Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Комсомольский-на-Амуре государственный университет»

УТВЕРЖДАЮ

Декан
факультета компьютерных технологий
(наименование факультета)
Я.Ю. Григорьев
(подпись, ФИО)
«07» 05 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Программно-аппаратные средства защиты информации

Направление подготовки	*10.05.03 "Информационная безопасность автоматизированных систем"*
Направленность (профиль) образовательной программы	*Анализ безопасности информационных систем*
Квалификация выпускника	*специалист по защите информации*
Год начала подготовки *(по учебному плану)*	*2021*
Форма обучения	*очная*
Технология обучения	*традиционная*

Курс	Семестр	Трудоемкость, з.е.
4	*8*	*4*

Вид промежуточной аттестации	Обеспечивающее подразделение
Зач_с_оц	*Кафедра ИБАС - Информационная безопасность автоматизированных систем*

Комсомольск-на-Амуре 2021

Разработчик рабочей программы:

доцент, к.т.н. _____ _____
(должность, степень, ученое звание) (подпись) (ФИО)

СОГЛАСОВАНО:

Заведующий кафедрой

ИБАС _____ _____
(наименование кафедры) (подпись) (ФИО)

1 Общие положения

Рабочая программа дисциплины «Программно-аппаратные средства защиты информации» составлена в соответствии с требованиями федерального государственного образовательного стандарта, утвержденного приказом Министерства науки и высшего образования Российской Федерации № 1457 от 26.11.2020, и основной профессиональной образовательной программы подготовки «Анализ безопасности информационных систем» по специальности 10.05.03 "Информационная безопасность автоматизированных систем".

Практическая подготовка реализуется на основе:

Профессиональный стандарт утвержденного приказом Министерства труда и социальной защиты от 15 сентября 2016 года N 522н №843 "Специалист по защите информации в автоматизированных системах" зарегистрированного в Министерстве юстиции Российской Федерации 28 сентября 2016 года, регистрационный N 43857. Обобщенные трудовые функции: A/03.5 Обеспечение защиты информации при выводе из эксплуатации автоматизированных систем, D/04.7 Разработка программных и программно-аппаратных средств для систем защиты информации автоматизированных систем, B/01.6 Диагностика систем защиты информации автоматизированных систем.

Задачи дисциплины	дать представление о методах и средствах защиты информации в компьютерных системах; о защитных механизмах, реализованных в средствах защиты компьютерных систем от несанкционированного доступа (НСД); о современных программно-аппаратных комплексах защиты информации; о применении средств криптографической защиты информации и средств защиты от НСД для решения задач обеспечения информационной безопасности.
Основные разделы / темы дисциплины	1. Применение СЗИ от НСД для организации защищенных компьютерных систем. Применение средств организации виртуальных частных сетей. 2. Защита программ от изучения, способы встраивания и защиты ПО Методы и средства ограничения доступа к компонентам вычислительных систем

2 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами образовательной программы

Процесс изучения дисциплины «Программно-аппаратные средства защиты информации» направлен на формирование следующих компетенций в соответствии с ФГОС ВО и основной образовательной программой (таблица 1):

Таблица 1 – Компетенции и планируемые результаты обучения по дисциплине

Код и наименование компетенции	Индикаторы достижения	Планируемые результаты обучения по дисциплине
Общепрофессиональные		
ОПК-11 Способен разрабатывать компоненты систем защиты информации автоматизированных систем	**ОПК-11.1 З**нает программно-аппаратные средства, используемые в качестве компонентов систем защиты информации в программном обеспечении автоматизированных систем; методы проектирования решений по обеспечению безопасности	**З**нает программно-аппаратные средства, используемые в качестве компонентов систем защиты информации в программном обеспечении автоматизированных систем

	автоматизированных систем	
	ОПК-11.2 Умеет проектировать защищенные распределенные информационные системы и компоненты систем защиты информации автоматизированных систем	Умеет проектировать компоненты систем защиты информации автоматизированных систем
	ОПК-11.3 Владеет навыками разработки компонентов систем защиты информации автоматизированных систем и защищенных распределенные информационные системы	Владеет навыками разработки компонентов систем защиты информации автоматизированных систем и защищенных распределенные информационные системы
ОПК-7.1. Способен использовать программные и программно-аппаратные средства для моделирования и испытания систем защиты информационных систем	**ОПК-7.1..1** Знает программные и программно-аппаратные средства для моделирования и испытания систем защиты информационных систем; методы применения программных и программно-аппаратных средств для моделирования и испытания систем защиты информационных систем	Знает программные и программно-аппаратные средства для моделирования и испытания систем защиты информационных систем; методы применения программных и программно-аппаратных средств для моделирования и испытания систем защиты информационных систем
	ОПК-7.1..2 Умеет выбирать программные и программно-аппаратные средства для моделирования и испытания систем защиты информационных систем	Умеет выбирать программные и программно-аппаратные средства для моделирования и испытания систем защиты информационных систем
	ОПК-7.1..3 Владеет навыками применения программных и программно-аппаратных средств для моделирования и испытания систем защиты информационных систем	Владеет навыками применения программных и программно-аппаратных средств для моделирования и испытания систем защиты информационных систем

3 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина(модуль) «Программно-аппаратные средства защиты информации» изучается на 4 курсе в 8 семестре.

Дисциплина является базовой дисциплиной, входит в состав блока 1 «Дисциплины (модули)» и относится к обязательным дисциплинам.

Для освоения дисциплины необходимы знания, умения, навыки и (или) опыт практической деятельности, сформированные в процессе изучения дисциплин / практик: разработка и эксплуатация автоматизированных систем в защищенном исполнении.

Знания, умения и навыки, сформированные при изучении дисциплины «Программно-аппаратные средства защиты информации», будут востребованы при изучении последующих дисциплин защита от хакерских угроз, системы интеллектуальной защиты информации, подготовка к сдаче и сдача государственного экзамена, подготовка к процедуре защиты и защита выпускной квалификационной работы.

Дисциплина «Программно-аппаратные средства защиты информации»» в рамках воспитательной работы направлена на развитие творчества, профессиональных умений, ответственности за выполнение учебно-производственных заданий.

4 Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

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

Распределение объема дисциплины (модуля) по видам учебных занятий представлено в таблице 2.

Таблица 2 – Объем дисциплины (модуля) по видам учебных занятий

Объем дисциплины	**Всего академических часов**
Общая трудоемкость дисциплины	144
Контактная аудиторная работа обучающихся с преподавателем (по видам учебных занятий), всего	64
В том числе:	
занятия лекционного типа (лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации педагогическими работниками)	32
занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия)	64
Самостоятельная работа обучающихся и контактная работа, включающая групповые консультации, индивидуальную работу обучающихся с преподавателями (в том числе индивидуальные консультации); взаимодействие в электронной информационно-образовательной среде вуза	48
Промежуточная аттестация обучающихся – Зач_с_оц	

5 Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебной работы

Таблица 3 – Структура и содержание дисциплины (модуля)

Наименование разделов, тем и содержание материала	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)			
	Контактная работа преподавателя с обучающимися			СРС
	Лекции	Семинарские (практические занятия)	Лабораторные занятия	

Наименование разделов, тем и содержание материала	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)			
	Контактная работа преподавателя с обучающимися			СРС
	Лекции	Семинарские (практические занятия)	Лабораторные занятия	
Раздел 1 Применение СЗИ от НСД для организации защищенных компьютерных систем. Применение средств организации виртуальных частных сетей НСД к информации. Виды и способы. Современные вызовы информационной безопасности. Существующие средства защиты информации в соответствии с требованиями ФСБ и ФСТЭК РФ. Изменение настроек сервиса PGPkeys. Шифрование и обмен шифрованной информацией. Система защиты конфиденциальной информации «StrongDisk». Основные характеристики системы. Классификация и общие характеристики СЗИ НСД. Инициализация системы. Создание защищенных логических дисков. Настройка параметров. Система защиты корпоративной информации «Secret Disk». Основные характеристики Создание защищенных логических дисков. Работа с защищенными дисками. Настройка параметров СКЗИ. Управление секретными дисками. Хранение конфиденциальной информации на съемных носителях. Администрирование. Изучение средства ФИКС, Изучение средства Терьер, Изучение средств Ревизор 1 XP и Ревизор 2 XP Использование специализированных аппаратно-программных средств защиты информации (СЗИ) Назначение и возможности СЗИ от НСД, требования, предъявляемые к ним. Контроль целостности. Печать штампа. Регистрация событий. Гарантированное удаление данных. Реализация запрета загрузки ПЭВМ в обход СЗИ. Применение СЗИ от НСД «Secret NET». Установка и регистрация в системе защиты. Создание учетных записей. Реализация дискреционной и мандатной	16		32 (8*)	24

Наименование разделов, тем и содержание материала	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)			
	Контактная работа преподавателя с обучающимися			СРС
	Лекции	Семинарские (практические занятия)	Лабораторные занятия	
моделей разграничения доступа. Обеспечение замкнутости программной среды. Контроль целостности. Регистрация событий. Гарантированное удаление данных. Настройка механизма шифрования. Реализация в СЗИ ограничения на вход в систему и политики разграничения доступа. Контроль технологического мусора. Обзор современных отечественных средств защиты информации. Установка и регистрация в системе защиты. Создание учетных записей. Реализация дискреционной и мандатной моделей разграничения доступа. Обеспечение замкнутости программной среды. Контроль целостности. Печать штампа. Регистрация событий. Гарантированное удаление данных. Применение СЗИ от НСД «Страж-NT». Создание учетных записей. Реализация дискреционной и мандатной моделей разграничения доступа. Обеспечение замкнутости программной среды. Контроль целостности. Организация учета сменных носителей информации. Регистрация событий. Гарантированное удаление данных. Применение СЗИ от НСД «Dallas Lock». Задачи, решаемые VPN. Туннелирование в VPN. Уровни защищенных каналов. Защита данных на канальном уровне. Организация VPN средствами протокола PPTP. Установка и настройка VPN. Анализ защищенности передаваемой информации. Защита данных на сетевом уровне. Протокол SKIP. Протокол IPSec. Организация VPN средствами СЗИ «VipNet». Использование протокола IPSec для защиты сетей. Шифрование трафика с использованием протокола IPSec. Настройка политики межсетевого экранирования с использованием				

Наименование разделов, тем и содержание материала	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)			
	Контактная работа преподавателя с обучающимися			СРС
	Лекции	Семинарские (практические занятия)	Лабораторные занятия	
протокола IPSec. Организация VPN средствами СЗИ «StrongNet». Описание системы. Генерация и распространение ключевой информации. Настройка СЗИ «StrongNet». Установка защищенного соединения. Настройка подсистем защиты Secret Net. Настройка подсистем защиты Dallas Lock; Настройка подсистем защиты Страж NT				
Раздел 2 Защита программ от изучения, способы встраивания и защиты ПО. Методы и средства ограничения доступа к компонентам вычислительных систем. Угрозы безопасности программного обеспечения разрушающие программные средства. Несанкционированное копирование, распространение и использование программ. Модели угроз безопасности программного обеспечения. Подходы к созданию модели угроз технологической безопасности ПО. Элементы модели угроз эксплуатационной безопасности ПО. Модель разрушающего программного средства. Самотестирующиеся и самокорректирующиеся программы. Подходы к защите разрабатываемых программ от автоматической генерации инструментальными средствами программных закладок АПМДЗ Соболь Защита с использованием АПМДЗ Аккорд Дизассемблеры и отладчики. Основные подходы к защите данных от НСД Шифрование. Контроль доступа. Разграничения доступа. Файл как объект доступа. Оценка надежности систем ограничения доступа – сведение к задаче оценки стойкости. Иерархический доступ к файлам Понятие атрибутов доступа. Организация	16		32 (8*)	24

Наименование разделов, тем и содержание материала	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)			
	Контактная работа преподавателя с обучающимися			СРС
	Лекции	Семинарские (практические занятия)	Лабораторные занятия	
доступа к файлам в различных ОС. Защита сетевого файлового ресурса на примерах организации доступа в ОС UNIX, Novell NetWare. Фиксация доступа к файлам. Способы фиксации фактов доступа. Журналы доступа. Критерии информативности журналов доступа. Выявление следов несанкционированного доступа к файлам, метод инициированного НСД. Доступ к данным со стороны процесса. Понятие доступа к данным со стороны процесса: отличия от доступа со стороны пользователя. Понятие и примеры скрытого доступа. Надежность систем ограничения доступа.Особенности защиты данных от изменения. Защита массивов информации от изменения (имитозащита). Криптографическая постановка защиты от изменения данных. Подходы к решению задачи защиты данных от изменения. Подход на основе формирования имитоприставки (МАС), способы построения МАС. Подход на основе формирования хэш-функции, требования к построению и способы реализации. Формирование электронной цифровой подписи (ЭЦП).Особенности защиты ЭД и исполняемых файлов. Проблема самоконтроля исполняемых модулей. Компоненты систем защиты информации Аппаратные модули систем защиты информации Методы и способы анализа автоматизированных систем на наличие уязвимостей. Изучение Secret Net Studio.				
ИТОГО	**32**		**64**	**48**

Наименование разделов, тем и содержание материала	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)			
	Контактная работа преподавателя с обучающимися			СРС
	Лекции	Семинарские (практические занятия)	Лабораторные занятия	
по дисциплине				

* реализуется в форме практической подготовки

6 Внеаудиторная самостоятельная работа обучающихся по дисциплине (модулю)

При планировании самостоятельной работы студенту рекомендуется руководствоваться следующим распределением часов на самостоятельную работу (таблица 4):

Таблица 4 – Рекомендуемое распределение часов на самостоятельную работу

Компоненты самостоятельной работы	Количество часов
Изучение теоретических разделов дисциплины	4
Подготовка к занятиям семинарского типа	4
Подготовка и оформление Контр.	40
Всего	48

7 Оценочные средства для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине (модулю)

Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации представлен в Приложении 1.

Полный комплект контрольных заданий или иных материалов, необходимых для оценивания результатов обучения по дисциплине (модулю), практике хранится на кафедре-разработчике в бумажном и электронном виде.

8 Учебно-методическое и информационное обеспечение дисциплины (модуля)

8.1 Основная литература

1. Челухин, В.А. Комплексное обеспечение информационной безопасности автоматизированных систем: Учебное пособие для вузов / В. А. Челухин. - Комсомольск-на-Амуре: Изд-во Комсомольского-на-Амуре гос.техн.ун-та, 2014. - 207с. - Библиогр.: с.201-207. - 273-00.

2. Программно-аппаратная защита информации: Учебное пособие / Хорев П.Б., - М.:Форум, НИЦ ИНФРА-М, 2014. - 352 с.: 60x90 1/16. - (Высшее образование) ISBN 978-5-00091-004-7 - Режим доступа: http://znanium.com/catalog/product/489084

3. 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

4. Аппаратно-программные средства защиты информации: Практикум / Душкин А.В., Дубровин А.С., Здольник В.В. - Воронеж:Научная книга, 2017. - 198 с.: ISBN 978-5-4446-1043-5 - Режим доступа: http://znanium.com/catalog/product/977192

8.2 Дополнительная литература

1. Новиков С.Н. Методы защиты информации [Электронный ресурс] : учебное пособие / С.Н. Новиков, О.И. Солонская. — Электрон. текстовые данные. — Новосибирск: Сибирский государственный университет телекоммуникаций и информатики, 2009. — 121 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/54767.html

2. Информационная безопасность и защита информации [Электронный ресурс] : учебно-методический комплекс / . — Электрон. текстовые данные. — Алматы: Нур-Принт, 2012. — 98 с. — 9965-756-05-8. — Режим доступа: http://www.iprbookshop.ru/67055.html

3. Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс] / В.Ф. Шаньгин. — Электрон. текстовые данные. — Саратов: Профобразование, 2017. — 702 с. — 978-5-4488-0070-2. — Режим доступа: http://www.iprbookshop.ru/63594.html

4. Система защиты информации от несанкционированного доступа «СТРАЖ NT». Версия 2.0. Описание применения. – 53 с. (прилагается на компакт диске с программным обеспечением, хранится на факультете компьютерных технологий)

5. Система защиты информации от несанкционированного доступа «Dallas Lock 8.0». Руководство по эксплуатации. – 88 с. (прилагается на компакт диске с программным обеспечением, хранится на факультете компьютерных технологий)

6. Система защиты информации «Secret Net 7». Автономный вариант для Windows 2000. Руководство по администрированию. – 142 с. (прилагается на компакт диске с программным обеспечением, хранится на факультете компьютерных технологий)

7. Трещев И.А. Программно-аппаратные средства обеспечения информационной безопасности : Для студентов / Издательские решения, 2020. — 104 с. ISBN 978-5-4496-0764-5

8. Трещев И.А. Программно-аппаратные средства обеспечения информационной безопасности. Часть вторая : Для студентов технических специальностей / Издательские решения, 2020. — 162 с. ISBN 978-5-4496-3210-4 (т. 2) ISBN 978-5-4496-3211-1

8.3 Методические указания для студентов по освоению дисциплины

Обучение дисциплине «Программно-аппаратные средства обеспечения информационной безопасности» предполагает изучение курса на аудиторных занятиях и в ходе самостоятельной работы. Аудиторные занятия проводятся в форме лекций и лабораторных занятий..

Таблица 7 Методические указания к отдельным видам деятельности

Вид учебного занятия	Организация деятельности студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения. Выделять ключевые слова, формулы, отмечать на полях уточняющие вопросы по теме занятия
Лабораторные занятие	Работа с автоматизированными рабочими местами.
Самостоятельная работа	Для более глубокого изучения разделов дисциплины предусмотрены отдельные виды самостоятельной работы: подготовка к лабораторным занятиям, изучение теоретических разделов дисциплины,

	подготовка контрольной работы.

Самостоятельная работа является наиболее продуктивной формой образовательной и познавательной деятельности студента в период обучения. СРС направлена на углубление и закрепление знаний студента, развитие практических умений. СРС по дисциплине «Программно-аппаратные средства обеспечения информационной безопасности» включает следующие виды работ:

– работу с лекционным материалом, поиск и обзор литературы и электронных источников информации по индивидуальному заданию;

– опережающую самостоятельную работу;

– изучение тем, вынесенных на самостоятельную проработку;

– подготовку к практическим занятиям;

– выполнение и оформление контрольной работы.

Контроль самостоятельной работы студентов и качество освоения дисциплины осуществляется посредством:

– представления в указанные контрольные сроки результатов выполнения заданий для текущего контроля;

– выполнения и защиты контрольной работы;

Контрольная работа должна быть оформлены в соответствии с требованиями внутренних нормативных документов ФГБОУ ВО КнАГУ.

8.4 Современные профессиональные базы данных и информационные справочные системы, используемые при осуществлении образовательного процесса по дисциплине

1. Электронно-библиотечная система ZNANIUM.COM – **Ошибка! Недопустимый объект гиперссылки.**.
2. Консультант+

8.5 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

1. Научная электронная библиотека Elibrary **http://elibrary.ru**.

С целью повышения качества ведения образовательной деятельности в университете создана электронная информационно-образовательная среда. Она подразумевает организацию взаимодействия между обучающимися и преподавателями через систему личных кабинетов студентов, расположенных на официальном сайте университета в информационно-телекоммуникационной сети «Интернет» по адресу https://student.knastu.ru. Созданная информационно-образовательная среда позволяет осуществлять взаимодействие между участниками образовательного процесса посредством организации дистанционного консультирования по вопросам выполнения практических заданий.

8.6 Лицензионное программное обеспечение, используемое при осуществлении образовательного процесса по дисциплине

В ходе изучения дисциплины используется специализированная лаборатория программно-аппаратных средств обеспечения информационной безопасности оснащенная необходимыми средствами защиты от несанкционированного доступа и средствами контроля защищенности.

Таблица 5 – Перечень используемого программного обеспечения

Наименование ПО	Реквизиты
Microsoft® Windows Professional 7 Russian	Лицензионный сертификат № 46243844 от 09.12.2009
Open Office или аналог	Свободно-распространяемое
Обозреватель Google Chrome или аналог	Свободно-распространяемое

9 Организационно-педагогические условия

Организация образовательного процесса регламентируется учебным планом и расписанием учебных занятий. Язык обучения (преподавания) — русский. Для всех видов аудиторных занятий академический час устанавливается продолжительностью 45 минут.

При формировании своей индивидуальной образовательной траектории обучающийся имеет право на перезачет соответствующих дисциплин и профессиональных модулей, освоенных в процессе предшествующего обучения, который освобождает обучающегося от необходимости их повторного освоения.

9.1 Образовательные технологии

Учебный процесс при преподавании курса основывается на использовании традиционных, инновационных и информационных образовательных технологий. Традиционные образовательные технологии представлены лекциями и семинарскими (практическими) занятиями. Инновационные образовательные технологии используются в виде широкого применения активных и интерактивных форм проведения занятий. Информационные образовательные технологии реализуются путем активизации самостоятельной работы студентов в информационной образовательной среде.

9.2 Занятия лекционного типа

Лекционный курс предполагает систематизированное изложение основных вопросов учебного плана.

На первой лекции лектор обязан предупредить студентов, применительно к какому базовому учебнику (учебникам, учебным пособиям) будет прочитан курс.

Лекционный курс должен давать наибольший объем информации и обеспечивать более глубокое понимание учебных вопросов при значительно меньшей затрате времени, чем это требуется большинству студентов на самостоятельное изучение материала.

9.3 Занятия семинарского типа

Семинарские занятия представляют собой детализацию лекционного теоретического материала, проводятся в целях закрепления курса и охватывают все основные разделы.

Основной формой проведения семинаров является обсуждение наиболее проблемных и сложных вопросов по отдельным темам, а также разбор примеров и ситуаций в аудиторных условиях. В обязанности преподавателя входят: оказание методической помощи и консультирование студентов по соответствующим темам курса.

Активность на семинарских занятиях оценивается по следующим критериям:

- ответы на вопросы, предлагаемые преподавателем;
- участие в дискуссиях;
- выполнение проектных и иных заданий;
- ассистирование преподавателю в проведении занятий.

Ответ должен быть аргументированным, развернутым, не односложным, содержать ссылки на источники.

Доклады и оппонирование докладов проверяют степень владения теоретическим материалом, а также корректность и строгость рассуждений.

Оценивание заданий, выполненных на семинарском занятии, входит в накопленную оценку.

9.4 Самостоятельная работа обучающихся по дисциплине (модулю)

Самостоятельная работа студентов – это процесс активного, целенаправленного приобретения студентом новых знаний, умений без непосредственного участия преподавателя, характеризующийся предметной направленностью, эффективным контролем и оценкой результатов деятельности обучающегося.

Цели самостоятельной работы:

· систематизация и закрепление полученных теоретических знаний и практических умений студентов;

· углубление и расширение теоретических знаний;

· формирование умений использовать нормативную и справочную документацию, специальную литературу;

· развитие познавательных способностей, активности студентов, ответственности и организованности;

· формирование самостоятельности мышления, творческой инициативы, способностей к саморазвитию, самосовершенствованию и самореализации;

· развитие исследовательских умений и академических навыков.

Самостоятельная работа может осуществляться индивидуально или группами студентов в зависимости от цели, объема, уровня сложности, конкретной тематики.

Технология организации самостоятельной работы студентов включает использование информационных и материально-технических ресурсов университета.

Контроль результатов внеаудиторной самостоятельной работы студентов может проходить в письменной, устной или смешанной форме.

Студенты должны подходить к самостоятельной работе как к наиважнейшему средству закрепления и развития теоретических знаний, выработке единства взглядов на отдельные вопросы курса, приобретения определенных навыков и использования профессиональной литературы.

В данной дисциплине в рамках самостоятельной работы студенты выполняют одну расчетно-графическую работу состоящую из двух частей.

9.5 Методические указания для обучающихся по освоению дисциплины

При изучении дисциплины обучающимся целесообразно выполнять следующие рекомендации:

1. Изучение учебной дисциплины должно вестись систематически.

2. После изучения какого-либо раздела по учебнику или конспектным материалам рекомендуется по памяти воспроизвести основные термины, определения, понятия раздела.

3. Особое внимание следует уделить выполнению отчетов по практическим занятиям и индивидуальным комплексным заданиям на самостоятельную работу.

4. Вся тематика вопросов, изучаемых самостоятельно, задается на лекциях преподавателем. Им же даются источники (в первую очередь вновь изданные в периодической научной литературе) для более детального понимания вопросов, озвученных на лекции.

При самостоятельной проработке курса обучающиеся должны:

· просматривать основные определения и факты;

· повторить законспектированный на лекционном занятии материал и дополнить его с учетом рекомендованной по данной теме литературы;

· изучить рекомендованную литературу, составлять тезисы, аннотации и конспекты наиболее важных моментов;

· самостоятельно выполнять задания, аналогичные предлагаемым на занятиях;

· использовать для самопроверки материалы фонда оценочных средств.

1. Методические указания при работе над конспектом лекции

В ходе лекционных занятий необходимо вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации, положительный опыт в ораторском искусстве. Желательно оставить в рабочих конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

2. Методические указания по самостоятельной работе над изучаемым материалом и при подготовке к лабораторным занятиям

Начинать надо с изучения рекомендованной литературы. Необходимо помнить, что на лекции обычно рассматривается не весь материал, а только его часть. Остальная его часть восполняется в процессе самостоятельной работы. В связи с этим работа с рекомендованной литературой обязательна. Особое внимание при этом необходимо обратить на содержание основных положений и выводов, объяснение явлений и фактов, уяснение практического приложения рассматриваемых теоретических вопросов. В процессе этой работы необходимо стремиться понять и запомнить основные положения рассматриваемого материала, примеры, поясняющие его, а также разобраться в иллюстративном материале. Оформлять отчеты следует руководствуясь внутренними нормативными документами КнАГУ.

3. Методические указания по выполнению расчетно-графической работы

Теоретическая часть расчетно-графической работы выполняется по установленным темам с использованием практических материалов. К каждой теме расчетно-графической работы рекомендуется примерный перечень узловых вопросов, список необходимой литературы. Излагая вопросы темы, следует строго придерживаться плана. Работа не должна представлять пересказ отдельных глав учебника или учебного пособия. Необходимо изложить собственные соображения по существу излагаемых вопросов, внести свои предложения. Общие положения должны быть подкреплены и пояснены конкретными примерами. Излагаемый материал при необходимости следует проиллюстрировать таблицами, схемами, диаграммами.

10 Описание материально-технического обеспечения, необходимого для осуществления образовательного процесса по дисциплине (модулю)

10.1 Учебно-лабораторное оборудование

Таблица 6 – Перечень оборудования лаборатории

Аудитория	Наименование аудитории (лаборатории)	Используемое оборудование
202/5	Лаборатория программно-аппаратных средств защиты информации	СЗИ НСД Secret Net, СЗИ НСД Dallas Lock, СЗИ НСД Страж NT, СЗИ НСД Щит РЖД, СЗИ НСД Аура ,СЗИ НСД Криптон ,СЗИ НСД Аккорд, ФИКС, Ревизор 1,2 как для операционных систем семейства Windows так и для Linux, Ревизор Сети 2.0, Анализатор сетевого траффика Астра,Агент инвентаризации сети,Сканер сетевой безопасности XSpider, Терьер, Secret Net Touch Memory Card, Криптон АМДЗ, Аккорд АМДЗ, КриптоПРО АРМ, ,CryptoPro CSP 3.6, VipNet firewall, Etoken PKI Client, Etoken, Ноутбук с Windows 7+проектор. 16 ПЭВМ на базе процессоров не ниже Intel Pentium IV

10.2 Технические и электронные средства обучения

Лекционные занятия

Аудитории для лекционных занятий укомплектованы мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории (наборы демонстрационного оборудования (проектор, экран, компьютер/ноутбук), учебно-наглядные пособия, тематические иллюстрации).

Лабораторные занятия

Для лабораторных занятий используется аудитория №_202_, оснащенная оборудованием, указанным в табл. 8:

Самостоятельная работа.

Помещения для самостоятельной работы оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и доступом к электронной информационно-образовательной среде КнАГУ:

- читальный зал НТБ КнАГУ;
- компьютерные классы (ауд. 311 корпус № 5, ауд. 205 корпус № 5, ауд. 313 корпус № 5).

11 Иные сведения

Методические рекомендации по обучению лиц с ограниченными возможностями здоровья и инвалидов

Освоение дисциплины обучающимися с ограниченными возможностями здоровья может быть организовано как совместно с другими обучающимися, так и в отдельных группах. Предполагаются специальные условия для получения образования обучающимися с ограниченными возможностями здоровья.

Профессорско-педагогический состав знакомится с психолого-физиологическими особенностями обучающихся инвалидов и лиц с ограниченными возможностями здоровья, индивидуальными программами реабилитации инвалидов (при наличии). При необходимости осуществляется дополнительная поддержка преподавания тьюторами, психологами, социальными работниками, прошедшими подготовку ассистентами.

В соответствии с методическими рекомендациями Минобрнауки РФ (утв. 8 апреля 2014 г. N АК-44/05вн) в курсе предполагается использовать социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений с другими студентами, создании комфортного психологического климата в студенческой группе. Подбор и разработка учебных материалов производятся с учетом предоставления материала в различных формах: аудиальной, визуальной, с использованием специальных технических средств и информационных систем.

Освоение дисциплины лицами с ОВЗ осуществляется с использованием средств обучения общего и специального назначения (персонального и коллективного использования). Материально-техническое обеспечение предусматривает приспособление аудиторий к нуждам лиц с ОВЗ.

Форма проведения аттестации для студентов-инвалидов устанавливается с учетом индивидуальных психофизических особенностей. Для студентов с ОВЗ предусматривается доступная форма предоставления заданий оценочных средств, а именно:

· в печатной или электронной форме (для лиц с нарушениями опорно-двигательного аппарата);

· в печатной форме или электронной форме с увеличенным шрифтом и контрастностью (для лиц с нарушениями слуха, речи, зрения);

· методом чтения ассистентом задания вслух (для лиц с нарушениями зрения).

Студентам с инвалидностью увеличивается время на подготовку ответов на контрольные вопросы. Для таких студентов предусматривается доступная форма предоставления ответов на задания, а именно:

· письменно на бумаге или набором ответов на компьютере (для лиц с нарушениями слуха, речи);

· выбором ответа из возможных вариантов с использованием услуг ассистента (для лиц с нарушениями опорно-двигательного аппарата);

· устно (для лиц с нарушениями зрения, опорно-двигательного аппарата).

При необходимости для обучающихся с инвалидностью процедура оценивания результатов обучения может проводиться в несколько этапов.

Приложение 1

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ[1]
по дисциплине

Программно-аппаратные средства защиты информации

Направление подготовки	*10.05.03 "Информационная безопасность автоматизированных систем"*
Направленность (профиль) образовательной программы	Анализ безопасности информационных систем
Квалификация выпускника	*специалист по защите информации*
Год начала подготовки *(по учебному плану)*	*2021*
Форма обучения	*очная*
Технология обучения	*традиционная*

Курс	Семестр	Трудоемкость, з.е.
4	*8*	*4*

Вид промежуточной аттестации	Обеспечивающее подразделение
Зач_с_оц	*Кафедра ИБАС - Информационная безопасность автоматизированных систем*

[1] В данном приложении представлены типовые оценочные средства. Полный комплект оценочных средств, включающий все варианты заданий (тестов, контрольных работ и др.), предлагаемых обучающемуся, хранится на кафедре в бумажном и электронном виде.

1 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами образовательной программы

Таблица 1 – Компетенции и планируемые результаты обучения по дисциплине

Код и наименование компетенции	Индикаторы достижения	Планируемые результаты обучения по дисциплине
Общепрофессиональные		
ОПК-11 Способен разрабатывать компоненты систем защиты информации автоматизированных систем	**ОПК-11.1 З**нает программно-аппаратные средства, используемые в качестве компонентов систем защиты информации в программном обеспечении автоматизированных систем; методы проектирования решений по обеспечению безопасности автоматизированных систем	**З**нает программно-аппаратные средства, используемые в качестве компонентов систем защиты информации в программном обеспечении автоматизированных систем
	ОПК-11.2 Умеет проектировать защищенные распределенные информационные системы и компоненты систем защиты информации автоматизированных систем	Умеет проектировать компоненты систем защиты информации автоматизированных систем
	ОПК-11.3 Владеет навыками разработки компонентов систем защиты информации автоматизированных систем и защищенных распределенные информационные системы	Владеет навыками разработки компонентов систем защиты информации автоматизированных систем и защищенных распределенные информационные системы
ОПК-7.1. Способен использовать программные и программно-аппаратные средства для моделирования и испытания систем защиты информационных систем	**ОПК-7.1..1** Знает программные и программно-аппаратные средства для моделирования и испытания систем защиты информационных систем; методы применения программных и программно-аппаратных средств для моделирования и испытания систем защиты информационных систем	Знает программные и программно-аппаратные средства для моделирования и испытания систем защиты информационных систем; методы применения программных и программно-аппаратных средств для моделирования и испытания систем защиты информационных систем
	ОПК-7.1..2 Умеет выбирать программные и программно-аппаратные средства для моделирования и испытания систем защиты информационных систем	Умеет выбирать программные и программно-аппаратные средства для моделирования и испытания систем защиты информационных систем
	ОПК-7.1..3 Владеет навыками применения программных и	Владеет навыками применения программных и програм-

	программно-аппаратных средств для моделирования и испытания систем защиты информационных систем	мно-аппаратных средств для моделирования и испытания систем защиты информационных систем

Таблица 2 – Паспорт фонда оценочных средств

Контролируемые разделы (темы) дисциплины	Формируемая компетенция	Наименование оценочного средства	Показатели оценки
1. Применение СЗИ от НСД для организации защищенных компьютерных систем. Применение средств организации виртуальных частных сетей	ОПК-11, ОПК-7.1	Практическое задание1,2 , лабораторные работы	Настроить систему зашиты информации в соответствии со стандартами по оценке защищенных систем. Настроить систему защиты в СЗИ НСД на невозможность использования внешних устройств с удаленных АРМ в виртуальной частной сети
2. Защита программ от изучения, способы встраивания и защиты ПО Методы и средства ограничения доступа к компонентам вычислительных систем	ОПК-11, ОПК-7.1	Практическое задание 3,4, лабораторные работы	Настроить эвристический анализ в антивирусе для всех типов файлов в автоматизированной системе. Настроить аудит всех типов событий с использованием СЗИ НСД и продемонстрировать возможность анализа с использованием журналов
Настройка СЗИ НСД.	ОПК-11, ОПК-7.1	Контрольная работа	Показывает умения и навыки по настройке средств защиты информации для реальных объектов информатизации в соответствии с требованиями руководящих документов

Промежуточная аттестация в пятом семестре проводится в форме Зач_с_оц.

2 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующие процесс формирования компетенций

Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, представлены в виде технологической карты дисциплины (таблица 3).

Таблица 3 – Технологическая карта

	Наименование оценочного средства	Сроки выполнения	Шкала оценивания	Критерии оценивания
_____ 7 семестр Промежуточная аттестация в форме Зач_с_оц				
1	Практическое задание по теме № 1, лабораторная работа	В течение семестра	5 баллов	5 баллов - студент правильно выполнил задание. Аккуратно оформлено графическая и текстовые части. 4 баллов – выполнил задание с небольшими неточностями. Есть замечания к оформлению графической и текстовой частям. 3 баллов – студент выполнил задание с существенными неточностями. Показал удовлетворительные знания в рамках освоенного учебного материала. 2 баллов – при выполнении задания студент продемонстрировал недостаточный уровень знаний. 0 баллов – задание не выполнено.
2	Практическое задание по теме № 2, лабораторная работа	В течение семестра	10 баллов	10 баллов - студент правильно выполнил задание. Показал отличные знания в рамках освоенного учебного материала. 5 балла - студент выполнил задание с небольшими неточностями. Показал хорошие знания в рамках освоенного учебного материала. 3 балла - студент выполнил задание с существенными неточностями. Показал удовлетворительные знания в рамках освоенного учебного материала. 2 балла - при выполнении задания студент продемонстрировал недостаточный уровень знаний. 0 баллов – задание не выполнено.
3	Практическое задание по заданной теме № 3, лабораторная работа	В течение семестра	10 баллов	10 баллов - студент правильно выполнил задание. Показал отличные знания в рамках освоенного учебного материала. 5 балла - студент выполнил задание с небольшими неточностями. Показал хорошие знания в рамках освоенного учебного материала. 3 балла - студент выполнил задание с существенными неточностями. Показал удовлетвори-

	Наименование оценочного средства	Сроки выполнения	Шкала оценивания	Критерии оценивания
				тельные знания в рамках освоенного учебного материала. 2 балла - при выполнении задания студент продемонстрировал недостаточный уровень знаний. 0 баллов – задание не выполнено.
4	Практическое задание по заданной теме № 4, лабораторная работа	В течение семестра	10 баллов	10 баллов - студент правильно ответил на вопросы. Показал отличные знания в рамках освоенного учебного материала. 5 балов - студент ответил на вопросы с небольшими неточностями. Показал хорошие знания в рамках освоенного учебного материала. 3 балла - студент ответил на вопросы с существенными неточностями. Показал удовлетворительные знания в рамках освоенного учебного материала. 2 балла - при выполнении задания студент продемонстрировал недостаточный уровень знаний. 0 баллов – задание не выполнено.
Контрольная работа		В течение семестра	30 баллов	30 баллов - студент правильно ответил на вопросы. Показал отличные знания в рамках освоенного учебного материала. 15 балов - студент ответил на вопросы с небольшими неточностями. Показал хорошие знания в рамках освоенного учебного материала. 10 балла - студент ответил на вопросы с существенными неточностями. Показал удовлетворительные знания в рамках освоенного учебного материала. 5 балла - при выполнении задания студент продемонстрировал недостаточный уровень знаний. 0 баллов – задание не выполнено.
ИТОГО:		-	65 баллов	-
Критерии оценки результатов обучения по дисциплине: 0 – 64 % от максимально возможной суммы баллов – «неудовлетворительно» (недостаточный уровень для промежуточной аттестации по дисциплине); 65 – 74 % от максимально возможной суммы баллов – «удовлетворительно» (пороговый (минимальный) уровень); 75 – 84 % от максимально возможной суммы баллов – «хорошо» (средний уровень); 85 – 100 % от максимально возможной суммы баллов – «отлично» (высокий (максималь-				

	Наименование оценочного средства	Сроки выполнения	Шкала оценивания	Критерии оценивания
ный) уровень)				

3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие процесс формирования компетенций в ходе освоения образовательной программы

3.1 Задания для текущего контроля успеваемости

Практическое задание № 1 Применение СЗИ от НСД для организации защищенных компьютерных систем.

Задание 1: Настроить средства аудита в СЗИ НСД

Задание 2: Провести аудит информационной безопасности АРМ с установленным СЗИ НСД с использованием openVAS или другого сканера безопасности.

Задание 3: Установить и настроить сервер SNS и в домене безопасности зарегистрировать минимум одного пользователя.

Задание 4: Установить Alien Vault. Провести сканирование с его помощью.

Задание 5:

1. В таблице 1 найти для вашего варианта значения характеристик P, V, T.
2. Вычислить по формуле (1) нижнюю границу S^* для заданных P, V, T.
3. Выбрать некоторый алфавит с мощностью A и получить минимальную длину пароля L, при котором выполняется условие (2).

2. Реализовать программу – генератор паролей пользователей. Программа должна формировать случайную последовательность символов длины L, при этом должен использоваться алфавит из A символов.
3. Оформить в отчет по лабораторной работе

Замечания:

При реализации программы могут быть полезны следующие функции

1. функция, возвращающая случайное число $0 \le r < N$.
2. функция, сбрасывающая начальное состояние датчика случайных чисел случайным образом.
3. функция, возвращающая символ с ASCII кодом X. Коды различных групп символов приведены ниже.

Коды символов

Коды английских символов : «A»=65,…,«Z»=90, «a»=97,…, «z» =122.

Коды цифр : «0» = 48, «9» = 57.

! - 33, “ – 34, # - 35, $ - 36, % - 37, & - 38, ‘ – 39, (- 40,) – 41, * - 42.

Коды русских символов : «А» - 128, … «Я» - 159, «а» - 160,…, «п» - 175, «р» - 224,…, «я» - 239.

Таблица 1

Вариант	P	V	T
1	10^{-4}	15 паролей/мин	2 недели
2	10^{-5}	3 паролей/мин	10 дней

3	10^{-6}	10 паролей/мин	5 дней
4	10^{-7}	11 паролей/мин	6 дней
5	10^{-4}	100 паролей/день	12 дней
6	10^{-5}	10 паролей/день	1 месяц
7	10^{-6}	20 паролей/мин	3 недели
8	10^{-7}	15 паролей/мин	20 дней
9	10^{-4}	3 паролей/мин	15 дней
10	10^{-5}	10 паролей/мин	1 неделя
11	10^{-6}	11 паролей/мин	2 недели
12	10^{-7}	100 паролей/день	10 дней
13	10^{-4}	10 паролей/день	5 дней
14	10^{-5}	20 паролей/мин	6 дней
15	10^{-6}	15 паролей/мин	12 дней
16	10^{-7}	3 паролей/мин	1 месяц
17	10^{-4}	10 паролей/мин	3 недели
18	10^{-5}	11 паролей/мин	20 дней
19	10^{-6}	100 паролей/день	15 дней
20	10^{-7}	10 паролей/день	1 неделя
21	10^{-4}	20 паролей/мин	2 недели
22	10^{-5}	15 паролей/мин	10 дней
23	10^{-6}	3 паролей/мин	5 дней
24	10^{-7}	10 паролей/мин	6 дней
25	10^{-4}	11 паролей/мин	12 дней
26	10^{-5}	100 паролей/день	1 месяц
27	10^{-6}	10 паролей/день	3 недели
28	10^{-7}	20 паролей/мин	20 дней
29	10^{-4}	15 паролей/мин	15 дней
30	10^{-5}	3 паролей/мин	1 неделя

Практическое задание № 2 Применение средств организации виртуальных частных сетей.

Задание 1: Организовать VPN туннель возможно использовать свободно распространяемый OpenVPN.

Задание 2: проконтролировать шифрование в туннеле используя wireshark

Задание 3: перехватить траффик между узлами с использованием туннелирования и без.

Задание 4: зашифровать файл с использованием veracrypt. Передать его по сети и перехватить. Посмотреть есть ли возможность получить доступ к содержимому файла.

Задание 5:

В таблице найти требования, которым должен удовлетворять генератор паролей, соответствующий Вашему варианту.

Написать программу-генератор паролей, в соответствие с требованиями Вашего варианта. Программа должна выполнять следующие действия:

a. Ввод идентификатора пользователя с клавиатуры. Данный идентификатор представляет собой последовательность символов $a_1 a_2 ... a_N$, где N – количество символов идентификатора (может быть любым), a_i - i – ый символ идентификатора пользователя.

b. Формирование пароля пользователя $b_1 b_2 ... b_M$ для данного идентификатора, где M – количество символов пароля, соответствующее Вашему варианту, и вывод его на экран. Алгоритм получения символов пароля b_i указан в перечне требований Таблицы 1 для Вашего варианта.

Таблица 1

Вариант	Количество символов пароля	Перечень требований
1	6	1. b_1, b_2 - случайные заглавные буквы английского алфавита. 2. $b_3 = N^2 \bmod 10$ (где mod 10 – остаток от деления числа на 10). 3. b_4 - случайная цифра. 4. b_5 - случайный символ из множества {!,",#,$,%,&,',(,),*}. 5. b_6 - случайная малая буква английского алфавита.
2	7	1. b_1, b_2, b_3 - случайные малые буквы английского алфавита. 2. b_4, b_5 - случайные заглавные буквы английского алфавита. 3. $b_6 b_7$ - двузначное число, равное $N^4 \bmod 100$. (Если остаток – однозначное число, то $b_6 = 0$).
3	8	1. b_1, b_2, b_3 - случайные цифры. 2. b_4, b_5 - случайные символы из множества {!,",#,$,%,&,',(,),*}. 3. b_7 - случайная заглавная буква английского алфавита. 4. b_8 - P –ая по счету малая буква английского алфавита, где $P = N^2 \bmod 10 + N^3 \bmod 10 + 1$.
4	9	1. $b_1, ..., b_{1+Q}$ - случайные символы из множества {!,",#,$,%,&,',(,),*}, где $Q = N \bmod 5$.

		2. Оставшиеся символы пароля, кроме b_9, - случайные малые буквы английского алфавита. 3. b_9 - случайная цифра.
5	10	1. $b_{10-Q},...,b_{10}$ - случайные цифры, где $Q = N \bmod 6$. 2. b_1, b_2 - случайные большие буквы английского алфавита. 3. $b_3,...,b_{10-Q-1}$ - случайные малые буквы английского алфавита.
6	11	1. b_1, b_2 - случайные цифры. 2. $b_3,...,b_{3+Q}$ - случайные большие буквы английского алфавита, где $Q = N \bmod 8$. 3. $b_{4+Q},...,b_{11}$ - случайные символы из множества {!,",#,$,%,&,',(,),*}.
7	11	1. b_1, b_2 - случайные цифры. 2. $b_3,...,b_{3+Q}$ - случайные малые буквы русского алфавита, где $Q = N \bmod 8$. 3. $b_{4+Q},...,b_{11}$ - случайные символы из множества {!,",#,$,%,&,',(,),*}.
8	12	1. $b_1,...,b_{1+Q}$ - случайные малые буквы английского алфавита, где $Q = N^3 \bmod 5$. 2. $b_{1+Q+1},...,b_{1+Q+1+P}$ - случайные заглавные буквы английского алфавита, где $P = N^2 \bmod 6$. 3. Оставшиеся символы пароля – случайные цифры.
9	12	1. $b_1,...,b_{1+Q}$ - случайные малые буквы русского алфавита, где $Q = N^3 \bmod 5$. 2. $b_{1+Q+1},...,b_{1+Q+1+P}$ - случайные заглавные буквы русского алфавита, где $P = N^2 \bmod 6$. 3. Оставшиеся символы пароля – случайные цифры.
10	10	1. $b_{10-Q},...,b_{10}$ - случайные цифры, где $Q = N \bmod 6$. 2. b_1, b_2 - случайные большие буквы русского алфавита. 3. $b_3,...,b_{10-Q-1}$ - случайные малые буквы русского алфавита.
11	9	1. $b_1, b_2 ... b_{1+Q}$ - случайные символы из множества {!,",#,$,%,&,',(,),*}, где $Q = N \bmod 5$.

		2. Оставшиеся символы пароля, кроме b_9, - случайные малые буквы русские алфавита. 3. b_9 - случайная цифра.
12	8	1. b_1, b_2, b_3 - случайные цифры. 2. b_4, b_5 - случайные символы из множества {!,",#,$,%,&,',(,),*}. 3. b_7 - случайная заглавная буква русского алфавита. 4. b_8 - Р –ая по счету малая буква русского алфавита, где $P = N^2 \bmod 15 + N^3 \bmod 15 + 1$.
13	7	1. b_1, b_2, b_3 - случайные малые буквы русского алфавита. 2. b_4, b_5 - случайные заглавные буквы русского алфавита. 3. $b_6 b_7$ - двузначное число, равное $N^4 \bmod 100$. (Если остаток – однозначное число, то $b_6 = 0$).
14	6	1. b_1, b_2 - случайные заглавные буквы русского алфавита. 2. $b_3 = N^2 \bmod 10$ (где mod 10 – остаток от деления числа на 10). 3. b_4 - случайная цифра. 4. b_5 - случайный символ из множества {!,",#,$,%,&,',(,),*}. 5. b_6 - случайная малая буква русского алфавита.
15	6	1. b_1, b_2 - случайные заглавные буквы английского алфавита. 2. $b_3 = N^2 \bmod 10$ (где mod 10 – остаток от деления числа на 10). 3. b_4 - случайная цифра. 4. b_5 - случайный символ из множества {!,",#,$,%,&,',(,),*}. 5. b_6 - случайная малая буква русского алфавита.
16	7	1. b_1, b_2, b_3 - случайные малые буквы русского алфавита. 2. b_4, b_5 - случайные заглавные буквы английского алфавита. 3. $b_6 b_7$ - двузначное число, равное $N^4 \bmod 100$. (Если остаток – однозначное число, то $b_6 = 0$).
17	8	1. b_1, b_2, b_3 - случайные цифры.

		2. b_4, b_5 - случайные символы из множества {!,",#,$,%,&,',(,),*}. 3. b_7 - случайная заглавная буква английского алфавита. 4. b_8 - P –ая по счету малая буква русского алфавита, где $P = N^2 \bmod 10 + N^3 \bmod 10 + 1$.
18	9	1. $b_1,...,b_{1+Q}$ - случайные цифры, где $Q = N \bmod 5$. 2. Оставшиеся символы пароля, кроме b_9, - случайные малые буквы английского алфавита. 3. b_9 - случайная цифра.
19	10	1. $b_{10-Q},...,b_{10}$ - случайные цифры, где $Q = N \bmod 6$. 2. b_1, b_2 - случайные большие буквы английского алфавита. 3. $b_3,...,b_{10-Q-1}$ - случайные малые буквы русского алфавита.
20	11	1. b_1, b_2 - случайные символы из множества {!,",#,$,%,&,',(,),*}. 2. $b_3,...,b_{3+Q}$ - случайные большие буквы английского алфавита, где $Q = N \bmod 8$. 3. $b_{4+Q},...,b_{11}$ - случайные цифры.
21	11	1. b_1, b_2 - случайные символы из множества {!,",#,$,%,&,',(,),*}. 2. $b_3,...,b_{3+Q}$ - случайные малые буквы русского алфавита, где $Q = N \bmod 8$. 3. $b_{4+Q},...,b_{11}$ - случайные цифры.
22	12	1. $b_1,...,b_{1+Q}$ - случайные малые буквы русского алфавита, где $Q = N^3 \bmod 5$. 2. $b_{1+Q+1},...,b_{1+Q+1+P}$ - случайные заглавные буквы английского алфавита, где $P = N^2 \bmod 6$. 3. Оставшиеся символы пароля – случайные цифры.
23	12	1. $b_1,...,b_{1+Q}$ - случайные малые буквы английского алфавита, где $Q = N^3 \bmod 5$. 2. $b_{1+Q+1},...,b_{1+Q+1+P}$ - случайные заглавные буквы русского алфавита, где $P = N^2 \bmod 6$. 3. Оставшиеся символы пароля – случайные цифры.

24	10	1. $b_{10-Q},...,b_{10}$ - случайные цифры, где $Q = N \bmod 6$. 2. b_1, b_2 - случайные большие буквы английского алфавита. 3. $b_3,...,b_{10-Q-1}$ - случайные малые буквы русского алфавита.
25	9	1. $b_1, b_2 ... b_{1+Q}$ - случайная цифра.. 2. Оставшиеся символы пароля, кроме b_9, - случайные малые буквы русские алфавита. 3. b_9 - случайные символы из множества {!,",#,$,%,&,',(,),*}, где $Q = N \bmod 5$.
26	8	1. b_1, b_2, b_3 - случайные цифры. 2. b_4, b_5 - случайные символы из множества {!,",#,$,%,&,',(,),*}. 3. b_7 - случайная заглавная буква английского алфавита. 4. b_8 - P –ая по счету малая буква русского алфавита, где $P = N^2 \bmod 15 + N^3 \bmod 15 + 1$.
27	7	1. b_1, b_2, b_3 - случайные малые буквы русского алфавита. 2. b_4, b_5 - случайные заглавные буквы английского алфавита. 3. $b_6 b_7$ - двузначное число, равное $N^4 \bmod 100$. (Если остаток – однозначное число, то $b_6 = 0$).
28	6	1. b_1, b_2 - случайные заглавные буквы английского алфавита. 2. $b_3 = N^2 \bmod 10$ (где mod 10 – остаток от деления числа на 10). 3. b_4 - случайная цифра. 4. b_5 - случайный символ из множества {!,",#,$,%,&,',(,),*}. 5. b_6 - случайная малая буква русского алфавита.

ЗАМЕЧАНИЯ

1. Коды английских символов - «A»=65,…,«Z»=90, «a»=97,…, «z» =122.
2. Коды цифр – «0» = 48, «9» = 57.
3. Коды спец. символов ! – 33, " – 34, # - 35, $ - 36, % - 37, & - 38, ' – 39, (- 40,) – 41, * - 42.
4. Коды русских символов – «А» - 128, … «Я» - 159, «а» - 160,…, «п» - 175, «р» - 224,…, «я» - 239.

4. В таблице 1 найти требования, которым должен удовлетворять генератор паролей, соответствующий Вашему варианту.

Практическое задание № 3 Защита программ от изучения, способы встраивания и защиты ПО.

Задание 1 Провести попытку дизассемблирования (изучения программного кода) для приложения.

Задание 2: Провести попытку дизассемблирования (изучения программного кода) для антивируса.

Задание 3: Провести попытку дизассемблирования приложения, разработанного на Visual C++ и C#

Задание 4: Провести попытку дизассемблирования приложения, разработанного на языке pyton.

Пусть множество S возможных операций над объектами компьютерной системы задано следующим образом: S={«Доступ на чтение», «Доступ на запись», «Передача прав»}.

1.Получить данные о количестве пользователей и объектов компьютерной системы из таблицы 2, соответственно Вашему варианту.

2.Реализовать программный модуль, создающий матрицу доступа пользователей к объектам компьютерной системы. Реализация данного модуля подразумевает следующее:

1.1. Выбрать идентификаторы пользователей, которые будут использоваться при их входе в компьютерную систему (по одному идентификатору для каждого пользователя, количество пользователей задано для Вашего варианта). Например, множество из 3 идентификаторов пользователей {Ivan, Sergey, Boris}. Один из данных идентификаторов должен соответствовать администратору компьютерной системы (пользователю, обладающему полными правами ко всем объектам).

1.2. Реализовать программное заполнение матрицы доступа, содержащей количество пользователей и объектов, соответственно Вашему варианту.

1.2.1. При заполнении матрицы доступа необходимо учесть, что один из пользователей должен являться администратором системы (допустим, пользователь Ivan). Для него права доступа ко всем объектам должны быть выставлены как полные.

1.2.2. Права остальных пользователей для доступа к объектам компьютерной системы должны заполняться случайным образом с помощью датчика случайных чисел. При заполнении матрицы доступа необходимо учесть, что пользователь может иметь несколько прав доступа к некоторому объекту компьютерной системы, иметь полные права, либо совсем не иметь прав.

2. Реализовать программный модуль, демонстрирующий работу в дискреционной модели политики безопасности. Данный модуль должен выполнять следующие функции:

2.1. При запуске модуля должен запрашиваться идентификатор пользователя (должна проводиться идентификация пользователя). При успешной идентификации пользователя должен осуществляться вход в систему. При неуспешной – выводиться соответствующее сообщение.

2.2. При входе в систему после успешной идентификации пользователя, на экране должен распечатываться список всех объектов системы с указанием перечня всех доступных прав доступа идентифицированного пользователя к данным объектам. Вывод можно осуществить, например, следующим образом:

User: Boris

Идентификация прошла успешно, добро пожаловать в систему

Перечень Ваших прав:

Объект1: Чтение

Объект2: Запрет

Объект3: Чтение, Запись

Объект4: Полные права

Жду ваших указаний >

3.3. После вывода на экран перечня прав доступа пользователя к объектам компьютерной системы, программа должна ждать указаний пользователя на осуществление действий над объектами в компьютерной системе. После получения команды от пользователя, на экран должно выводиться сообщение об успешности либо не успешности операции. При выполнении операции передачи прав (grant), должна модифицироваться матрица доступов. Должна поддерживаться операция выхода из системы (quit), после которой должен запрашиваться другой идентификатор пользователя. Диалог можно организовать, например, следующим образом:

Жду ваших указаний > read

Над каким объектом производится операция? 1

Операция прошла успешно

Жду ваших указаний > write

Над каким объектом производится операция? 2

Отказ в выполнении операции. У Вас нет прав для ее осуществления

Жду ваших указаний > grant

Право на какой объект передается? 3

Отказ в выполнении операции. У Вас нет прав для ее осуществления

Жду ваших указаний > grant

Право на какой объект передается? 4

Какое право передается? read

Какому пользователю передается право? Ivan

Операция прошла успешно

Жду ваших указаний > quit

Работа пользователя Boris завершена. До свидания.

User:

3. Прогнать реализованную программу, продемонстрировав реализованную модель дискреционной политики безопасности преподавателю.

4. Оформить отчет по лабораторной работе согласно примеру, приведенному на последней странице.

Таблица 2

Вариант	Количество субъектов доступа (пользователей)	Количество объектов доступа
1	3	3
2	4	4

3	5	4
4	6	5
5	7	6
6	8	3
7	9	4
8	10	4
9	3	5
10	4	6
11	5	3
12	6	4
13	7	4
14	8	5
15	9	6
16	10	3
17	3	4
18	4	4
19	5	5
20	6	6
21	7	3
22	8	4
23	9	4
24	10	5
25	3	6
26	4	3
27	5	4
28	6	4
29	6	5
30	8	6

ПРИМЕР ПРОГОНКИ ПРОГРАММЫ

User: Sergey

Идентификация прошла успешно, добро пожаловать в систему

Перечень Ваших прав:

Объект1: Полные права

Объект2: Полные права

Объект3: Полные права

Объект4: Полные права

Жду ваших указаний > quit

Работа пользователя Sergey завершена. До свидания.

User: Ivan

Идентификация прошла успешно, добро пожаловать в систему

Перечень Ваших прав:

Объект1: Запрет

Объект2: Запрет

Объект3: Запрет

Объект4: Запрет

Жду ваших указаний > quit

Работа пользователя Ivan завершена. До свидания.

User: Boris

Идентификация прошла успешно, добро пожаловать в систему

Перечень Ваших прав:

Объект1: Чтение

Объект2: Запрет

Объект3: Чтение, Запись

Объект4: Полные права

Жду ваших указаний > read

Над каким объектом производится операция? 1

Операция прошла успешно

Жду ваших указаний > write

Над каким объектом производится операция? 2

Отказ в выполнении операции. У Вас нет прав для ее осуществления

Жду ваших указаний > grant

Право на какой объект передается? 3

Отказ в выполнении операции. У Вас нет прав для ее осуществления

Жду ваших указаний > grant

Право на какой объект передается? 4

Какое право передается? read

Какому пользователю передается право? Ivan

Операция прошла успешно

Жду ваших указаний > quit

Работа пользователя Boris завершена. До свидания.

User:Ivan

Идентификация прошла успешно, добро пожаловать в систему

Перечень Ваших прав:

Объект1: Запрет

Объект2: Запрет

Объект3: Запрет

Объект4: Чтение

Жду ваших указаний > quit

Работа пользователя Ivan завершена. До свидания.

User:

Практическое задание № 4 Методы и средства ограничения доступа к компонентам вычислительных систем.

Задание 1 Настроить средство защиты от НСД для ограничения использования внешних накопителей в системе.

Задание 2: Настроить средство защиты от НСД для ограничения доступа пользователей к удаленным рабочим столам.

Задание 3: Настроить средство защиты от НСД для ограничения количества попыток входа в систему.

Задание 4: Настроить аппаратно-программный модуль доверенной загрузки(любой) на выполнение сброса через определенное время.

Задание 5:

Пусть задано множество атрибутов безопасности A={«Совершенно секретно», «Секретно», «Открытые данные»}.

1. Получить информацию о количестве объектов и субъектов компьютерной системы из таблицы 1, соответственно Вашему варианту.
2. Реализовать программный модуль, создающий мандатную модель политики безопасности. Реализация данного модуля подразумевает следующее:
   1.1. Выбрать идентификаторы пользователей-субъектов, которые будут использоваться при их входе в компьютерную систему (по одному идентификатору для каждого пользователя, количество пользователей-субъектов задано для Вашего варианта). Например, множество из 3 идентификаторов пользователей {Ivan, Sergey, Boris}.
   1.2. Заполнить вектор *OV*, задающий уровни конфиденциальности объектов, случайным образом. Множество атрибутов безопасности *A* представлено выше.
   1.3. Заполнить вектор *UV*, задающий уровни допуска пользователей, случайным образом. Множество атрибутов безопасности *A* представлено выше.

1.4. Распечатать на экране вектора *OV* и *UV*, определяющие уровни конфиденциальности объектов и уровни допуска пользователей. Вывод можно осуществить, например, следующим образом:

Уровни конфиденциальности объектов (*OV*):

Объект_1: Открытые данные

Объект_2: Секретно

Объект_3: Совершенно секретно

Объект_4: Открытые данные

Уровни допуска пользователей (*UV*)

Ivan: Совершенно секретно

Sergey: Секретно

Boris: Открытые данные

2. Реализовать программный модуль, демонстрирующий работу системы в мандатной модели политики безопасности. Данный модуль должен выполнять следующие функции:

2.1. Выполнять идентификацию пользователя при входе в систему. При успешной идентификации пользователя должен осуществляться вход в систему. При неуспешной – выводиться соответствующее сообщение.

2.2. При входе в систему после успешной идентификации пользователя, на экране должен распечатываться список тех объектов системы, к которым у вошедшего пользователя есть доступ. Вывод можно осуществить, например, следующим образом:

User: Boris

Идентификация прошла успешно, добро пожаловать в систему

Перечень доступных объектов: Объект_1, Объект_4.

Жду ваших указаний >

3.3. После вывода на экран перечня доступных объектов, программа должна ждать указаний пользователя на осуществление действий над объектами в компьютерной системе (команда request). После получения команды request от пользователя, на экран должно выводиться сообщение об успешности либо не успешности операции. Должна поддерживаться операция выхода из системы (quit), после которой должен запрашиваться другой идентификатор пользователя. Диалог можно организовать, например, следующим образом:

Жду ваших указаний > request

К какому объекту хотите осуществить доступ? 1

Операция прошла успешно

Жду ваших указаний > request

К какому объекту хотите осуществить доступ? 2

Отказ в выполнении операции. Недостаточно прав.

Жду ваших указаний > quit

Работа пользователя Boris завершена. До свидания.

User:

4. Прогнать реализованную программу, продемонстрировав реализованную модель мандатной политики безопасности преподавателю.

5. Оформить отчет по лабораторной работе согласно примеру, приведенному на последней странице.

ЗАМЕЧАНИЕ

1. Атрибуты безопасности объектов и уровни доступа субъектов могут быть закодированы цифрами для удобства хранения и сравнения.

Таблица 1

Вариант	Количество субъектов доступа	Количество объектов доступа
1	3	3
2	4	4
3	5	4
4	6	5
5	7	6
6	8	3
7	9	4
8	10	4
9	3	5
10	4	6
11	5	3
12	6	4
13	7	4
14	8	5
15	9	6
16	10	3
17	3	4
18	4	4
19	5	5
20	6	6
21	7	3
22	8	4

23	9	4
24	10	5
25	3	6
26	4	3
27	5	4
28	6	4
29	6	5
30	8	6

ПРИМЕР РАБОТЫ С ПРОГРАММНОЙ МОДЕЛЬЮ МАНДАТНОЙ ПОЛИТИКИ БЕЗОПАСНОСТИ

Уровни конфиденциальности объектов (*OV*):

Объект_1: Открытые данные

Объект_2: Секретно

Объект_3: Совершенно секретно

Объект_4: Открытые данные

Уровни допуска пользователей (*UV*)

Ivan: Совершенно секретно

Sergey: Секретно

Boris: Открытые данные

User: Boris

Идентификация прошла успешно, добро пожаловать в систему

Перечень доступных объектов: Объект_1, Объект_4.

Жду ваших указаний > request

К какому объекту хотите осуществить доступ? 1

Операция прошла успешно

Жду ваших указаний > request

К какому объекту хотите осуществить доступ? 2

Отказ в выполнении операции. Недостаточно прав.

Жду ваших указаний > quit

Работа пользователя Boris завершена. До свидания.

User:

Задания для выполнения лабораторных работ

Изучение средства ФИКС

Установить средство фиксации и контроля программного комплекса. Снять контрольные суммы с папки. Папка согласуется с преподавателем.

Установить любой калькулятор хеш функций и сравнить его работу с работой ФИКС.

Изучение средства Терьер

Установить средство поиска и гарантированного уничтожения информации. Создать файл с фамилией студента и расширением txt. Удалить его. Найти удаленный файл с использованием Терьер. Восстановить данный файл любым средством автоматического восстановления.

Изучение средств Ревизор 1 XP и Ревизор 2 XP

Установить средства создания и проверки модели разграничения доступа в автоматизированных системах. Создать модель разграничения доступа. Изменить настройки безопасности произвольного файла. Проверить модель и сравнить с полученной ранее.

Настройка подсистем защиты Secret Net.

Установить и настроить СЗИ НСД Secert Net 5.1

Настройка подсистем защиты Dallas Lock;

Установить и настроить СЗИ НСД Dallas Lock

Настройка подсистем защиты Страж NT

Установить и настроить СЗИ НСД Страж

АПМДЗ Соболь

Установить и инициализировать плату Соболь.

Защита с использованием АПМДЗ Аккорд

Установить и инициализировать плату Аккорд.

Дизассемблеры и отладчики

Исследовать возможности objdump и дизассемблировать приложение по согласованию с преподавателем. Выполнить дизассемблирование с использованием IDA.

Компоненты систем защиты информации

В Secret Net разрешить подключение только доверенных флеш-накопителей.

Аппаратные модули систем защиты информации

Установить и настроить плату Соболь совместно с Secret Net.

Контрольная работа

Выполнить задание по следующим вариантам (тематика указана примерная и может изменяться):

1. Установить и настроить Secret Net Studio для выполнения требований класса 3а.
2. Установить и настроить Secret Net Studio для выполнения требований класса 3б.
3. Установить и настроить Secret Net Studio для выполнения требований класса 2а.
4. Установить и настроить Secret Net Studio для выполнения требований класса 2б.
5. Установить и настроить Secret Net Studio для выполнения требований класса 1а.

6. Установить и настроить Secret Net Studio для выполнения требований класса 1б.
7. Установить и настроить Secret Net Studio для выполнения требований класса 1в.
8. Установить и настроить Secret Net Studio для выполнения требований класса 1г.
9. Установить и настроить Secret Net Studio для выполнения требований класса УЗ1.
10. Установить и настроить Secret Net Studio для выполнения требований класса УЗ2.
11. Установить и настроить Secret Net Studio для выполнения требований класса УЗ3.
12. Установить и настроить Secret Net Studio для выполнения требований класса К1.
13. Установить и настроить Secret Net Studio для выполнения требований класса К2.
14. Установить и настроить Secret Net Studio для выполнения требований класса К3.

Выбор средства защиты информации может быть изменен по согласованию с преподавателем из существующих сертифицированных средств защиты информации.

Задания выполнить в соответствии с требованиями единой системы документации (ЕСПД) и РД 013-2016 «Текстовые студенческие работы. Правила оформления».

Структурными элементами данной работы должны быть:
- титульный лист;
- текст задания (в соответствии с вариантом);
- содержание;
- введение
- основная часть;
- заключение и выводы;
- список использованных источников;
- приложения.

Во введении дается краткое описание изучаемой дисциплины, которой посвящена данная работа, а также приводится обзор выполненной работы.

Задания для организации «входного» контроля знаний обучающихся.

1. Автоматизированная система:
а) разделенная система;
б) разобщенная система
в) информационная система, включая СВТ, персонал, документацию.
2. Что относится к средствам защиты:
а) межсетевой экран;
б) ОС;
в) текстовый процессор;
3. Что относится к средствам защиты:
а) средства защиты от НСД;
б) монитор;
в) клавиатура.
4. Что относится к средствам защиты
а) Антивирус;
б) Word;
в) Excel;
5. Что относится к средствам защиты:
а) система обнаружения и предотвращения вторжений;
б) система работы с диском;
в) система поиска информации;
6. Орган власти отвечающий за защиту информации не криптографическими средствами:
а) ФСБ;
б) ФСТЭК;

в) Роскомнадзор.
7. Руководящий документ по защите конфиденциальной информации:
а) СТР;
б) СТР-К;
в) СТК-И.
8. Руководящий документ по информационным системам персональных данных:
а) ФЗ 152;
б) ПП 1119;
в) РД ФСТЭК. АС классификация.
9. Руководящий документ по автоматизированным системам:
а) ФЗ 152;
б) ПП 1119;
в) РД ФСТЭК. АС классификация.
10. Служба отвечающая за защиту информации криптографическими средствами:
а) ФСБ;
б) ФСТЭК;
в) Роскомнадзор.
11. Что относится к программно-аппаратным средствам обеспечения информационной безопасности
а) системы, допускающие реальные отклонения от заданных параметров;
б) системы администрирования;
в) системы защиты от несанкционированного доступа;
12. Обязательным условием использования средств защиты на территории РФ является:
а) наличие действующего сертификата ФСТЭК;
б) наличие предписания;
в) наличие разрешения.
13. Что не относится к программно-аппаратным средствам обеспечения информационной безопасности:
а) системы обнаружения и предотвращения вторжений;
б) анализаторы исходных текстов программного обеспечения;
в) аппаратно-программные модули доверенной загрузки.
14. Что не является сертифицированной системой анализа на уязвимости:
а) Сканер ВС;
б) MaxPatrol;
в) namp.
15. Что не является СЗИ от НСД:
а) SecretNet;
б) DallsLock;
в) Cisco ASA.

Вопросы для защиты контрольной работы

1. Одноуровневая модель разграничения доступа, достоинства и недостатки.
2. Многоуровневая модель разграничения доступа, достоинства и недостатки.
3. Применение специализированных программных средств защиты информации, их достоинства и недостатки.
4. Физические носители кодов паролей.
5. Требования к специализированным средствам защиты информации от несанкционированного доступа.
6. Организация виртуальных логических дисков.
7. Механизмы организации контроля доступа до загрузки ОС. Механизмы доверенной загрузки ОС, реализованные в СЗИ.

8. Подсистемы защиты информации и их реализация в СЗИ от НСД «Страж-NT».
9. Подсистемы защиты информации и их реализация в СЗИ от НСД «Dallas Lock».
10. Подсистемы защиты информации и их реализация в СЗИ от НСД «Secret NET».
11. Организация защищенных вычислительных сетей на базе СЗИ сетевого действия.
12. Организация VPN-сетей. Задачи, решаемые VPN. Туннелирование в VPN.
13. Электронные сертификаты. Понятие инфраструктуры открытых ключей.
14. Протоколы и средства организации VPN на сетевом уровне. Назначение, область применения, аутентификация и шифрование данных в протоколах SKIP и IPSec.
15. Протоколы PPTP, SSL. Назначение, область применения, аутентификация и шифрование данных.
16. Организация защищенного обмена данными в сети с применением сертифицированных систем.
17. Шифрование и обмен шифрованной информацией с использованием системы «PGP».
18. Защита сетевого трафика средствами протокола IPSec в ОС Windows NT 5.0.
19. Организация защищенного документооборота с использованием криптографических средств, предоставляемых СКЗИ «КриптоПро».
20. Защита от подключения устройств не зарегистрированных в системе.
21. Настроить Secret Net для АС класса 3а.
22. Настроить механизм замкнутой программной среды для Secret Net.
23. Установить на ЭВМ СЗИ НСД Dallas Lock.
24. Провести аудит ИБ для ПЭВМ с СЗИ НСД.
25. Настроить механизм контроля устройств для СЗИ НСД.
26. Создайте с использованием СЗИ «StrongDisk» 3 виртуальных диска с различными апараметрами. Для этих дисков в специальном каталоге создайте ложные диски, обеспечьте «правдоподобность» информации на ложных дисках. Проведите эксперимент по экстренному уничтожению дисков.
27. Средствами СЗИ «StrongDisk» гарантированно удалите с дискеты жесткого диска текстовый файл. Убедитесь в надежности удаления данных.
28. С использованием СЗИ «Страж-NT» создать пользователя. Назначить пользователю уровень допуска «Секретно». Создать каталог Секрет, назначить каталогу гриф секретности «Секретно». Для программ Проводник и Блокнот назначить соответствующий режим запуска. Зарегистрироваться пользователем. Продемонстрировать, что пользователь сможет создавать, читать и редактировать текстовые файлы в каталоге «Секретно». Продемонстрировать, что файл, созданный в каталоге «Секретно», а так же его часть, не может быть скопирован в каталог с низшим грифом секретности.
29. С использованием СЗИ «Dallas Lock» создать пользователя. Назначить пользователю уровень допуска «Секретно». Создать каталог Секрет, назначить каталогу гриф секретности «Секретно». Продемонстрировать, что пользователь сможет создавать, читать и редактировать текстовые файлы в каталоге «Секретно». Продемонстрировать, что файл, созданный в каталоге «Секретно», а так же его часть, не может быть скопирован в каталог с низшим грифом секретности.
30. Осуществите криптографическую защиту сетевого трафика средствами ОС Windows 2000. Перехватите в локальной сети пакеты, убедитесь в шифровании трафика.
31. Настройте Web-сервер для организации защищенного доступа к Web-странице с использованием протокола SSL. Файл-сертификат открытого ключа прилагается.
32. Сгенерируйте и получите в виде файла сертификат открытого ключа с использованием ОС Windows Server 2003.
33. Настройте входящее подключение VPN с использованием протокола PPTP. Настройте и установите подключение клиентского узла. Выполнить с использованием ОС Windows Server 2003.

Лист регистрации изменений к РПД

	Номер протокола заседания кафедры, дата утверждения изменения	Количество страниц изменения	Подпись разработчика РПД