Министерство образования и науки Российской Федерации

федеральное государственное бюджетное образовательное учреждение высшего образования
РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

Кафедра Информационных технологий и систем безопасности

Рабочая программа по дисциплине

ЗАЩИТА ПРОГРАММНЫХ СРЕДСТВ ЗАЩИЩЕННЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

Основная профессиональная образовательная программа
высшего образования программы специалитета по специальности

10.05.02 «Информационная безопасность телекоммуникационных систем»

Специализация:
Разработка защищенных телекоммуникационных систем

Квалификация:
Специалист

Форма обучения
Очная

Согласовано
Руководитель ОПОП
«Информационная безопасность телекоммуникационных систем»

_____ Бурлов В.Г.

Утверждаю
Председатель УМС _____И.И. Палкин

Рекомендована решением
Учебно-методического совета
18 июня 2018 г., протокол № 4

Рассмотрена и утверждена на заседании кафедры
17 мая 2018 г., протокол № 5
Зав. кафедрой _____ Бурлов В.Г.

Авторы-разработчики:
_____Ананченко И.В.

Санкт-Петербург 2018

1. Цели освоения дисциплины

Цели освоения дисциплины «Защита программных средств защищенных ТКС» является формирование у студентов знаний и умений по защите компьютерной информации, обрабатываемой и хранимой в современных автоматизированных системах (АС), от неправомерного доступа, перехвата и разрушающего программного воздействия, на основе применения современных программно-аппаратных средств.

Приобретенные знания позволят студентам выполнять задачи по проектированию и разработке программно-аппаратных средств защиты информации, правильно ориентироваться в многообразии выпускаемых и предлагаемых средств информационной защиты, обоснованно выбирать те из них, которые отвечают требованиям, предъявляемым к защите информации в конкретной автоматизированной системе, а также оценивать эффективность безопасности информационных технологий.

Задачи получение учащимися базовых знаний о процессе и методах использования программно-аппаратных средств для обеспечения информационной безопасности.

2. Место дисциплины в структуре ОП

Дисциплина «Защита программных средств защищенных ТКС» для направления подготовки 10.05.02 – информационная безопасность телекоммуникационных систем относиться к дисциплинам базовой части блока дисциплин (модулей) (Б1.Б.35.05) профессионального цикла.

Для освоения данной дисциплины, необходимо обладать базовыми знаниями (общее среднее образование), а также освоить учебный материал предшествующих дисциплин:
«Информатика», «Теория вероятностей и математическая статистика», «Дискретная математика», «Основы информационной безопасности», «Телекоммуникационные системы», «Сети и системы передачи информации», «Моделирование систем и сетей телекоммуникаций», «Теория принятия решения в условиях информационных конфликтов», «Проектирования защищенных телекоммуникационных систем», «Сетевое администрирование», «Информационная безопасность ТКС», «Разработка защищенных ТКС спец. назначения».

Знания и практики, полученные обучаемыми по дисциплине «Защита программных средств защищенных ТКС», непосредственно используются при написании выпускной работы студента и в практической профессиональной деятельности, связанной с защитой информации от утечки по техническим каналам.

3. Компетенции обучающегося, формируемые в результате освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Код компетенции	Компетенция
ОК-8	способностью к самоорганизации и самообразованию
ПК-8	способностью проводить анализ эффективности технических и программно-аппаратных средств защиты телекоммуникационных систем
ПК-14	способностью выполнять установку, настройку, обслуживание, диагностику, эксплуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты телекоммуникационных сетей и систем
ПСК-7.5	способностью обеспечивать защиту программных средств защищенных телекоммуникационных систем;

В результате освоения компетенций в рамках дисциплины обучающийся должен:

Код компетенции	Результаты обучения
ОК-8	Знать: основные этапы организации самостоятельной работы над проектом Уметь: планировать свою работу над проектом Владеть: навыками поиска и обработки информации
ПК-8	Знать как проводить анализ эффективности технических и программно-аппаратных средств защиты телекоммуникационных систем Уметь: применять технические и программные средства для анализ эффективности технических и программно- аппаратных средств защиты телекоммуникационных систем Владеть: навыками анализа эффективности технических и программно-аппаратных средств защиты телекоммуникационных систем
ПК-14	Знать тенденции развития информационной безопасности телекоммуникационных систем, как выполнять установку, настройку, обслуживание, диагностику, эксплуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, технических и программно- аппаратных средств защиты телекоммуникационных сетей и систем Уметь: выполнять установку, настройку, обслуживание, диагностику, эксплуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты телекоммуникационных сетей и систем Владеть. методами установки, настройки, обслуживания, диагностики, эксплуатации и восстановления работоспособности телекоммуникационного оборудования и приборов, технических и программно- аппаратных средств защиты телекоммуникационных сетей и систем

ПСК -7.5	Знать как обеспечивать защиту программных средств защищенных телекоммуникационных систем Уметь: обеспечивать защиту программных средств защищенных телекоммуникационных систем Владеть: методами разработки защиты программных средств защищенных телекоммуникационных систем

Основные признаки проявленности формируемых компетенций в результате освоения дисциплины «Защита программных средств защищенных ТКС» сведены в таблице.

Уровень освоения компетенции	**Результат обучения**	**Результат обучения**	**Результат обучения**	**Результат обучения**
	ОК -8: Знать, уметь, владеть	ПК -8: Знать, уметь, владеть	ПК –14: Знать, уметь, владеть	ПСК -7.5Знать, уметь, владеть
минимальный	Способен дать собственную критическую оценку изучаемого материала	Владеет основными навыками работы с источниками и критической литературой	Способен дать собственную критическую оценку изучаемого материала	Владеет основными навыками работы с источниками и критической литературой
	Может соотнести основные идеи с современными проблемами	Способен представить ключевую проблему в ее связи с другими процессами	Может соотнести основные идеи с современными проблемами	Способен представить ключевую проблему в ее связи с другими процессами
	Способен выделить характерный авторский подход	Понимает специфику основных рабочих категорий	Способен выделить характерный авторский подход	Понимает специфику основных рабочих категорий
базовый	Способен сравнивать концепции, аргументированно излагает материал	Свободно излагает материал, однако не демонстрирует навыков сравнения основных идей и концепций	Способен сравнивать концепции, аргументированно излагает материал	Свободно излагает материал, однако не демонстрирует навыков сравнения основных идей и концепций
	Аргументированно проводит сравнение концепций по заданной проблематике	Способен выделить и сравнить концепции, но испытывает сложности с их практической привязкой	Аргументированно проводит сравнение концепций по заданной проблематике	Способен выделить и сравнить концепции, но испытывает сложности с их практической привязкой
	Способен выделить специфику концепций в заданной проблемной области	Знает основные отличия концепций в заданной проблемной	Способен выделить специфику концепций в заданной проблемной области	Знает основные отличия концепций в заданной проблемной области

		области		
продвинутый	Способен грамотно обосновать собственную позицию относительно решения современных проблем в заданной области	Видит источники современных проблем в заданной области анализа, владеет подходами к их решению	Способен грамотно обосновать собственную позицию относительно решения современных проблем в заданной области	Видит источники современных проблем в заданной области анализа, владеет подходами к их решению
	Свободно ориентируется в заданной области анализа. Понимает ее основания и умеет выделить практическое значение заданной области	Выявляет основания заданной области анализа, понимает ее практическую ценность, однако испытывает затруднения в описании сложных объектов анализа	Свободно ориентируется в заданной области анализа. Понимает ее основания и умеет выделить практическое значение заданной области	Выявляет основания заданной области анализа, понимает ее практическую ценность, однако испытывает затруднения в описании сложных объектов анализа
	Может дать критический анализ современным проблемам в заданной области анализа	Знает основное содержание современных научных идей в рабочей области анализа, способен их сопоставить	Может дать критический анализ современным проблемам в заданной области анализа	Знает основное содержание современных научных идей в рабочей области анализа, способен их сопоставить

Соответствие уровней освоения компетенции планируемым результатам обучения и критериям их оценивания

Этап (уровень) освоения компетенции	Основные признаки проявленности компетенции (дескрипторное описание уровня)				
	1.	2.	3.	4.	5.
минимальный	не владеет	слабо ориентируется в терминологии и содержании	Способен выделить основные идеи текста, работает с критической литературой	Владеет основными навыками работы с источниками и критической литературой	Способен дать собственную критическую оценку изучаемого материала
	не умеет	не выделяет основные идеи	Способен показать основную идею в развитии	Способен представить ключевую проблему в ее связи с другими процессами	Может соотнести основные идеи с современными проблемами
	не знает	допускает грубые ошибки	Знает основные рабочие категории, однако не ориентируется в их специфике	Понимает специфику основных рабочих категорий	Способен выделить характерный авторский подход
базовый	не владеет	плохо ориентируется в терминологии и содержании	Владеет приемами поиска и систематизации, но не способен свободно изложить материал	Свободно излагает материал, однако не демонстрирует навыков сравнения основных идей и концепций	Способен сравнивать концепции, аргументированно излагает материал
	не умеет	выделяет основные идеи, но не видит проблем	Выделяет конкретную проблему, однако излишне упрощает ее	Способен выделить и сравнить концепции, но испытывает сложности с их практической привязкой	Аргументированно проводит сравнение концепций по заданной проблематике
	не знает	допускает много ошибок	Может изложить основные рабочие категории	Знает основные отличия концепций в заданной проблемной области	Способен выделить специфику концепций в заданной проблемной области
продвинутый	не владеет	ориентируется в терминологии и содержании	В общих чертах понимает основную идею, однако плохо связывает ее с существующей проблематикой	Видит источники современных проблем в заданной области анализа, владеет подходами к их решению	Способен грамотно обосновать собственную позицию относительно решения современных проблем в заданной области
	не умеет	выделяет основные идеи, но не видит их в развитии	Может понять практическое назначение основной идеи, но затрудняется выявить ее основания	Выявляет основания заданной области анализа, понимает ее практическую ценность, однако испытывает затруднения в описании сложных объектов анализа	Свободно ориентируется в заданной области анализа. Понимает ее основания и умеет выделить практическое значение заданной области
	не знает	допускает ошибки при выделении рабочей области анализа	Способен изложить основное содержание современных научных идей в рабочей области анализа	Знает основное содержание современных научных идей в рабочей области анализа, способен их сопоставить	Может дать критический анализ современным проблемам в заданной области анализа

4. Структура и содержание дисциплины

Общая трудоемкость (объем) дисциплины (модуля) составляет 4 зачетные единицы, 144 академических часа.

Объём дисциплины	**Всего часов**
	Очная форма обучения
Общая трудоёмкость дисциплины	144
Контактная работа обучающихся с преподавателям (по видам аудиторных учебных занятий) – всего:	80
в том числе:	
лекции	32
Лабораторные работы	32
практические занятия	16
семинарские занятия	
Самостоятельная работа (СРС) – всего:	64
в том числе:	
курсовая работа	
контрольная работа	
Вид промежуточной аттестации (зачет/экзамен)	экзамен
Всего:	144

4.1. Структура дисциплины

№ п/п	**Раздел и тема дисциплины**	**Семестр**	**Виды учебной работы, в т.ч. самостоятельная работа студентов, час.**			**Формы текущего контроля успеваемост и**	**Занятия в активной и интерактивно й форме, час.**	**Формируемые компетенции**
			Лекции	**Лаборат. Практич.**	**Самост. работа**			
1	Введение. Предмет курса и его задачи.	**10**	4	4	6	Устный опрос по изучаемой теме. Вопрос на экзамене	8/4	ОК-8 ПСК-7.5, ПК-14
2	Использование программных и аппаратных ключей серии для защиты программного обеспечения (SENTINEL HASP HL и SENTINEL HASP SL)	**10**	4	6	6	Устный опрос по изучаемой теме. Вопрос на экзамене	10/6	ОК-8 ПСК-7.5, ПК-8

3	Обеспечение конфиденциальной работы с электронной почтой на основе электронных цифровых сертификатов, хранящихся в защищенных носителях аппаратных ключах	**10**	4	6	8	Устный опрос по изучаемой теме. Вопрос на экзамене	10/6	ОК-8 ПК-8, ПК-14
4	Современные тенденции развития угроз, связанных с применением программного обеспечения, принципы и технологии, используемые для борьбы с вредоносными программами.	**10**	4	4	4	Устный опрос по изучаемой теме. Вопрос на экзамене	8/4	ОК-8 ПК-8, ПК-14
5	Построение программно-аппаратных комплексов шифрования	**10**	2	4	6	Устный опрос по изучаемой теме. Вопрос на экзамене	6/4	ОК-8 ПСК-7.5, ПК-8
6	Методы и средства ограничения доступа к компонентам ЭВМ	**10**	4	8	6	Устный опрос по изучаемой теме. Вопрос на экзамене	12/4	ОК-8 ПК-14, ПК-8
7	Особенности защиты данных от изменения. Программно-аппаратные средства шифрования	**10**	2	6	4	Устный опрос по изучаемой теме. Вопрос на экзамене	8/4	ОК-8 ПК-14, ПК-8
8	Защита программ от изучения. Аппаратный ключ с точки зрения электроники.	**10**	4	6	14	Устный опрос по изучаемой теме. Вопрос на экзамене	12/6	ОК-8 ПК-14, ПК-8

9	Защита от разрушающих программных воздействий.	**10**	4	4	10	Устный опрос по изучаемой теме. Вопрос на экзамене	8/4	ОК-8 ПК-14, ПК-8
	ИТОГО		32	48	64		80/36	

4.2. Содержание разделов дисциплины

4.2.1. Введение

Предмет курса и его задачи. Основные подходы к защите программного обеспечения.

4.2.2. Использование программных и аппаратных ключей серии для защиты программного обеспечения (SENTINEL HL и SENTINEL SL)

Защита программного обеспечения программно-аппаратными ключами марки SENTINEL HL Pro. Защита программного обеспечения программно-аппаратными ключами марки SENTINEL HL Basic. Защита сетевого программного обеспечения программно-аппаратными ключами марки SENTINEL HL Net. Лизинг программного обеспечения с использованием технологии защита программного обеспечения программно-аппаратными ключами марки SENTINEL HL Time. Лизинг сетевого программного обеспечения с использованием технологии защита программного обеспечения программно-аппаратными ключами марки SENTINEL HL TimeNet. Защита программного обеспечения комплекса, исполняемая программа формата ex4 и вызываемая ею библиотека dll, ключами серии SENTINEL HL. Защита программного обеспечения комплекса, исполняемая программа формата ex4 и вызываемая ею библиотека dll, электронными ключами SENTINEL HASP Sl.

4.2.3 Обеспечение конфиденциальной работы с электронной почтой на основе электронных цифровых сертификатов, хранящихся в защищенных носителях аппаратных ключах

Обеспечение конфиденциальной работы с электронной почтой на основе электронных цифровых сертификатов, хранящихся в защищенных носителях аппаратных ключах серии e-token. Обеспечение конфиденциальной работы с электронной почтой на основе электронных цифровых сертификатов, хранящихся в защищенных носителях аппаратных ключах серии ru-token. Обеспечение конфиденциальной работы с электронной почтой на основе электронных цифровых сертификатов, хранящихся в защищенных носителях аппаратных ключах серии ru-token.

4.2.4 Современные тенденции развития угроз, связанных с применением программного обеспечения, принципы и технологии, используемые для борьбы с вредоносными программами.

Основы теории компьютерных вирусов (вирусы, классификация вирусов), современные тенденции развития угроз, связанных с применением программного обеспечения, принципы и технологии, используемые для борьбы с вредоносными программами и другими сетевыми угрозами, общие принципы построения систем антивирусной защиты, а также примеры построения

антивирусной защиты компьютерной сети. Защита исполняемых файлов VMProtect SenseLock Edition. VMProtect SenseLock Edi- tion (VMProtect SE). Совместное использование VMProtect и электронных ключей Sense- Lock.

4.2.5 Сетевое программное обеспечение - уязвимости и методы защиты. Построение программно-аппаратных комплексов шифрования

Сетевое программное обеспечение - уязвимости и методы защиты. Различные категории атак, их определения и условия для осуществления атак. Рассмотрение механизм проведения атак. Аппаратные и программно-аппаратные средства криптозащиты данных.

4.2.6 Методы и средства ограничения доступа к компонентам ЭВМ

Компоненты ПЭВМ. Классификация защищаемых компонент ПЭВМ: отчуждаемые и неотчуждаемые компоненты ПЭВМ. Процесс начальной загрузки ПЭВМ, взаимодействие аппаратной и программной частей. Механизмы расширения BIOS. Преимущества и недостатки программных и аппаратных средств. Проблемы использования расширенной BIOS: эмуляция файловой системы до загрузки ОС и т.д.

4.2.7 Проблема защиты отчуждаемых компонентов ПЭВМ. Привязка ПО к внешним (добавляемым) аппаратным элементам

Способы защиты информации на съемных дисках. Организация прозрачного режима шифрования. Надежность средств защиты компонент. Понятие временной и гарантированной надежности. Защита программ от несанкционированного копирования. Юридические аспекты несанкционированного копирования программ. Обще понятие защиты от копирования. Разновидности задач защиты от копирования. Подходы к задаче защиты от копирования.

Привязка к портовым ключам. Использование дополнительных плат расширения. Методы «водяных знаков» и методы «отпечатков пальцев». Хранение ключей информации. Пароли и ключи. Секретная информация, используемая для контроля доступа: ключи и пароли. Злоумышленник и ключи. Классификация средств хранения ключей и идентифицирующей информации. Организация хранения ключей (с примерами реализации). Магнитные диски прямого доступа. Магнитные и интеллектуальные карты. Средство TouchMemory. Типовые решения в организации типовых систем. Открытое распределение ключей. Метод управляемых векторов.

428. Защита программ от изучения. Аппаратный ключ с точки зрения электроники.

Изучение и обратное проектирование ПО. Понятие изучения и обратного проектирования ПО. Цели и задачи изучения работы ПО. Способы изучения ПО: статистическое и динамическое изучение. Роль программной и аппаратной среды. Временная надежность (невозможность обеспечения гарантированной надежности). Задачи защиты от изучения и способы их решения. Динамическое преобразование кода. Исследование программного обеспечения на предмет отсутствия не декларированных возможностей.

Защита от отладки. Итеративный программный замок. Принцип ловушек и избыточного кода. Защита от дизассемблирования. Принцип внешней загрузки файлов. Динамическая модификация программы. Защита от трассировки по прерываниям. Способы ассоциирования защиты и программного обеспечения. Оценка надежности защиты от отладки. Ключи на базе перепрограммируемой

постоянной памяти. Ключи на базе заказных чипов. Примеры реализации ключей (SENTINEL HASP, eToken, ruToken, Guardant). Ключи на базе микропроцессоров.

429. Защита от разрушающих программных воздействий.

Модели взаимодействия прикладной программы и программы злоумышленника, компьютерные вирусы как особый класс РПВ, активная и пассивная защита, необходимые и достаточные условия недопущения разрушающего воздействия; понятие изолированной программной среды, защита программ от изменения и контроль целостности. Основные категории требований к программной и программно-аппаратной реализации средств обеспечения ИБ. Основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности; программно- аппаратные средства обеспечения информационной безопасности в типовых ОС, СУБД, вычислительных сетях.

4.3. Практические, лабораторные занятия, их содержание

№ п/п	№ раздела дисциплины	Тема занятия	Форма проведения	Формируемые компетенции
1	1	Sentinel Admin Control Center - управление менеджерами лицензий и ключами Sentinel (HASP). Комплект разработчика Sentinel HASP - Sentinel License Development Kit (LDK). Стартовый комплект разработчика Sentinel HASP. Исследование программного обеспечения на предмет отсутствия не декларированных возможностей. Использование программных и аппаратных ключей серии SENTINEL HASP HL и SENTINEL HASP SL для защиты программного обеспечения	Практика, лабораторная	ОК-8 ПСК-7.5, ПК-14
2	2	Использование программных и аппаратных ключей серии GUARDANT для защиты программного обеспечения	Практика, лабораторная	ОК-8 ПСК-7.5, ПК-8
3	3	Использование ключей серий eToken и ruToken для шифрования информации и ЭЦП	Практика, лабораторная	ОК-8 ПК-14, ПК-8
4	4	Разработка программы шифрования с обратной связью. Цель работы приобретение практических навыков разработки утилит шифрования, разработка программы шифрования с обратной связью. Защита программы программным ключом.	Практика, лабораторная	ОК-8 ПК-14, ПК-8
5	5	Разработка программы псевдослучайной генерации чисел. Цель работы: получить	Практика, лабораторная	ОК-8 ПСК-7.5, ПК-14
		практические навыков разработки специализированных приложений, разработка программы псевдослучайной генерации чисел. Защита программы аппаратным ключом.	Практика, лабораторная	

6	6	Разработка программы сканирования портов. Цель работы: разработать программу сканирования портов средствами Visual Studio. Защита программы аппаратным ключом.	Практика, лабораторная	ОК-8 ПК-8, ПК-14
7	7	Разработка программы антивируса-монитора. Цель работы приобретение практических навыков работы по созданию антивирусных утилит, разработка резидентных приложений – разработка программы антивируса-монитора.	Практика, лабораторная	ОК-8 ПК-14, ПК-8
8	8	Разработка программы, имитирующей вирусоподобные действия. Цель работы: разработка средствами Visual Studio программы, имитирующей вирусоподобные действия	Практика, лабораторная	ОК-8 ПК-8, ПК-14
9	9	Разработка программы атаки на криптоалгоритм методом встречи в середине атаки. Цель работы: разработка программы атаки на криптоалгоритм методом встречи в середине атаки.	Практика, лабораторная	ОК-8 ПК-8, ПК-14

5. Учебно-методическое обеспечение самостоятельной работы студент и оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

5.1. Текущий контроль

Текущий контроль производится путем тестирования и проверки контрольных работ.

5.2. Методические указания по организации самостоятельной работы

Во время самостоятельной работы студенты знакомятся с проведением расчетов проектируемых параметров сети. В перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине «Защита программных средств защищенных ТКС» входит:

1. Методические указания по выполнению практических работ.
2. Дополнительный лекционный материал

Контроль исполнения самостоятельных работ осуществляется преподавателем с участием студентов в форме обсуждения выполненных заданий и работ.

Источники для самостоятельной подготовки:

1. Ананченко И. В., Смирнов П. И., Шапаренко Ю. М.. Информационная безопасность телекоммуникационных систем. Часть 1. Аппаратные ключи eToken. Средство защиты eToken Network Logon: учебное пособие – СПб.: РГГМУ, – 2016. – 24 с., ил. - Режим доступа: http://elib.rshu.ru/files_books/pdf/rid_934e2a15ca2e4a408df0517464e9941f.pdf

5.3. Промежуточный контроль: экзамен

Перечень вопросов для промежуточной аттестации (экзамен):

1. Состав и краткая характеристика основных угроз доступности?
2. Состав и краткая характеристика основных угроз целостности?
3. Состав и краткая характеристика основных угроз конфиденциальности?
4. Классификация категорий хакеров и их целей?
5. Состав и краткая характеристика организационно коммуникативных средств НСД?
6. Состав и краткая характеристика технических средств НСД?
7. Состав и краткая характеристика программных средств НСД?
8. Характеристика основных угроз ИБ при взаимодействии с Internet? требования к подсистеме защиты от угроз ИБ при взаимодействии с Internet?
9. Классификация сетевых атак?
10. Определение сниффера пакетов и характеристика основных средств защиты от сниффинга?
11. Определение IP спуфинга и характеристика основных средств защиты от него?
12. Определение атак типа DoS («отказ в обслуживании») и характеристика основных средств защиты от них?
13. Определение парольных атак и характеристика основных средств защиты от них?
14. Определение атак на уровне приложений и типа Man in the Middle и характеристика основных средств защиты от них?
15. Определение сетевой разведки и переадресации портов и характеристика основных средств защиты от них?
16. Основные методы и условия неавторизованного доступа к ЛВС?
17. Краткая характеристика основных условий НСД к ЛВС?
18. Краткая характеристика основных условий раскрытия данных ЛВС?
19. Краткая характеристика неавторизованной модификации данных и программ и основных условий ее возникновения?
20. Краткая характеристика основных условий раскрытия и подмены трафика ЛВС?
21. Основные угрозы ИБ ЛВС при распределенном хранении файлов и удаленных вычислениях?
22. Основные сервисы безопасности?
23. Основные принципы архитектурной безопасности и их краткая характеристика?
24. Структурная схема системы ЗИ для типовой информационной системы, краткая характеристика ее основных блоков?
25. Основные функции централизованного управления рисками и администрирования системы безопасности?
26. Основные функции защиты управления приложениями?
27. Основные функции защиты системы сетей?
28. Основные функции защиты конечных пользователей?
29. Классификация средств защиты программного обеспечения и характеристика их основных категорий?
30. Классификация средств защиты в составе вычислительной системы (ВС) и характеристика их основных оставляющих?
31. Принципы организации и технического исполнения защиты магнитных дисков и защитных механизмов устройств ВС?
32. Принципы организации и технического исполнения замков защиты и защиты типа

«изменение функций»?
33. Классификация средства защиты с запросом информации и характеристика их основных составляющих?
34. Назначение и принцип формирования паролей, шифров, сигнатур?
35. Назначение и основные принципы построения аппаратуры защиты?
36. Классификация средств активной защиты и характеристика их основных составляющих?
37. Определение и характеристика основных внутренних средств активной защиты?
38. Определение и характеристика основных внешних средств активной защиты?
39. Классификация средств пассивной защиты и характеристика их основных составляющих?
40. Назначение и основные принципы организации идентификации программ?
41. Назначение и основные принципы построения устройств контроля?
42. Общий состав требований по обеспечению ИБ?
43. Требования к программно-аппаратным средствам?
44. Требования к подсистеме идентификации и аутентификации?
45. Требования к подсистеме управления доступом?
46. Требования к подсистеме протоколирования аудита?
47. Требования к подсистеме защиты повторного использования объектов и к защите критичной информации?
48. Требования к средствам обеспечения целостности?
49. Требования к средствам управления ИБ?
50. Общий состав требований к межсетевому экрану?
51. Подсистема управления доступом в автоматизированной системе и основные требования к ней для защиты от НСД?
52. Подсистема регистрации и учета в автоматизированной системе и основные требования к ней для защиты от НСД?
53. Криптографическая подсистема ЗИ в автоматизированной системе и основные требования к ней для защиты от НСД?
54. Подсистема обеспечения целостности в автоматизированной системе и основные требования к ней для защиты от НСД?
55. Показатели защищенности информации от НСД для компьютерных систем и их краткая характеристика?
56. Показатели защищенности межсетевых экранов и их краткая характеристика.
57. Электронные ключи Guardant. Электронный ключ Guardant Sign. Электронный ключ Guardant Code. Лицензирование сетевых приложений. Защищенные схемы продаж.
58. Электронные ключи Guardant. Guardant SP. Сервер активации. Принцип работы. Технические характеристики.
59. Электронные ключи Guardant. Выбор модели ключа. Защита Windows-приложений.
60. Электронные ключи Guardant. Выбор модели ключа. Удаленное обновление памяти ключа. Guardant TRU API
61. Комплекты разработчика Guardant. Выбор модели ключа.
62. Электронный идентификатор Rutoken. Электронный идентификатор Rutoken. Комплект разработчика Rutoken
63. Комплект разработчика Rutoken. Электронные идентификаторы Рутокен Web.

64. Аппаратные ключи защиты серии SENTINEL HASP. Аппаратные ключи защиты SENTINEL HASP 4-го и 5-го поколения.
65. Ключ Guardant: назначение, основные характеристики, пример использования Net.
66. Аппаратные ключи защиты RuToken
67. Инфраструктура с открытыми ключами PKI. Аппаратные ключи защиты eToken
68. Виртуальные защищенные сети: виды, характеристики и варианты реализации.
69. Ключ eToken: назначение, основные характеристики, пример использования
70. Ключ ruToken: назначение, основные характеристики, пример использования
71. Аппаратные ключи защиты серий HASP HL и HASP 4. Сравнительные характеристики, область применения.
72. Использование аппаратных ключей защиты eToken и SENTINEL HASP для защиты ПО и информации пользователей.
73 Понятие – информационная безопасность. Информационная безопасность в сфере компьютерных сетевых технологий. Протокол https, криптопротоколы SSL, TLS.
74. Защита почтовых систем. Защита серверов и рабочих станций. Защита программного обеспечения – общие подходы и принципы. Электронные цифровые сертификаты. Принцип работы. Формальное описание. Структура сертификата. Российские стандарты.
75. Защита программного обеспечения с помощью аппаратных ключей серии Guardant
76. Семейство электронных ключей Guardant для защиты программного обеспечения от несанкционированного копирования и распространения.
77. Частные сети (VPN): принципы построения, конфигурирование, варианты реализации.
78. Защита программного обеспечения с помощью аппаратных ключей SENTINEL HASP HL, Hasp 4.
79. Ключи серий SENTINEL HASP HL и Hasp 4. Область применения, основные отличия.
80. Электронный ключ (аппаратный ключ). Принципы работы, классификация, примеры использования.
81. Ключи серий ruToken и eToken – сравнительная характеристика, область применения.
82. Технологии аутентификации и шифрования. Реализация безопасной сетевой инфраструктуры для web-сервера.
83. Защита ПО с помощью аппаратных или программных ключей Sentinel HASP

Образец экзаменационного билета:

№ 1

1) Способы и средства защиты программ от несанкционированного копирования. Защищенные операционные системы

2) Назначение и основные принципы построения аппаратуры защиты. Классификация средств активной защиты и характеристика их

основных составляющих.

6. Учебно-методическое и информационное обеспечение дисциплины

а) основная литература:

1. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — М. : Издательство Юрайт, 2018. — 312 с. — (Серия : Специалист). — ISBN 978-5-9916-9043-0.- Режим доступа: https://biblio-online.ru/viewer/E458AFCD-826E-4A1F-9BAB-68BB83EA616F
2. Ананченко И. В., Смирнов П. И., Шапаренко Ю. М.. Информационная безопасность телекоммуникационных систем. Часть 1. Аппаратные ключи eToken. Средство защиты eToken Network Logon: учебное пособие – СПб.: РГГМУ, – 2016. – 24 с., ил. - Режим доступа: http://elib.rshu.ru/files_books/pdf/rid_934e2a15ca2e4a408df0517464e9941f.pdf

б) дополнительная литература:

1. Проектирование защищенных информационных систем [Текст] : учебное пособие. Ч. 1. Конструкторское проектирование. Защита от физических полей. . П. П. Бескид, В. Ю. Суходольский, Ю. М. Шапаренко. – СПб.: Изд-во РГГМУ, 2008. – 195 с.

в) программное обеспечение и Интернет-ресурсы:

Программное обеспечение:

- windows 7
- office 2007
- dr Web
- Программа оптимизации структуры защищенной компьютерной сети с применением генетического алгоритма №2016611252
- Экспертная система выбора оптимальных средств защиты электронного контента №2016611251

Интернет-ресурсы

- https://biblio-online.ru – ЭБС Юрайт
- http://znanium.com – ЭБС Знаниум
- http://www.prospektnauki.ru – ЭБС Проспект науки
- http://elib.rshu.ru ЭБС ГидроМетеоОнлайн
- https://нэб.рф - Национальная электронная библиотека

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

	Организация деятельности студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удается разобраться в

	материале, необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии.
Практические	На практических занятиях выполняются задания по обеспечению информационной безопасности с использованием программно-аппаратных средств, изученных во время лекционных занятий. Как правило, на каждом занятии студент должен показать результаты выполнения практического задания преподавателю.
Внеаудиторная работа	представляет собой вид занятий, которые каждый студент организует и планирует самостоятельно. Самостоятельная работа студентов включает самостоятельное изучение разделов дисциплины.
Подготовка к зачёту	При подготовке к зачету необходимо ориентироваться на конспекты лекций, рекомендуемую литературу и др.

8. Информационные технологии, используемые при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

Тема (раздел) дисциплины	Образовательные и информационные технологии	Перечень программного обеспечения и информационных справочных систем
Основы использования программно-аппаратных средств для обеспечения информационной безопасности.	Лекции, мультимедиа, практические и лабораторные работы	https://biblio-online.ru http://znanium.com http://www.prospektnauki.ru http://elib.rshu.ru https://нэб.рф windows 7 office 2007 dr Web Программа оптимизации структуры защищенной компьютерной сети с применением генетического алгоритма №2016611252 Экспертная система выбора оптимальных средств защиты электронного контента №2016611251 Аппаратные ключи серий SENTINEL HASP, Guardant, eToken, ruToken.
Идентификация пользователей КС – субъектов доступа к данным	Лекции, мультимедиа, практические и лабораторные работы	
Средства и методы ограничения доступа к файлам	Лекции, мультимедиа, практические и лабораторные работы	
Особенности защиты данных от изменения. Программно-аппаратные средства шифрования	Лекции, мультимедиа, практические и лабораторные работы	
Построение программно-аппаратных комплексов шифрования	Лекции, мультимедиа, практические и лабораторные работы	
Методы и средства ограничения доступа к компонентам ЭВМ	Лекции, мультимедиа, практические и лабораторные работы	

Особенности защиты данных от изменения. Программно-аппаратные средства шифрования	Лекции, мультимедиа, практические и лабораторные работы	
Защита программ от изучения. Аппаратный ключ с точки зрения электроники.	Лекции, мультимедиа, практические и лабораторные работы	
Защита от разрушающих программных воздействий.	Лекции, мультимедиа, практические и лабораторные работы	

9. Особенности освоения дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

Обучение обучающихся с ограниченными возможностями здоровья при необходимости осуществляется на основе адаптированной рабочей программы с использованием специальных методов обучения и дидактических материалов, составленных с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся (обучающегося).

При определении формы проведения занятий с обучающимся-инвалидом учитываются рекомендации, содержащиеся в индивидуальной программе реабилитации инвалида, относительно рекомендованных условий и видов труда.

При необходимости для обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья создаются специальные рабочие места с учетом нарушенных функций и ограничений жизнедеятельности.

10. Материально-техническое обеспечение дисциплины

Учебная аудитории для проведения занятий лекционного типа – укомплектована специализированной (учебной) мебелью, набором демонстрационного оборудования и учебно-наглядными пособиями, обеспечивающими тематические иллюстрации, соответствующие рабочим учебным программам дисциплин (модулей).

Учебная аудитории для проведения занятий практического типа - укомплектована специализированной (учебной) мебелью,техническими средствами обучения, служащими для представления учебной информации.

Учебная аудитория для проведения занятий лабораторного типа - Учебная лаборатория Программно-аппаратных средств обеспечения информационной безопасности. Помещение оснащено: специализированной (учебной) мебелью, 15 компьютеров, антивирусными программными комплексами и аппаратными средствами аутентификации пользователя

Учебная аудитория для групповых и индивидуальных консультаций - укомплектована специализированной (учебной) мебелью, техническими

средствами обучения, служащими для представления учебной информации.

Учебная аудитория для текущего контроля и промежуточной аттестации - укомплектована специализированной (учебной) мебелью, техническими средствами обучения, служащими для представления учебной информации.

Помещение для хранения и профилактического обслуживания учебного оборудования – укомплектовано специализированной мебелью для хранения оборудования и техническими средствами для его обслуживания.

Рассмотрено и рекомендовано к использованию в учебном процессе на 2019/2020 учебный год без изменений.

Протокол заседания кафедры ИТиСБ от 07.05.2019 №5