МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное
учреждение высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

«СОГЛАСОВАНО»
Руководитель ОП

Варлатая С.К.
(подпись) (Ф.И.О.)

«УТВЕРЖДАЮ»
И.о. заведующего кафедрой
информационной безопасности
(название кафедры)

Добржинский Ю.В.
(подпись) (Ф.И.О.)

«15» июня 2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Программно-аппаратные средства защиты информации
Направление 10.03.01 Информационная безопасность
(Комплексная защита объектов информатизации)
Форма подготовки очная

курс 3 семестр 6
лекции 36 час.
практические занятия 18 час.
лабораторные работы 18 час.
в том числе с использованием МАО лек. 00 / пр. 00 / лаб. 00 час.
всего часов аудиторной нагрузки 72 час.
в том числе с использованием МАО 00 час.
самостоятельная работа 36 час.
в том числе на подготовку к экзамену 00 час.
контрольные работы (количество) не предусмотрены
курсовая работа / курсовой проект не предусмотрены
зачет 6 семестр
экзамен не предусмотрен

Рабочая программа составлена в соответствии с требованиями образовательного стандарта, самостоятельно устанавливаемого ДВФУ, утвержденного приказом ректора от 20.07.2017 №12-13-1479.

Рабочая программа обсуждена на заседании кафедры информационной безопасности
протокол № 10 от «15» июня 2019 г.

И.о. заведующего кафедрой: Добржинский Ю.В., с.н.с., к.т.н.
Составитель: Смирнов М.Е., ст. преподаватель

Владивосток
2019

Оборотная сторона титульного листа РПД

I. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «_____» _____ 20___ г. № _____

Заведующий кафедрой _____ _____
(подпись) (И.О. Фамилия)

II. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «_____» _____ 20___ г. № _____

Заведующий кафедрой _____ _____
(подпись) (И.О. Фамилия)

III. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «_____» _____ 20___ г. № _____

Заведующий кафедрой _____ _____
(подпись) (И.О. Фамилия)

IV. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «_____» _____ 20___ г. № _____

Заведующий кафедрой _____ _____
(подпись) (И.О. Фамилия)

Аннотация к рабочей программе дисциплины «Программно-аппаратные средства защиты информации»

Рабочая программа по курсу «Программно-аппаратные средства защиты информации» разработана для студентов по направлению 10.03.01 «Информационная безопасность» в соответствии с требованиями ФГОС ВО.

Общая трудоемкость освоения дисциплины составляет 108 часов (3 з.е.). Учебным планом предусмотрены лекционные занятия (36 часов), практические занятия (18 часов), лабораторные работы (18 часов) самостоятельная работа студентов (36 часов). Дисциплина «Программно-аппаратные средства защиты информации» реализуется на 3 курсе в 6 семестре. Форма контроля – зачет.

Цель: формирование основополагающих знаний по программному и аппаратному обеспечению информационной безопасности в области системного анализа и принятия решений.

Задачи:

- угроз информационной безопасности в автоматизированных системах обработки данных;

- принципов разделения доступа и защиты программ и данных от НСД;

- использования программно-аппаратных средств защиты информации;

- проектирования систем защиты информации в АСОД.

- изучение основных угроз безопасности информации в автоматизированных системах и освоение методов защиты от данных угроз;

- изучение методов, алгоритмов, программно-аппаратных средств обеспечения ин формационной безопасности автоматизированных систем;

- изучение основных мер по защите информации и программных продуктов от несанкционированного доступа, модификации и изучения в автоматизированных системах;

- изучение современных технологий защищенных сетей передачи данных в автоматизированных системах.

В результате изучения данной дисциплины у обучающихся формируются следующие общепрофессиональные и профессиональные компетенции.

Код и формулировка компетенции	**Этапы формирования компетенции**	
ПК-1 способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Знает	архитектуру и базовые принципы функционирования вычислительных систем, сетей и современных многозадачных многопользовательских операционных систем
	Умеет	развертывать и настраивать программные и аппаратные средства для защиты локальных и распределенных вычислительных систем
	Владеет	программно-аппаратными комплексами управления ключами, сертификатами и правами пользователей в защищенных автоматизированных системах
ПК-2 способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	Знает	виды, функции и требования к современным средствам программной и аппаратной аутентификации пользователей и программ в клиент-серверных приложениях
	Умеет	обеспечивать надежную аутентификацию и управление доступом к информационным ресурсам с учетом требований нормативно-технической документации
	Владеет	программно-аппаратными комплексами управления ключами, сертификатами и правами пользователей в защищенных автоматизированных системах
ПК-12 способностью проводить анализ информацио нной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	Знает	методы и программно-аппаратные средства защиты программного обеспечения от несанкционированного изучения, копирования и модификации
	Умеет	настраивать каналы безопасного обмена информацией в локальных и распределенных автоматизированных системах
	Владеет	программно-аппаратными комплексами управления ключами, сертификатами и правами пользователей в защищенных автоматизированных системах
ПК-15 способностью разрабатывать планы и программы проведения научных исследований и технических разработок	Знает	модульную структуру подсистемы безопасное™ современных операционных систем и способы интеграции средств защиты
	Умеет	настраивать системы обнаружения вторжений и антивирусные системы
	Владеет	программно-аппаратными комплексами управления ключами, сертификатами и правами пользователей в

		защищенных автоматизированных системах
ОПК-7способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Знает	методы и алгоритмы управления и генерации ключей и их аппаратно-программная реализация и применение в автоматизированных системах
	Умеет	настраивать системы предотвращения вторжений
	Владеет	инструментарием, обеспечивающим программно-аппаратную защиту информационных ресурсов от изучения, модификации и копирований
ПСК-3.2 способностью формировать предложения по оптимизации комплекса технических средств, применяемых в функциональном процессе защищаемого объекта и его информационных составляющих, с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы и предложения по тактике защиты объектов и локализации защищаемых элементов	Знает	организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации
	Умеет	разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации
	Владеет	методами формирования требований по защите информации
ПСК-3.3 способностью разрабатывать комплекс организационных и технических мер по обеспечению информационной безопасности объекта информатизации, проводить выбор необходимых технологий и технических средств, организовать внедрение и последующее сопровождение	Знает	комплекс организационных и технических мер по обеспечению информационной безопасности объекта информатизации
	Умеет	проводить выбор необходимых технологий и технических средств, организовать их внедрение
	Владеет	методами формирования требований по защите информации

Для формирования вышеуказанных компетенций в рамках дисциплины «Программно-аппаратные средства защиты информации» применяются

следующие методы активного/ интерактивного обучения: интерактивные и проблемные лекции, лекции-диалоги, работа в малых группах, метод обучения в парах. Используемые оценочные средства: собеседование (ОУ-1), коллоквиум (ОУ-2), лабораторные работы (ПР-6), конспект (ПР-7).

I. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА

МОДУЛЬ 1. Основы защиты информации и средства, методы защиты. (36час)

Раздел I. Основы защиты информации (18час.)

Тема 1 Основные понятия программно-аппаратной защиты информации **(6ч)**

Тема 2. Идентификация пользователей кс-субъектов доступа к данным **(6ч.)**

Тема 3. Средства и методы ограничения доступа к файлам **(3ч)**

Тема 4. Программно-аппаратные средства шифрования **(3ч)**

Раздел II. Средства и методы защиты (18ч)

Тема 1. Методы и средства ограничения доступа к компонентам ЭВМ **(6ч)**

Тема 2. Защита программ от несанкционированного копирования **(6ч)**

Тема 3. Хранение ключевой информации **(3ч.)**

Тема 4. Защита программ от изучения **(3ч)**

II. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА

Практические занятия (18 час.)

1. Основы использования средств защиты от несанкционированного доступа в операционной системе Linux **(4 ч)**
2. Система безопасности Windows XP **(4 ч)**

3. Антивирус Касперского 6.0 для Windows Workstations. Локальная установка и управление **(5 ч)**
4. Основные признаки присутствия вредоносных программ и методы по устранению последствий вирусных заражений **(5 ч)**

Лабораторные работы (18 час.)

Лабораторная работа №1. Система защиты информации Secret Net 6.0**(9ч)**

Цель: ознакомиться с особенностями системы защиты информации в программной среде Secret Net 6.0

Ход работы: устанавливаем программную среду на ПК, знакомимся с её особенностями

Лабораторная работа №2. Система защиты информации Dallas Lock 8.0-K**(6ч)**

Цель: ознакомиться с особенностями системы защиты информации в программной среде Dallas Lock 8.0-K

Ход работы: устанавливаем средство от НСД на ПК, знакомимся с особенностями

Лабораторная работа №3. Система защиты информации Dallas Lock 8.0-C**(3ч)**

Цель: ознакомиться с особенностями системы защиты информации Dallas Lock 8.0-C

Ход работы: устанавливаем средство от НСД на ПК, знакомимся с особенностями

III. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине «Программно-аппаратные средства защиты информации» представлено в Приложении 1 и включает в себя:

план-график выполнения самостоятельной работы по дисциплине, в том числе примерные нормы времени на выполнение по каждому заданию;

характеристика заданий для самостоятельной работы обучающихся и методические рекомендации по их выполнению;

требования к представлению и оформлению результатов самостоятельной работы;

критерии оценки выполнения самостоятельной работы.

IV. КОНТРОЛЬ ДОСТИЖЕНИЯ ЦЕЛЕЙ КУРСА

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства - наименование	
				текущий контроль	промежуточная аттестация
1	Раздел I. Основы защиты информации.	ОПК-7 ПК-1 ПК-2 ПК-12 ПК-15 ПСК-3.2 ПСК-3.3	Знает	ТС-1	1-25
			Умеет	ТС-1	1-25
			Владеет	ТС-1	1-25
2	Раздел II. Средства и методы защиты.	ОПК-7 ПК-1 ПК-2 ПК-12 ПК-15 ПСК-3.2 ПСК-3.3	Знает	ТС-1	26-50
			Умеет	ТС-1	26-50
			Владеет	ТС-1	26-50

Типовые контрольные задания, методические материалы, определяющие процедуры оценивания знаний, умений и навыков и опыта деятельности, а также критерии и показатели, необходимые для оценки знаний, умений, навыков и характеризующие этапы формирования компетенций в процессе освоения образовательной программы, представлены в Приложении 2.

V. СПИСОК УЧЕБНОЙ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература

1. Программно-аппаратные средства защиты информации : учебник для вузов / В. В. Платонов,

Москва: Академия, 2013, 331 с. http://lib.dvfu.ru:8080/lib/item?id=chamo:692876&theme=FEFU

2. Аппаратные и программные средства защиты информации: Учебное пособие / Душкин А.В., Кольцов А., Кравченко А. - Воронеж:Научная книга, 2016. - 232 с. ISBN 978-5-4446-0746-6 - Режим доступа: http://znanium.com/catalog/product/923168

3. Технологии защиты информации в компьютерных сетях [Электронный ресурс]/ Н.А. Руденков [и др.].— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 368 с.— Режим доступа: http://www.iprbookshop.ru/73732.html.— ЭБС «IPRbooks»

4. 1. Варлатая С.К., Шаханова М.В. Аппаратно-программные средства и методы защиты информации : учебное пособие для вузов/ С.К. Варлатая, М.В. Шаханова – Владивосток : Изд-во Дальневосточного технического университета, 2007. – 276 с. – Режим доступа: http://lib.dvfu.ru:8080/lib/item?id=chamo:386993&theme=FEFU

Дополнительная литература

1. Каторин Ю.Ф. Техническая защита информации [Электронный ресурс]: лабораторный практикум/ Каторин Ю.Ф., Разумовский А.В., Спивак А.И.— Электрон. текстовые данные.— СПб.: Университет ИТМО, 2013.— 113 с.— Режим доступа: http://www.iprbookshop.ru/68715.html.— ЭБС «IPRbooks»

2. Титов А.А. Инженерно-техническая защита информации [Электронный ресурс]: учебное пособие/ Титов А.А.— Электрон. текстовые данные.— Томск: Томский государственный университет систем управления и

радиоэлектроники, 2010.— 197 с.— Режим доступа: http://www.iprbookshop.ru/13931.html.— ЭБС «IPRbooks»

3. Голиков А.М. Защита информации от утечки по техническим каналам [Электронный ресурс]: учебное пособие/ Голиков А.М.— Электрон. текстовые данные.— Томск: Томский государственный университет систем управления и радиоэлектроники, 2015.— 256 с.— Режим доступа: http://www.iprbookshop.ru/72090.html.— ЭБС «IPRbooks»

Перечень информационных технологий и программного обеспечения

Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 318, Компьютерный класс кафедры информационной безопасности, аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	1) IBM SPSS Statistics Premium Campus Edition. Поставщик ЗАО Прогностические решения. Договор ЭА-442-15 от 18.01.16 лот 5. Срок действия договора 30.06.2016. Лицензия бессрочно. 2) SolidWorks Campus 500. Поставщик Солид Воркс Р. Договор 15-04-101 от 23.12.2015. Срок действия договора 15.03.2016. Лицензия бессрочно. 3) АСКОН Компас 3D v17. Поставщик Навиком. Договор 15-03-53 от 20.12.2015. Срок действия договора 31.12.2015. Лицензия бессрочно. 4) MathCad Education Universety Edition. Поставщик Софт Лайн Трейд. Договор 15-03-49 от 02.12.2015. Срок действия договора 30.11.2015. Лицензия бессрочно. 5) Corel Academic Site. Поставщик Софт Лайн Трейд. Договор ЭА-442-15 от 18.01.16 лот 4. Срок действия договора 30.06.2016. Лицензия закончилась 28.01.2019. 6) Microsoft Office, Microsoft Visual Studio. Поставщик Софт Лайн Трейд. Договор ЭА-261-18 от 02.08.18 лот 4. Срок действия договора 20.09.2018. Лицензия до 30.06.2020 7) Dallas Lock. Поставщик Конфидент. Партнерское соглашение БП-8-16/576-16-ЦЗ/1 от 23.11.2016. Срок действия договора 23.11.2019. Лицензия до 23.11.2019
Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 546, Компьютерный класс кафедры информационной безопасности, аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных	1) IBM SPSS Statistics Premium Campus Edition. Поставщик ЗАО Прогностические решения. Договор ЭА-442-15 от 18.01.16 лот 5. Срок действия договора 30.06.2016. Лицензия бессрочно. 2) SolidWorks Campus 500. Поставщик Солид Воркс Р. Договор 15-04-101 от 23.12.2015. Срок действия договора 15.03.2016. Лицензия бессрочно. 3) АСКОН Компас 3D v17. Поставщик Навиком. Договор 15-03-53 от 20.12.2015. Срок действия договора 31.12.2015. Лицензия бессрочно. 4) MathCad Education Universety Edition. Поставщик Софт Лайн Трейд. Договор 15-03-49 от 02.12.2015. Срок действия договора 30.11.2015. Лицензия бессрочно. 5) Corel Academic Site. Поставщик Софт Лайн Трейд.

консультаций, текущего контроля и промежуточной аттестации.	Договор ЭА-442-15 от 18.01.16 лот 4. Срок действия договора 30.06.2016. Лицензия закончилась 28.01.2019. 6) Microsoft Office, Microsoft Visual Studio. Поставщик Софт Лайн Трейд. Договор ЭА-261-18 от 02.08.18 лот 4. Срок действия договора 20.09.2018. Лицензия до 30.06.2020.

VI. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Для более эффективного освоения и усвоения материала рекомендуется ознакомиться с теоретическим материалом по той или иной теме до проведения семинарского занятия. Работу с теоретическим материалом по теме с использованием учебника или конспекта лекций можно проводить по следующей схеме:

- название темы;
- цели и задачи изучения темы;
- основные вопросы темы;
- характеристика основных понятий и определений, необходимых для усвоения данной темы;
- список рекомендуемой литературы;
- наиболее важные фрагменты текстов рекомендуемых источников, в том числе таблицы, рисунки, схемы и т.п.;
- краткие выводы, ориентирующие на определенную совокупность сведений, основных идей, ключевых положений, систему доказательств, которые необходимо усвоить.

В ходе работы над теоретическим материалом достигается:

- понимание понятийного аппарата рассматриваемой темы;
- воспроизведение фактического материала;
- раскрытие причинно-следственных, временных и других связей;
- обобщение и систематизация знаний по теме.

При подготовке к экзамену рекомендуется проработать вопросы, рассмотренные на лекционных и практических занятиях и представленные в рабочей программе, используя основную литературу, дополнительную литературу и интернет-ресурсы.

VII. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 318, Компьютерный класс кафедры информационной безопасности, аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	Помещение укомплектовано специализированной учебной мебелью (посадочных мест – 15) Оборудование: Моноблок HPP-B0G08ES#ACB/8200E AIO i52400S 500G 4.0G 28 PC Электронная доска Poly Vision Walk-and-Talk WTL 1810 Мультимедийная аудитория: Экран проекционный ScreenLine Trim White Ice 50 см черная кайма сверху, размер рабочей области 236x147 см Документ-камера Avervision CP355AF ЖК-панель 47", Full HD, LG M4716 CCBA Мультимедийный проектор Mitsubishi EW33OU, 3000 ANSI Lumen, 1280x800 Сетевая видеокамера Multipix MP-HD718 Доска аудиторная
Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 546, Компьютерный класс кафедры информационной безопасности, аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	Помещение укомплектовано специализированной учебной мебелью (посадочных мест – 15) Оборудование: "Компьютер (твердотельный диск - объемом 128 ГБ; жесткий диск - объем 1000 ГБ; форм-фактор - Tower; комплектуется клавиатурой, мышью, монитором AOC i2757Fm; комплектом шнуров эл. питания) модель - M93p 1 Мультимедийное оборудование: Экран проекционный ScreenLine Trim White Ice 50 см черная кайма сверху, размер рабочей области 236x147 см Документ-камера Avervision CP355AF ЖК-панель 47"", Full HD, LG M4716 CCBA Мультимедийный проектор, Mitsubishi EW33OU, 3000 ANSI Lumen, 1280x800 Сетевая видеокамера Multipix MP-HD718" Доска аудиторная

Приложение 1 к рабочей программе учебной дисциплины

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

по дисциплине «Программно-аппаратные средства защиты информации»
Направление подготовки 10.03.01 «Информационная безопасность»
Профиль подготовки - «Комплексная защита объектов информатизации»
Форма подготовки - очная

Владивосток
2019

План-график выполнения самостоятельной работы по дисциплине

№ п/п	Дата/сроки выполнения	Вид самостоятельной работы	Примерные нормы времени на выполнение	Форма контроля
1	5 неделя	Ознакомится с основными функциями Secret Net 6.0	9	ТС-1
2	12 неделя	Зачет	27	УО-1

Самостоятельная работа студентов включает:

– освоение лекционного материала;

– выполнение индивидуального домашнего задания;

– оформление выполненного индивидуального домашнего задания;

– подготовку к защите выполненного индивидуального домашнего задания.

Приложение 2 к рабочей программе учебной дисциплины

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине «Программно-аппаратные средства защиты информации»
Направление подготовки 10.03.01 «Информационная безопасность»
Профиль подготовки - «Комплексная защита объектов информатизации»
Форма подготовки - очная

Владивосток
2019

Обучающиеся должны выполнять индивидуальные задания. Задания должны быть выполнены в процессе изучения соответствующего раздела курса. При выполнении заданий возможно использование учебно-методической литературы и электронных лекций курса.

Вопросы к экзамену.

1. Структура КС.
2. Идентификация пользователей КС.
3. Шифрование.
4. Контроль доступа.
5. Иерархический доступ к файлам.
6. Фиксация доступа к файлам.
7. Особенности защиты данных от изменения.
8. Программно-аппаратные средства шифрования.
9. Компоненты ПЭВМ.
10. Несанкционированное копирование программ.
11. Хранение ключевой информации.
12. Идентификация субъекта
13. Идентифицирующая информация
14. Понятие защищённой системы
15. Правила разграничения доступа
16. Модели ОС. Сравнительный анализ ОС
17. Избирательное разграничение доступа
18. Изолированная программная среда
19. Полномочное разграничение доступа без контроля информационных потоков
20. Полномочное разграничение доступа
21. Матрица доступа и вектор доступа
22. Обеспечение конфиденциальности (правила NRU и NWD)
23. Критерии информационной безопасности

24. Технология ЭЦП
25. Понятие “лобовой атаки”, методы формирования паролей
26. Методы борьбы с подбором идентифицирующей информации
27. Методы борьбы с подбором паролей, полученных на основе ошибок администратора
28. Методы борьбы с подбором паролей, полученных на основе ошибок реализации
29. Социальная психология и иные способы получения паролей
30. Принципы построения криптосистем
31. Уровни криптосистем
32. Компоненты Криптосистем
33. Функции Криптосистем
34. Методы получения “случайности”
35. Принципы построения генераторов ПСП и ИСП.
36. Архивация. Алгоритмы архивации
37. Генерация ключей. Распределение ключей. Главный ключ.
38. Восстановление системы при компрометации ключей
39. Классификация криптоалгоритмов
40. Симметричные криптоалгоритмы
41. Асимметричные криптоалгоритмы
42. Технология Хэш-функций
43. Противодействие изучению исходных текстов
44. Противодействие анализу двоичного кода
45. Защита от РПВ
46. Классификация РПВ
47. Методы и средства защиты информации от технических сбоев, поломок, стихийных бедствий
48. Понятие избыточности
49. Принципы функционирования систем в чрезвычайных условиях.
50. Восстановление работоспособности систем