответствующих методических материалах и локальных нормативных актах Университета.

Для оценивания учебных достижений студентов в Университете действует балльно-рейтинговая система.

Если оценка, соответствующая набранной в семестре сумме рейтинговых баллов, удовлетворяет студента, то она является итоговой оценкой по дисциплине при проведении промежуточной аттестации в форме экзамена/зачета с оценкой/зачета.

Условием сдачи экзамена/зачета с оценкой/зачета с целью повышения итоговой оценки по дисциплине является сдача студентом экзамена, за который он получает экзаменационные баллы без учета баллов, полученных за текущий контроль:

Шкала оценивания учебных достижений по дисциплине,завершающейся зачетом без оценки

Баллы по дисциплине	60 и менее		61-73		74-90		91-100
Итоговая оценка по дисциплине	Незачет		Зачет				
Баллы в международной шкале ECTS с буквенным обозначением уровня	50 и менее	51-60	61-67	68-73	74-83	84-90	91-100
	F	Fx	E	D	C	B	A
Уровень сформированности компетенций	Не сформированы		Пороговый		Высокий		Повышенный

Шкала оценивания учебных достижений по дисциплине, завершающейся экзаменом/ зачетом с оценкой

Баллы по дисциплине	60 и менее		61-73		74-90		91-100
Итоговая оценка по дисциплине	Неудовлетворительно		Удовлетворительно		Хорошо		Отлично
Баллы в международной шкале ECTS с буквенным обозначением уровня	<50	51-60	61-67	68-73	74-83	84-90	91-100
	F	Fx	E	D	C	B	A
Уровень сформированности компетенций	Не сформированы		Пороговый		Высокий		Повышенный

9.1. Типовые контрольные задания для текущего контроля

Собеседование, опрос/Контрольная работа №1

Разработка средств:

1. Проектирование интерфейсов для мобильных устройств и планшетов.

Собеседование, опрос/Контрольная работа №2

1. Проектирование интерфейсов, не зависящих от размера экрана.

Коллоквиум/Проект (групповой проект) №1

1. Классификация сетевых угроз.
2. Файерволлы.
3. Антивирусы.
4. Обновление и настройка операционной системы.
5. Шифрование и пароли.
6. Архивирование и резервное копирование.
7. Социальная инженерия.
8. Захват пароля с применением атаки ARP-spoofing.
9. Следы пребывания Хакера.
10. Подмена Mac-адресов.
11. Мониторинг и анализ защищенности компьютера.
12. Идентификация и аутентификация, управление доступом, протоколирование и аудит, криптография, экранирование.
13. Обзор методов построения:

13.1. Средств, разработанных для защиты информации от НСД в информационных сетях, но допускающие применение и в персональных компьютерах;
13.2. Средств, принципиально применимых только в компьютерных сетях и предназначенные для разделения информационных потоков, — так называемые межсетевые экраны;
13.3. Средств, принципиально предназначенных для защиты информации от НСД в персональных компьютерах.

Расчетно-графическая работа №1

Разработка средств:

1. Служба отправки и получения СМС.
2. Поддержка протоколов Bluetooth /Wi -Fi.
3. Установка шлюза через Wi -Fi Direct.
4. Управление анимацией.
5. Использование NFC.
6. Служба push-нотификаций.
7. Служба уведомлений и доставки.
8. Управление потоками и асинхронными задачами

Расчетно-графическая работа №2

Разработка средств:

1. Средства, разработанные для защиты информации от НСД в информационных сетях, но допускающие применение и в персональных компьютерах;
2. Средства, принципиально применимые только в компьютерных сетях и предназначенные для разделения информационных потоков;
3. Средства, принципиально предназначенные для защиты информации от НСД в персональных компьютерах

Деловая игра/Кейс-задача №1

1. «Записная книжка» Требуется разработать приложение с графическим пользовательским интерфейсом, поддерживающее создание/редактирование/удаление/поиск заметок. Два варианта хранения заметок:

А) В базе SQLite.

Б) С использованием файловой системы.

2. «Карманный навигатор» Создайте приложение с графическим пользовательским интерфейсом с функциями:

А) Определение местоположения пользователя на карте Google Map.

Б) Определение скорости и направления движения пользователя. - Масштабирование карты. Программа должна быть конфигурируемой.

3. «Песочные часы» Разработайте приложение-таймер с использованием датчика ориентации в виде песочных часов.

4. Программа для обмена мгновенными сообщениями. Требуется разработать приложение для обмена мгновенными сообщениями через WiFi/Bluetooth. Поддерживаемые режимы:

А) Активный режим. Приложение занимает весь экран, содержит поля для отправки сообщений и список принятых сообщений.

Б) Режим уведомлений. Приложение через уведомления показывает принятые сообщения.

5. Разработка интерфейсов, не зависящих от разрешения и плотности пикселов.

6. Акселерометр, датчик ориентации и компас: регулировка и программные функции.

7. Межпроцессное взаимодействие. Язык AIDL.

8. Основные права и полномочия для запуска приложений на устройстве.

9. Работа с настройками сотовой сети, подключение голосовых услуг, получение и отправка коротких сообщений.

9.2. Примерный перечень тем курсовой работы

Не предусмотрено учебным планом

9.3. Типовые контрольные задания для промежуточной аттестации: экзамен

Примерный перечень теоретических вопросов к экзамену:

Вопрос № 1

Типовые практико-ориентированные задания (задачи, кейсы):

1. Основные виды криптографических преобразований информации.
2. Математическая модель системы шифрования-дешифрования информации (представление системы шифрования графом).
3. Стойкость системы шифрования (классификация систем шифрования по стойкости, теорема об абсолютно стойкой системе шифрования).
4. Вычислительно стойкие системы шифрования (понятие о сложности криптоанализа, основные подходы к вскрытию криптографических систем).
5. Линейный рекуррентный регистр и его свойства.
6. Принципы построения формирователей шифрующей гаммы (понятие эквивалентной линейной сложности, применение нелинейных узлов для повышения линейной сложности).
7. Основные операции модульной арифметики, теоремы Эйлера, Ферма.
8. Система шифрования Эль-Гамаля. Система шифрования РША.
9. Понятие хэш-функции.
10. Определение, классификация, основные свойства ЭЦП.
11. Аутентификация сообщений в телекоммуникационных системах (модель системы имитозащиты, стратегии навязывания, показатели имитозащищенности.
12. Аутентификация пользователей, способ паролирования, варианты применения.
13. Управление закрытыми ключами (генерирование, распределение ключей, доставка, хранение).
14. Распределение ключей в асимметричных криптоситемах, протокол распределения ключей Диффи -Хеллмана.
15. Принцип управления открытыми ключами посредством сертификатов. Управление

сертификатами открытых ключей.
16. Понятие и принципы построения виртуальных защищенных сетей.
17. Назначение, принципы построения межсетевых экранов и фильтров.
18. Понятие DDOS-атаки, способы организации атаки. Способы противодействия DDOS-атакам.
19. Компьютерные вирусы и их классификация.

Примерный перечень практических заданий к экзамену:
Вопрос № 2

Рассчитать апостериорные вероятности использованных ключей для заданного зашифрованного сообщения $\bar{e}$:
а. P(a) = 0.1, P(b) = 0.7, P(c) = 0.2, $\bar{e}$ = abaacac,
б. P(a) = 0.9, P(b) = 0.09, P(c) = 0.01, $\bar{e}$ = cbaccca,
в. P(a) = 0.14, P(b) = 0.06, P(c) = 0.8, $\bar{e}$ = bbabbcab,
г. P(a) = 0.7, P(b) = 0.05, P(c) = 0.25, $\bar{e}$ = cccacbbc,
д. P(a) = 0.1, P(b) = 0.7, P(c) = 0.2, $\bar{e}$ = abbbbab.

Раздел билета	Компетенции	Планируемые результаты обучения по дисциплине	Количество баллов
Вопрос №1 Теоретический вопрос (проверяет знания («знать»), сформированные дисциплиной)	ПК-9	Знает требования и потребности в информационной безопасности, стандарты и методики управления информационной безопасностью.	40
Вопрос №2 Практическое задание (проверяет умения («уметь»), проверяет практические навыки («владеть»), сфор-мированные дисциплиной)	ПК-9	Уметь оценивать и контролировать качество процесса управления информационной безопасностью. Владеет навыками организации и контроля за изменениями в области информационной безопасности в корпоративных информационных системах.	60