Государственное бюджетное образовательное учреждение высшего образования Московской области

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

«УТВЕРЖДАЮ»
Проректор по учебно-методической работе
_____ Н.В. Бабина
«28» апреля 2020 г.

ИНСТИТУТ ТЕХНИКИ И ЦИФРОВЫХ ТЕХНОЛОГИЙ

ФАКУЛЬТЕТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ»

Направление подготовки: 10.03.01 Информационная безопасность

Профиль: Информационно-аналитические системы финансового мониторинга

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Королев
2020

2

Автор: к.т.н. Журавлев С.И. Рабочая программа дисциплины: «Программно-аппаратные средства защиты информации». – Королев МО: «Технологический университет», 2020.

Рецензент: **к.в.н., доцент Соляной В.Н.**

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки бакалавров 10.03.01 «Информационная безопасность» и Учебного плана, утвержденного Ученым советом Университета. Протокол № 9 от 28.04.2020 года.

Рабочая программа рассмотрена и одобрена на заседании кафедры:

Заведующий кафедрой (ФИО, ученая степень, звание, подпись)	к.в.н., доцент Соляной В.Н.			
Год утверждения (переутверждения)	2020	2021	2022	2023
Номер и дата протокола заседания кафедры	Протокол № 8 от 26.03.2020			

Рабочая программа согласована:
Руководитель ОПОП ВО к.в.н., доцент Воронов А.Н.

Рабочая программа рекомендована на заседании УМС:

Год утверждения (переутверждения)	2020	2021	2022	2023
Номер и дата протокола заседания УМС	№ 7 от 28.04.2020			

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ОПОП ВО

Целью изучения дисциплины является формирование у студентов базовых знаний о реализации механизмов и технологий защиты информации в программно-аппаратных средствах и системах защиты информации, а также практических навыков использования штатных средств защиты и специализированных программно-аппаратных средств защиты информации для решения типовых или практических задач.

В процессе обучения студент приобретает и совершенствует следующие компетенции:

Общепрофессиональные компетенции:

- ОПК-2: способность применять соответствующий математический аппарат для решения профессиональных задач.

Профессиональные компетенции:

- ПК-1: способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;
- ПК-6: способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации;
- ПК-9: способность осуществлять подбор, изучение и обобщение научно- технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности.

Основными задачами дисциплины являются:

- формирование у студентов базовых знаний в области реализации технологий защиты информации, основанных на технологиях аутентификации, принципах криптографической защиты информации и криптографических алгоритмах;
- ознакомление с технологиями построения защищенных компьютерных систем, с методами и средствами ограничения доступа к компонентам информационных систем;
- привитие навыков практической работы по инсталяции (установки) программно-аппаратных средств защиты информации на ПЭВМ;
- привитие навыков по использованию программно-аппаратных средств защиты информации для решения типовых или

практических задач, выбору и грамотному использованию программно-аппаратных средств защиты информации при решении практических задач защиты объектов вычислительной техники и сетевого периметра организации.

После завершения освоения данной дисциплины студент должен
Знать:
- основные подходы к защите данных от несанкционированного доступа;
– программно-аппаратные средства шифрования;
– основы построения аппаратных компонент криптозащиты данных, принцип чувствительной области и принцип главного ключа, необходимые и достаточные функции аппаратного средства криптозащиты;
– особенности формирования и применения электронной цифровой подписи (ЭЦП);
– основы построения систем защиты информации локальной вычислительной сети организации с применением современных программно-аппаратных средств защиты информации;
– технологии защиты межсетевого обмена данными, основы построения виртуальных защищенных сетей VPN, защиты на канальном, сеансовом, сетевом уровнях и применяемых протоколах обмена данными;
Уметь:
- инсталлировать и настраивать в соответствии с установленными правилами разграничения доступа программные и программно-аппаратные средства защиты информации;
- использовать технические, программно-аппаратные и программные средства для исключения каналов утечки информации на объектах защиты;
Владеть:
- навыками инсталляции (установки) программно-аппаратных средств защиты информации на объектах защиты;
- способами защиты данных от несанкционированного доступа в информационных системах;
- методологией контроля и разграничение доступа к информационным ресурсам организации, методами и средства ограничения доступа к компонентам ЭВМ.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Программно-аппаратные средства защиты информации» относится к базовой части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность», профиль: «Информационно-аналитические системы финансового мониторинга».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Аппаратные средства вычислительной техники», «Языки программирования», «Информатика», «Основы информационной безопасности», «Математический анализ», «Основы управления информационной безопасностью», «Криптографические методы защиты информации» и компетенциях: ОК-5, ОПК-2,3,4,5,7 и ПК-1,2,4,7,13.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Организация информационно-аналитического обеспечения финансового мониторинга», «Защищённые информационные системы банковской деятельности», «Основы расследования нарушений в финансовой сфере», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

3. Объем дисциплины (модуля) и виды учебной работы

Общая трудоемкость дисциплины составляет 3 зачетные единицы, 108 часов.

Таблица 1

Виды занятий	**Очное отделение**	**Очно-заочное отделение**
	Количество часов	
	7 семестр	-
Общая трудоемкость	108	-
Аудиторные занятия	48	-
Лекции (Л)	16	-
Практические занятия (ПЗ)	16	-
Лабораторные работы (ЛР)	16	-
Курсовая работа (КР)	+	-
Самостоятельная работа	60	-
КСР	-	-
Контрольная работа	-	-
Домашнее задание	-	-
Текущий контроль знаний (7 - 8, 15 - 16 недели)- 2ч.	тест	-
Вид итогового контроля	Экзамен	-

4. Содержание дисциплины

4.1.Темы дисциплины и виды занятий

Таблица 2

Наименование тем	Лекции, час. Очное	Практические занятия, час Очное	Лабораторные занятия, час Очное	Занятия в интерактивной форме, час Очное	Код компетенций
Тема 1. Введение в дисциплину, предмет и задачи программно-аппаратной защиты информации	1	1	1	1.5	ОПК-2; ПК -1,6,9
Тема 2. Идентификация субъекта, понятие протокола идентификации, идентифицирующая информация	1	1	1	1.5	ОПК-2; ПК -1,6,9
Тема 3. Основные подходы к защите данных от НСД	1	1	1	1.5	ОПК-2; ПК -1,6,9
Тема 4. Шифрование, контроль доступа и разграничение доступа, иерархический доступ к файлу, защита сетевого файлового ресурса, фиксация доступа к файлам	1	1	1	1.5	ОПК-2; ПК -1,6,9
Тема 5. Доступ к данным со стороны процесса, способы фиксации факта доступа,	1	1	1	1.5/	ОПК-2; ПК -1,6,9

надежность систем ограничения доступа					
Тема 6. Защита файлов от изменения. Электронная цифровая подпись (ЭЦП).	1	1	1	1.5	ОПК-2; ПК -1,6,9
Тема 7. Программно-аппаратные средства шифрования. Построение аппаратных компонент криптозащиты данных	2	2	2	1.5	ОПК-2; ПК -1,6,9
Тема 8. Защита алгоритма шифрования. Принцип чувствительной области и принцип главного ключа, необходимые и достаточные функции аппаратного средства криптозащиты. Пароли и ключи, организация хранения ключей	2	2	2	1.5	ОПК-2; ПК -1,6,9
Тема 9. Методы и средства ограничения доступа к компонентам ЭВМ	2	2	2	1	ОПК-2; ПК -1,6,9
Тема 10. Защита программ от несанкционированного копирования. Защита программ от изучения; защита от отладки, защита от дизассемблирования, защита от трассировки по	2	2	2	1	ОПК-2; ПК -1,6,9

прерываниям.					
Тема 11. Защита от разрушающих программных воздействий (РПВ). Компьютерные вирусы как особый класс РПВ. Необходимые и достаточные условия недопущения разрушающего воздействия. Понятие изолированной программной среды.	2	2	2	4	ОПК-2; ПК -1,6,9
Итого:	**16**	**16**	**16**	**18**	

4.2. Содержание тем дисциплины

Тема 1. Введение в дисциплину, предмет и задачи программно-аппаратной защиты информации

1. Основные понятия защиты информации и информационной безопасности. Компоненты информационных систем.

2. Предмет и задачи программно-аппаратной защиты информации. Программно-аппаратные средства и комплексы защиты персональных ЭВМ и информационных систем.

3. Компьютерная система (КС). Структура и компоненты КС. Классы и типы КС. Сети ЭВМ.

4. Электронный документ (ЭД). Понятие ЭД. Типы ЭД. Понятие исполняемого модуля.

5. Виды информации в КС. Информационные потоки в КС.

Тема 2. Идентификация субъекта, понятие протокола идентификации, идентифицирующая информация

1. Понятие доступа, субъект и объект доступа. Понятие несанкционированного доступа (НСД). Классы и виды НСД. Несанкционированное копирование программ как особый вид НСД.

2. Понятие злоумышленника; злоумышленник в криптографии и при решении проблем компьютерной безопасности (КБ).

3. Основные понятия и определения процесса идентификации, идентифицирующая информация; требования к идентификации и

аутентификации, возможные классификации механизмов авторизации, реализованных в системах защиты информации.

4. Управление доступом на основе использования механизмов идентификации, аутентификации и авторизации. Понятие протокола идентификации, их категории, «слабая» и «сильная» идентификация, личные идентификационные номера, атаки на протоколы идентификации.

Тема 3. Основные подходы к защите данных от НСД

1. Способы и приемы НСД, несанкционированный доступ как вид компьютерных нарушений. Основные методы реализации угроз информационной безопасности. Технические средства несанкционированного доступа к информации.

2. Основные подходы к защите данных от НСД в широком смысле и узком. Защита данных: от наблюдения и фотографирования; от подслушивания; от незаконного подключения к линиям связи; от радиоперехвата.

3. Методы и средства ограничения доступа к компонентам информационных систем. Система разграничения доступа к информации, ее состав и выполняемые функции. Диспетчер доступа, его функциональная схема и особенности работы.

Тема 4. Шифрование, контроль доступа и разграничение доступа, иерархический доступ к файлу, защита сетевого файлового ресурса, фиксация доступа к файлам

1. Технологии построения безопасной среды функционирования электронного бизнеса: аутентификация; управление доступом; шифрование; цифровая подпись.

2. Основные понятия криптографической защиты информации, обобщенная схема криптосистемы шифрования. Симметричные, ассиметричные и комбинированные криптосистемы шифрования.

3. Основные типы управления доступом в информационных системах. Контроль доступа пользователей к ресурсам информационной системы. Модели управления доступом.

4. Особенности управления доступом в распределенной корпоративной сети, средства управления сетевым доступом и Web-доступом. Организация защищенного удаленного доступа, протоколы аутентификации удаленных пользователей, централизованный контроль удаленного доступа.

5. Контроль доступа к файлам, иерархический доступ к файлу, защита сетевого файлового ресурса. Управление доступом по схеме однократного входа с авторизацией SSO. Использование протокола Kerberos. Фиксация доступа к файлам. (17-03-2015 ИБО-03).

Тема 5. Доступ к данным со стороны процесса, способы фиксации факта доступа, надежность систем ограничения доступа.

1. Проблемы безопасности программного обеспечения. Процесс, как субъект доступа.
2. Необходимость защиты программ обработки данных; механизмы защиты процессов, процедур и программ обработки данных; фиксации факта доступа.
3. Уровни защиты процедур и программ. Оценка надежности систем ограничения доступа, понятия отказа и его характеристики, время восстановления системы защиты и ее коэффициент готовности.

Тема 6. Защита файлов от изменения. Электронная цифровая подпись (ЭЦП).

Защита файлов от изменения с использованием алгоритмов контроля целостности программ и данных. ЭЦП и использование алгоритма хэш-функции. Основные процедуры цифровой подписи.

Тема 7. Программно-аппаратные средства шифрования. Построение аппаратных компонент криптозащиты данных

Основные характеристики и особенности построения лицензионных и сертифицированных в Российской Федерации программно-аппаратных средств шифрования. Построение аппаратных компонент криптозащиты данных.

Тема 8. Защита алгоритма шифрования. Принцип чувствительной области и принцип главного ключа, необходимые и достаточные функции аппаратного средства криптозащиты. Пароли и ключи, организация хранения ключей

Стойкость шифров, возможные криптоатаки для вскрытия шифртекстов. Защита алгоритма шифрования.

Принцип чувствительной области и принцип главного ключа, необходимые и достаточные функции аппаратного средства криптозащиты. Хранения ключевой информации. Пароли и ключи, организация хранения ключей.

Секретная информация, используемая для контроля доступа: ключи и пароли. Злоумышленник и ключи. Классификация средств хранения ключей и идентифицирующей информации. Организация хранения ключей (с примерами реализации) Магнитные диски прямого доступа. Магнитные и интеллектуальные карты. Средство TouchMemory.

Типовые решения в организации ключевых систем Открытое распределение ключей. Метод управляемых векторов.Управление криптоключами, метод распределения ключей Диффи-Хеллмана.

Тема 9. Методы и средства ограничения доступа к компонентам ЭВМ

Классификация защищаемых компонент ПЭВМ: отчуждаемые и неотчуждаемые компоненты ПЭВМ. Процесс начальной загрузки ПЭВМ, взаимодействие аппаратной и программной частей.

Механизмы расширения BIOS, структура расширенного BIOS. Преимущества и недостатки программных и аппаратных средств. Проблемы использования расширений BIOS: эмуляция файловой системы до загрузки ОС и т. д. Проблема защиты отчуждаемых компонентов ПЭВМ Способы защиты информации на съемных дисках.

Организация прозрачного режима шифрования. Надежность средств защиты компонент. Понятие временной и гарантированной надежности.

Защита средств управления, коммутации и внутреннего монтажа компьютерных систем. Метод контроля вскрытия аппаратуры. Комплексирование механизмов защиты информации от НСД.

Тема 10. Защиты программ от несанкционированного копирования. Защита программ от изучения; защита от отладки, защита от дизассемблирования, защита от трассировки по прерываниям

Особенности защиты программных средств в процессе эксплуатации. Способы защиты программ от несанкционированного копирования. Методы противодействия дизассемблированию. Защита программ от отладки и от трассировки по прерываниям. Защита программного обеспечения от изучения.

Тема 11. Защита от разрушающих программных воздействий (РПВ). Компьютерные вирусы как особый класс РПВ. Необходимые и достаточные условия недопущения разрушающего воздействия. Понятие изолированной программной среды

5. Перечень учебно-методического обеспечения для самостоятельной работы по дисциплине

1. «Методические указания для обучающихся по освоению дисциплины» приведены в приложении 2.

6. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

Структура фонда оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине «Программно-аппаратные средства защиты информации» приведена в Приложении 1.

7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

Рекомендуемая литература.

Основная литература:

1. А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков и др.: под редакцией А.П. Зайцева и А.А. Шелупанова. Технические средства и методы защиты информации. Учебное пособие для вузов. – 4-е издание исправленное и дополненное. - М.: Горячая линия – Телеком, 2012. - 616с
2. Рябко Б.Я., Фионов А.Н. Основы современной криптографии и стеганографии – 2-е издание- М.: Горячая линия – Телеком, 2013. – 232с.
3. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах: Учебное пособие для вузов. – 4-е издание, стереотип- М.: Горячая линия – Телеком, 2011. - 146с.
4. А.И. Баранчиков, П.А. Баранчиков, А.Н. Пылькин Алгоритмы и модели ограничения доступа к записям баз данных. - М. Горячая линия – Телеком, 2011 – 182с.
5. А.Ф. Чепига Информационная безопасность автоматизированных систем. М.: «Гелиос АРВ», 2010. -336с.
6. В.Ф. Шаньгин Комплексная защита информации в корпоративных системах. М.: ИД «Форум»: ИНФРА-М., 2010.-592с.
7. О.А.Романов, С.А. Бабин, С.Г. Жданов Организационное обеспечение информационной безопасности М.: Издательский центр «Академия», 2008,-192.
8. Васильков А.В., Васильков А.А., Васильков И.А. Информационные системы и их безопасность М.: ФОРУМ, 2011,-528с.

Дополнительная литература:

1. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей. Учебное пособие. 2008. Москва, «ИД ФОРУМ – ИНФРА-М».
2. Малюк А.А. Теория защиты информации.-М.:Горячая линия-Телеком,2012.
3. Хорев П.Б. Программно-аппаратная защита информации. М.: ФОРУМ, 2009г.-352с.
4. В.А.Северин. Комплексная защита информации на предприятии. М.: Издательский дом «Городец»,2008.- 368с.
5. Мельников В.П. идр Информационная безопасность.М.: Издателский центр «Академия» , 2008.-336с.
6. Шепитько Г.Е. Теория информационной безопасности и методология защиты информации. – М.: РГСУ, 2012

Электронные книги:

1. Метод пособие Анализ рисков в области ЗИ. Изд.дом «Афина» (www.inside – zi.ru) 2009.

2. Метод. пособие Защита конфиденциальной информации. Изд.дом «Афина» (www.inside – zi.ru) 2009.
3. Метод. пособие Обеспечение безопасности персональных данных. Изд.дом «Афина» (www.inside – zi.ru) 2010.
4. www.biblioclub.ru
5. www.rucont.ru.

8. Перечень ресурсов информационно-телекоммуникационной сети Интернет, необходимых для освоения дисциплины (модуля).

1. ISO27000.ru (портал по ИБ, аналитика, информация по законодательству и стандартам, блоги, каталоги ресурсов и ПО).
2. wikIsec - Энциклопедия ИБ (публикации, статьи).
3. WinSecurity.ru (статьи, документация, новости по безопасности Windows).
4. Журнал Информационная безопасность (публикации, статьи, обзоры, форум).
5. http://www.minfin.ru - официальный сайт Министерства финансов Российской Федерации.
6. http://www.gov.ru - сервер органов государственной власти Российской Федерации.

9. Методические указания для обучающихся по освоению дисциплины

Методические указания для обучающихся, по освоению дисциплины, приведены в Приложении 2.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

Перечень программного обеспечения: *MSOffice*

Информационные справочные системы:

1. Ресурсы информационно-образовательной среды МГОТУ
2. Рабочая программа и методическое обеспечение по дисциплине: «Программно-аппаратные средства защиты информации»

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Лекционные занятия:

- аудитория, оснащенная презентационной техникой (проектор, экран);
- комплект электронных презентаций/слайдов.

Практические занятия:

- компьютерный класс с проектором для интерактивного обучения и проведения занятий в форме слайд-презентаций, оборудованный современными лицензионными программно-техническими средствами:

операционная система не ниже WindowsXP, эмуляции виртуальных машин (VM-vare, VM-box или др.)

- рабочее место преподавателя, оснащенное компьютером с доступом в Интернет;
- рабочие места студентов, оснащенные компьютерами с доступом в Интернет.

Лабораторные занятия:

- компьютерный класс с проектором для интерактивного обучения и проведения занятий в форме слайд-презентаций, оборудованный современными лицензионными программно-техническими средствами: операционная система не ниже WindowsXP, эмуляции виртуальных машин (VM-vare, VM-box или др.)
- рабочее место преподавателя, оснащенное компьютером с доступом в Интернет;
- рабочие места студентов, оснащенные компьютерами с доступом в Интернет.

Приложение 1

ИНСТИТУТ ТЕХНИКИ И ЦИФРОВЫХ ТЕХНОЛОГИЙ

ФАКУЛЬТЕТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

«ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ»

(Приложение 1 к рабочей программе)

Направление подготовки: 10.03.01 Информационная безопасность

Профиль: Информационно-аналитические системы финансового мониторинга

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Королев
2020

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

№ п/п	Индекс компе-тенции	Содержание компетенции (или ее части)*	Раздел дисциплины, обеспечивающий формирование компетенции (или ее части)	В результате изучения раздела дисциплины, обеспечивающего формирование компетенции (или ее части), обучающийся должен:		
				Знать	уметь	владеть
1.	ОПК-2	способность применять соответствующий математический аппарат для решения профессиональных задач	Тема 1,3,4,5,8,9	основные подходы к защите данных от несанкционированного доступа;	инсталлировать и настраивать в соответствии с установленными правилами разграничения доступа программные и программно-аппаратные средства защиты информации;	навыками инсталляции (установки) программно-аппаратных средств защиты информации на объектах защиты;
2.	ПК-1	способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Тема 1,3,4,5,8,9	основные подходы к защите данных от несанкционированного доступа;	инсталлировать и настраивать в соответствии с установленными правилами разграничения доступа программные и программно-аппаратные средства защиты информации;	навыками инсталляции (установки) программно-аппаратных средств защиты информации на объектах защиты;
3.	ПК-6	способность принимать участие в организации и проведении контрольных проверок работоспособности и и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	Тема 1-5,8,9	программно-аппаратные средства шифрования;	Выделять компоненты системы, способствующие нарушению целостности и доступности информации, а также ее утечке по техническим каналам	Навыками системного подхода к решению поставленной задачи
4.	ПК-9	способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и	Темы 1-3,8,9	технологии защиты межсетевого обмена данными, основы построения виртуальных	Выбирать методические и нормативные документы в соответствии с решаемой задачей	способами защиты данных от несанкционированного доступа в информационных системах;

		методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности		защищенных сетей VPN, защиты на канальном, сеансовом, сетевом уровнях и применяемых протоколах обмена данными;		

2.Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Код компетенции	Инструменты, оценивающие сформированность компетенции	Показатель оценивания компетенции	Критерии оценки
ОПК-2	Доклад в форме презентации	A) полностью сформирована **5 баллов** B) частично сформирована **3-4 балла** C) не сформирована **2 балла**	Проводится устно с использованием мультимедийных систем, а также с использованием технических средств Время, отведенное на процедуру – 10 - 15 мин. Неявка – 0. Критерии оценки: 1.Соответствие представленной презентации заявленной тематике (1 балл). 2.Качество источников и их количество при подготовке доклада и разработке презентации (1 балл). 3.Владение информацией и способность отвечать на вопросы аудитории (1 балл). 4.Качество самой представленной презентации (1 балл). 5.Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл). Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся непосредственно в день проведения презентации – для текущего контроля. Оценка проставляется в электронный журнал.
ПК-1	Доклад в форме презентации	A) полностью сформирована **5 баллов** B) частично сформирована **3-4 балла** C) не сформирована **2 балла**	Проводится устно с использованием мультимедийных систем, а также с использованием технических средств Время, отведенное на процедуру – 10 - 15 мин. Неявка – 0. Критерии оценки: 1.Соответствие представленной презентации заявленной тематике (1 балл). 2.Качество источников и их количество при подготовке доклада и разработке презентации (1 балл). 3.Владение информацией и способность отвечать на вопросы аудитории (1 балл). 4.Качество самой представленной презентации (1 балл). 5.Оригинальность подхода и

			всестороннее раскрытие выбранной тематики (1 балл). Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся непосредственно в день проведения презентации – для текущего контроля. Оценка проставляется в электронный журнал.
ПК-6	Доклад в форме презентации	А) полностью сформирована **5 баллов** В) частично сформирована **3-4 балла** С) не сформирована **2 балла**	Проводится устно с использованием мультимедийных систем, а также с использованием технических средств Время, отведенное на процедуру – 10 - 15 мин. Неявка – 0. Критерии оценки: 1.Соответствие представленной презентации заявленной тематике (1 балл). 2.Качество источников и их количество при подготовке доклада и разработке презентации (1 балл). 3.Владение информацией и способность отвечать на вопросы аудитории (1 балл). 4.Качество самой представленной презентации (1 балл). 5.Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл). Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся непосредственно в день проведения презентации – для текущего контроля. Оценка проставляется в электронный журнал.
ПК-9	Доклад в форме презентации	А) полностью сформирована **5 баллов** В) частично сформирована **3-4 балла** С) не сформирована **2 балла**	1. Проводится устно в форме защиты отчета 2.Время, отведенное на процедуру – 10 - 15 мин. Неявка – 0. Критерии оценки: 1.Соответствие оформления требованиям (1 балл). 2. Соответствие разработанного устройства техническому заданию (1 балл) 3. Моделирование работы разработанного устройства (1 балл) 4. Качество и количество используемых источников (1 балл)

			5. Правильность и полнота ответов на контрольные вопросы (1 балл) Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся непосредственно после защиты – для текущего контроля. Оценка проставляется в электронный журнал.

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

Примерная тематика докладов в форме презентации:

1. Автоматизация процесса обработки конфиденциальной информации и меры по ее защите.
2. Определение актуальных угроз безопасности компьютерных систем и выработка требований по минимизации рисков.
3. Исследование и совершенствование механизмов идентификации и аутентификации пользователей компьютерных систем.
4. Совершенствование системы защиты информации предприятия (фирмы) на основе комплексного применения программно-аппаратных средств защиты информации.
5. Разработка и обоснование требований к системе защиты информации предприятия (фирмы) и рекомендаций по её эффективному наращиванию.
6. Разработка проекта системы защиты информации локальной вычислительной сети организации.
7. Исследование воздействий программных закладок на компьютеры и разработка мероприятий по их минимизации.
8. Совершенствование системы защиты информации компьютерной системы предприятия при использовании механизмов безопасности на аппаратном уровне.
9. Совершенствование системы защиты информации предприятия (фирмы) при использовании средств защиты в составе вычислительной системы.
10. Исследование и совершенствование методов управления криптографическими ключами и хранения ключевой информации.

4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Формой контроля знаний по дисциплине «Программно-аппаратные средства защиты информации» являются две текущие аттестации в виде тестов и итоговая аттестация в виде экзамена.

Неделя текущего контроля	Вид оценочного средства	Код компетенций, оценивающий знания, умения, навыки	Содержание оценочного средства	Требования к выполнению	Срок сдачи (неделя семестра)	Критерии оценки по содержанию и качеству с указанием баллов
Согласно учебному плану	тестирование	ОПК-2; ПК-1; ПК-6; ПК-9	20 вопросов	Компьютерное тестирование ; время отведенное на процедуру - 30 минут	Результаты тестирования предоставляются в день проведения процедуры	Критерии оценки определяются процентным соотношением. Не явка - Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%.
Согласно учебному плану	тестирование	ОПК-2; ПК-1; ПК-6; ПК-9	20 вопросов	Компьютерное тестирование; время отведенное на процедуру – 30 минут	Результаты тестирования предоставляются в день проведения процедуры	Критерии оценки определяются процентным соотношением. Не явка -0 Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%. Максимальная оценка – 5 баллов.
Согласно учебному плану	Экзамен	ОПК-2; ПК-1; ПК-6; ПК-9	3 вопроса	Экзамен проводится в письменной форме, путем ответа на вопросы. Время, отведенное на процедуру – 30 минут.	Результаты предоставляются в день проведения экзамена	Критерии оценки: «**Отлично**»: 1. знание основных понятий предмета; 2. умение использовать и применять полученные знания на практике; 3. работа на практически

						х занятиях; 4. знание основных научных теорий, изучаемых предметов; 5. ответ на вопросы билета. «**Хорошо**»: • знание основных понятий предмета; • умение использовать и применять полученные знания на практике; • работа на практических занятиях; • знание основных научных теорий, изучаемых предметов; • ответы на вопросы билета • неправильно решено практическое задание «У**довлетвори-тельно**»: 1. демонстрирует частичные знания по темам дисциплин; 2. незнание неумение использовать и применять полученные знания на практике; 3. не работал на

						практических занятиях; «**Неудовлетвори-тельно**»: 4. демонстрирует частичные знания по темам дисциплин; 5. незнание основных понятий предмета; 6. неумение использовать и применять полученные знания на практике; 7. не работал на практических занятиях; 8. не отвечает на вопросы.

4.1. Типовые вопросы, выносимые на тестирование

Тесты используются в режиме промежуточного контроля. По форме заданий выбраны закрытые тесты (с выборочным ответом). Каждому вопросу соответствует один вариант ответа.

1. Что относится к атрибутивным идентификаторам, которые используются для идентификации субъекта доступа в КС?
2. Каким требованиям должна удовлетворять подсистема аудита ОС.
3. Какую последовательность действий включает общий алгоритм механизма защиты от несанкционированного использования программ в «чужой» среде?
4. Как называется код, использующийся для аутентификации и авторизации в кредитных, банковских и сим-картах?
5. В соответствии со стандартом X.509 какого типа строгой аутентификации НЕ существует?
6. В какой криптосистеме для шифрования и расшифрования используется один и тот же ключ?

7. В какой криптосистеме для шифрования и расшифрования используется разные ключи?

8. Что используется для проверки целостности документов и установления лица, отправившего документ?

4. Как называется код, использующийся для аутентификации и авторизации в кредитных, банковских и сим-картах?

5. В соответствии со стандартом X.509 какого типа строгой аутентификации НЕ существует?

6. В какой криптосистеме для шифрования и расшифрования используется один и тот же ключ?

7. В какой криптосистеме для шифрования и расшифрования используется разные ключи?

8. Что используется для проверки целостности документов и установления лица, отправившего документ?

9. Какие применяют средства для ограничения доступа к компонентам ЭВМ.

10. Последовательность жизненного цикла компьютерных вирусов?

11. Субъект доступа – это…

12. К методам противодействия дизассемблированию программ для ЭВМ относится:

13. Аутентификация – это…

14. Матрица доступа – это…

15. Домен безопасности – это…

16. Односторонняя хэш-функция используется для:

17. Для чего создается система разграничения доступа (СРД) компьютерной системы?

18. В чем заключается биометрическая аутентификация пользователей?

4.2. Типовые вопросы, выносимые на экзамен

1. Перечислите защитные механизмы, реализуемые программно-аппаратными комплексами (средствами) защиты информации в компьютерных системах (ПЭВМ). Дайте определение понятию - «субъект доступа», какие процедуры реализуются при его обращении к компьютерной системе.

2. Перечислите методы противодействия дизассемблированию программ для ЭВМ, охарактеризуйте их.

3. В чем заключается процедура простой аутентификации, какими способами она производится, поясните схематично ее реализацию с использованием пароля.

4. Перечислите основные модели разграничения доступа, действующие в операционных системах, и поясните, в чем они заключаются. Дайте определение понятиям «матрица доступа» и «домен безопасности».

5. Поясните использование односторонней хэш-функции для проверки пароля при аутентификации пользователя ресурсов компьютерной системы.

6. Чем достигается защита средств управления, коммутации и внутреннего монтажа компьютерных систем (ПЭВМ), из чего состоит и как действует единая система контроля вскрытия устройств (СКВУ).

7. Для чего создается система разграничения доступа (СРД) компьютерной системы, какие функциональные блоки она включает. Поясните работу функциональной схемы диспетчера доступа.

8. В чем заключается биометрическая аутентификация пользователей, какие у нее достоинства и недостатки.

9. Дайте определение основным понятиям процесса разграничения доступа к объектам операционной системы (ОС): «объект доступа»; «метод доступа»; «субъект доступа»; «право доступа». Каким требованиям должны удовлетворять правила разграничения доступа.

10. Приведите примеры сущностей субъекта доступа для подтверждения своей подлинности при осуществлении аутентификации в компьютерной системе (ПЭВМ).

11. Какими способами блокируется угроза несанкционированного копирования информации ПЭВМ, в чем они заключаются, раскройте их содержание.

12. В зависимости от предъявления субъектом доступа каких сущностей можно разделить процессы аутентификации в компьютерных системах (ПЭВМ)?

13. Основные подходы к защите данных от НСД: какие действия выполняются при организации доступа к оборудованию и ПО компьютерных систем (ПЭВМ); оценка эффективности наращивания средств контроля доступа по кривой роста относительного уровня обеспечения безопасности компьютерных систем (ПЭВМ).

14. Перечислите атрибутивные идентификаторы, используемые для идентификации субъекта доступа в КС, и коротко дайте им определение.

15. Какие основные функции выполняет подсистема защиты операционных систем (ОС), дайте коротко им определение. В чем заключается процедура аудита применительно к ОС, чем она обусловлена, каким требованиям она должна удовлетворять.

16. Какую последовательность действий включает общий алгоритм механизма защиты от несанкционированного использования программ в «чужой» среде.

17. Раскройте методы аутентификации, использующие пароли и PIN-коды.

18. Перечислите и раскройте способы строгой аутентификации.

19. Какие существуют криптосистемы шифрования, раскройте их смысл функционирования.

20. Раскройте основные процедуры формирования электронной цифровой подписи и функции хэширования.

21. Как осуществляется управление криптоключами, требования к распределению ключей, методы распределения ключей.

22. Раскройте классификацию и жизненный цикл компьютерных вирусов.

23. Перечислите методы ограничения доступа к компонентам ЭВМ, какие применяют средства для ограничения доступа к компонентам ЭВМ.

24. 12. В чем заключается задача идентификации пользователя, дайте определение понятию протокола идентификации.

25.В чем заключается локальная и удаленная идентификация, что такое идентифицирующая информация.

26.Какие существуют способы хранения идентифицирующей информации, их связь с ключевыми системами.

Приложение 2

ИНСТИТУТ ТЕХНИКИ И ЦИФРОВЫХ ТЕХНОЛОГИЙ

ФАКУЛЬТЕТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

«ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ»

(Приложение 2 к рабочей программе)

Направление подготовки: 10.03.01 Информационная безопасность

Профиль: Информационно-аналитические системы финансового мониторинга

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Королев
2020

1. Общие положения

Цель дисциплины:

- приобретение студентами знаний и представлений об основных принципах и закономерностях функционирования современной вычислительной техники ;
- приобретение студентами теоретических сведений и практических навыков, позволяющих формировать устройства вычислительной техники с заданными техническими характеристиками.

Задачи дисциплины:

- формирование представлений о принципах обеспечения информационной безопасности при использовании вычислительной техники;
- изучение принципов построения и работы основных цифровых узлов;
- приобретение опыта выбора элементной базы и типовых цифровых узлов вычислительной техники.

2. Указания по проведению практических занятий

Практическое занятие 1. Предмет и задачи программно-аппаратной защиты информации.

Учебные вопросы.

1. Компьютерная система (КС). Структура и компоненты КС. Классы и типы КС. Сети ЭВМ.
2. Основные понятия программно-аппаратной защиты информации: электронный документ (ЭД) и их типы; виды информации в КС; информационные потоки в КС; понятие исполняемого модуля.
3. Уязвимость компьютерных систем: понятие доступа, субъект и объект доступа; понятие несанкционированного доступа (НСД); классы и виды НСД; несанкционированное копирование программ как особый вид НСД; понятие злоумышленника; злоумышленник в криптографии и при решении проблем компьютерной безопасности (КБ).

Продолжительность занятия — 3 часа

Практическое занятие 2. Идентификация пользователей КС - субъектов доступа к данным.

Учебные вопросы.

1. Понятие идентификации пользователя.
2. Задача идентификации пользователя.
3. Понятие протокола идентификации.
4. Локальная и удаленная идентификация.

5. Идентифицирующая информация. Понятие идентифицирующей информации.
6. Способы хранения идентифицирующей информации, связь с ключевыми системами.

Продолжительность занятия — 3 часа

Практическое занятие 3. Средства и методы ограничения доступа к файлам.

Учебные вопросы.

1. Основные подходы к защите данных от НСД: шифрование; контроль доступа; рзграничения доступа; файл как объект доступа; оценка надежности систем ограничения доступа - сведение к задаче оценки стойкости.
2. Организация доступа к файлам: иерархический доступ к файлам; понятие атрибутов доступа; организация доступа к файлам в различных ОС; защита сетевого файлового ресурса на примерах организации доступа в ОС UNIX, Novell NetWare и т. д.
3. Фиксация доступа к файлам: способы фиксации фактов доступа; журналы доступа; критерии информативности журналов доступа; выявление следов несанкционированного доступа к файлам; метод инициированного НСД.
4. 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.
5. Особенности защиты данных от изменения: зашита массивов информации от изменения (имитозащита); криптографическая постановка защиты от изменения данных; подходы к решению задачи защиты данных от изменения; подход на основе формирования имитоприставки (MAC), способы построения MAC; 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.

Продолжительность занятия — 3 часа

Практическое занятие 4. Программно-аппаратные средства шифрования

Учебные вопросы.

1. Построение программно-аппаратных комплексов шифрования: аппаратные и программно-аппаратные средства криптозащиты данных; построение аппаратных компонент криптозащиты данных, специализированные СБИС как носители алгоритма шифрования.
2. Защита алгоритма шифрования, принцип чувствительной области и принцип главного ключа.

3. Необходимые и достаточные функции аппаратного средства криптозащиты, проектирование модулей криптопреобразований на основе сигнальных процессоров.
4. Плата Криптон-3 (Криптон-4): архитектура платы; организация интерфейса с приложениями. 5. Другие программно-аппаратные СКЗД.

Продолжительность занятия — 3 часа

Практическое занятие 5. Защита программ от несанкционированного копирования

Учебные вопросы.

1. Несанкционированное копирование программ: несанкционированное копирование программ как тип НСД; юридические аспекты несанкционированного копирования программ; общее понятие защиты от копирования. Разновидности задач защиты от копирования.
2. Подходы к задаче защиты от копирования: привязка ПО к аппаратному окружению и физическим носителям как единственное средство защиты от копирования ПО; привязка программ к гибким магнитным дискам (ГМД); структура данных на ГМД; управление контроллером ГМД; способы создания некопируемых меток; точное измерение характеристик форматирования дорожки; технология «слабых битов»; физические метки и технология работы с ними; привязка программ к жестким магнитным дискам (ЖМД); особенности привязки к ЖМД; виды меток на ЖМД; привязка к прочим компонентам штатного оборудования ПЭВМ; привязка к внешним (добавляемым) элементам ПЭВМ; привязка к портовым ключам; использование дополнительных плат расширения; методы «водяных знаков» и методы «отпечатков пальцев».

Продолжительность занятия — 2 часа

Практическое занятие 6. Защита программ от изучения

Учебные вопросы.

1. Изучение и обратное проектирование ПО: понятие изучения и обратного проектирования ПО; цели и задачи изучения работы ПО; способы изучения ПО: статическое и динамическое изучение; роль программной и аппаратной среды; временная надежность (невозможность обеспечения гарантированной надежности).
2. Задачи защиты от изучения и способы их решения: защита от отладки; динамическое преобразование кода; итеративный программный замок А. Долгина; принцип ловушек и избыточного кода; защита от дизассемблирования; принцип внешней загрузки файлов; динамическая модификация программы; защита от трассировки по прерываниям.
3. Аспекты проблемы защиты от исследования: способы ассоциирования защиты и программного обеспечения; оценка надежности защиты от отладки.
4. Вирусы: защита от разрушающих программных воздействий; вирусы как особый класс разрушающих программных воздействий;

необходимые и достаточные условия недопущения разрушающего воздействия; понятие изолированной программной среды.

Продолжительность занятия — 2 часа

3. Указания по проведению курсовой работы (проекта)

Курсовые работы (проекты)

В процессе обучения студенты выполняют курсовую работу, задание на которую разрабатывается индивидуально для каждого студента и выдается на первом аудиторном занятии. Срок выполнения курсовой работы – 6-ая неделя семестра. Отчет по контрольной работе должен содержать требования к программно-аппаратным средствам защиты информации.

3.1 Перечень тематик курсовых работ (проектов)

1. Автоматизация процесса обработки конфиденциальной информации и меры по ее защите.
2. Определение актуальных угроз безопасности компьютерных систем и выработка требований по минимизации рисков.
3. Исследование и совершенствование механизмов идентификации и аутентификации пользователей компьютерных систем.
4. Совершенствование системы защиты информации предприятия (фирмы) на основе комплексного применения программно-аппаратных средств защиты информации.
5. Разработка и обоснование требований к системе защиты информации предприятия (фирмы) и рекомендаций по её эффективному наращиванию.
6. Разработка проекта системы защиты информации локальной вычислительной сети организации.
7. Исследование воздействий программных закладок на компьютеры и разработка мероприятий по их минимизации.
8. Совершенствование системы защиты информации компьютерной системы предприятия при использовании механизмов безопасности на аппаратном уровне.
9. Совершенствование системы защиты информации предприятия (фирмы) при использовании средств защиты в составе вычислительной системы.
10. Исследование и совершенствование методов управления криптографическими ключами и хранения ключевой информации.

3.2 Методические указания по выполнению курсовых работ

Цель курсовой работы – закрепление теоретических знаний, полученных при
освоении дисциплины, и их адаптация к конкретной предметной области.
Выбор темы курсовой работы осуществляется студентом либо самостоятельно, либо с помощью преподавателя.

На титульном листе указывается: наименование учреждения образования; факультета и кафедры; полное наименование дисциплины (записывается с прописной буквы); тема курсовой работы; шифр учебной группы; фамилия, имя, отчество студента в родительном падеже; фамилия и инициалы преподавателя.

Оформление курсовой работы:

- текст должен быть напечатан на одной стороне листа белой бумаги формата А4;
- работу выполнять шрифтом Times New Roman;
- размер шрифта -14;
- межстрочный интервал -1,5;
- поля: 30 мм — левое, 20 мм - правое, 20 мм — верхнее и нижнее;
- применять сквозную нумерацию страниц;
- объем работы-10-12 страниц.

Курсовые работы выполнять в строгом соответствии с вариантом студента, утвержденным преподавателем.

Текст работы должен быть написан в строгом соответствии с правилами русской орфографии, синтаксиса и пунктуации. Описки, ошибки при расчетах, обнаруженные в процессе выполнения курсовой работы, допускается исправлять аккуратной подчисткой и нанесением на том же месте исправленного текста.

В конце курсовой работы приводится перечень использованной литературы.

В конце курсовой работы необходимо ставить подпись и дату.

Дата написания (завершения) курсовой работы проставляется после списка использованной литературы в левой части страницы, а подпись студента - с правой части страницы. Оформляется дата двумя способами: словесно-числовым или только числовым (арабскими цифрами), например 1 января 2012 г. или 01. 01.2012.

Примечание:

- Курсовая работа, оформленная небрежно, а также выполненная по неправильно выбранному варианту, возвращается студенту без проверки с указанием причин возврата.
- В случае выполнения работы по неправильно выбранному варианту студент должен выполнить работу согласно своему варианту задания.
- Не засчитывается и возвращается студенту на доработку с подробной рецензией курсовая работа, если в ней не раскрыты теоретические вопросы задания или ответы на них полностью переписаны из учебной литературы, без адаптации к конкретному заданию.
- Доработанный вариант незачтенной курсовой работы представляется на рецензирование вместе с прежним вариантом, при этом правильно выполненная часть задания не переписывается.
- Студенты, не выполнившие курсовую работу, к итоговой аттестации не допускаются.

Сроки сдачи курсовой работы определяются техническим заданием, выданным преподавателем.

4. Указания по проведению самостоятельной работы студентов

На практических занятиях рассматриваются вопросы численного расчета и анализа электрических цепей, рассмотренных на лекционных занятиях, либо изученных в процессе самостоятельной работы. Поэтому перед практическим занятием следует повторить тот теоретический материал, по которому будет проводиться практическое занятие.

При подготовке к лабораторным работам следует повторить теоретический материал, по теме которого будет проводиться лабораторная работа. Необходимо также выполнить предварительное задание, которое предшествует каждой лабораторной работе, и, для закрепления материала, ответить на контрольные вопросы.

Самостоятельная работа включает в себя закрепление материала, полученного на лекционных занятиях, подготовку к практическим и лабораторным занятиям и выполнение контрольных работ и домашних заданий.

Объем времени на самостоятельную работу, и виды самостоятельной работы представлены в таблице 1.

Таблица 1

Объем времени и виды самостоятельной работы

Виды самостоятельной работы	**Очная форма обучения**
	Всего академических часов
Всего часов на самостоятельную работу	**60**
Вопросы, выносимые на самостоятельное изучение	18
Подготовка к практическим занятиям	12
Подготовка к лабораторным занятиям	8
Подготовка докладов	10
Выполнение практических заданий	12

Тематическое содержание самостоятельной работы представлено в таблице 2.

Таблица 2

Тематическое содержание самостоятельной работы

№ п/п	**Виды самостоятельной работы**	**Количество часов**	**Перечень заданий**
1.	Вопросы, выносимые на самостоятельное изучение	18	Изучение открытых источников
2.	Подготовка к практическим занятиям	12	Изучение открытых источников при подготовке доклада на выбранную тему.
3.	Подготовка к лабораторным занятиям	8	Изучение открытых источников
4.	Тематика докладов	10	1. Внутренние аппаратные средства персонального компьютера 2. Внешние периферийные устройства персонального

			компьютера
5.	Выполнение практических заданий	12	Разработка аппаратного средства вычислительной техники по заданным характеристикам

К выполнению контрольных работ и домашних заданий следует приступать после проработки материала лекций по конспекту и по учебникам. Необходимо повторить также аналогичный материал, рассмотренный на практических занятиях. Сроки выполнения, варианты заданий и требования к содержанию определены в п.5.5. Качество выполнения работ проверяется путем моделирования рассчитываемых устройств и сравнения результатов моделирования с полученными расчетным путем.

5. Указания по проведению лабораторных работ

5.1. Требования к структуре

Структура лабораторной работы должна способствовать раскрытию темы: иметь титульный лист, содержание, введение, основную часть, заключение, список литературы.

5.2. Требования к содержанию (основной части)

5.5.1 Во введении обосновывается актуальность темы, определяется цель работы, задачи и методы исследования.

5.5.2 Основная часть работы раскрывает процесс проектирования заданного аппаратного устройства и должна содержать соответствующие таблицы или временные диаграммы, которые должны формироваться разрабатываемым устройством, принципиальную схему устройства и описание его работы.

5.5.3 В процессе изложения материала необходимо давать ссылки на используемую литературу.

4. Заключение должно содержать сделанные автором работы выводы, итоги исследования.

5. Вслед за заключением идет список литературы, который должен быть составлен в соответствии с установленными требованиями.

5.3. Требования к оформлению

Объём лабораторной работы – 5-6 страниц формата А 4, напечатанного с одной стороны текста (1,5 интервал, шрифт Times New Roman).

5.4 Тематика лабораторных работ

Лабораторная работа 1.

Тема: Введение в дисциплину, предмет и задачи программно-аппаратной защиты информации. Идентификация субъекта, понятие протокола идентификации, идентифицирующая информация. Основные подходы к защите данных от НСД. Шифрование, контроль доступа и

разграничение доступа, иерархический доступ к файлу, защита сетевого файлового ресурса, фиксация доступа к файлам.

Цель занятия: выявить основные подходы к защите данных от НСД, принципы шифрования, контроля и разграничения доступа.

Продолжительность занятия – 4 ч.

Задание:

1. Изучить предмет и задачи программно-аппаратной защиты информации.
2. Идентификация субъекта, понятие протокола идентификации, идентифицирующая информация.
3. Основные подходы к защите данных от НСД.
4. Шифрование, контроль доступа и разграничение доступа, иерархический доступ к файлу, защита сетевого файлового ресурса, фиксация доступа к файлам.
5. Оформить отчет по проведенному исследованию.

Лабораторная работа 2.

Тема: Доступ к данным со стороны процесса, способы фиксации факта доступа, надежность систем ограничения доступа. Защита файлов от изменения. Электронная цифровая подпись (ЭЦП). Программно-аппаратные средства шифрования. Построение аппаратных компонент криптозащиты данных.

Цель занятия: выявить основные способы доступа к данным со стороны процесса, способы фиксации факта доступа, надежность систем ограничения доступа.

Продолжительность занятия – 4 ч.

Задание:

1. Доступ к данным со стороны процесса, способы фиксации факта доступа, надежность систем ограничения доступа.
2. Защита файлов от изменения. Электронная цифровая подпись (ЭЦП).
3. Программно-аппаратные средства шифрования.
4. Построение аппаратных компонент криптозащиты данных.
5. Оформить отчет по проведенному исследованию.

Лабораторная работа 3.

Тема: Защита алгоритма шифрования. Принцип чувствительной области и принцип главного ключа, необходимые и достаточные функции аппаратного средства криптозащиты. Пароли и ключи, организация хранения ключей. Методы и средства ограничения доступа к компонентам ЭВМ.

Цель занятия:

Продолжительность занятия – 4 ч.

Задание:

1. Защита алгоритма шифрования. Принцип чувствительной области и принцип главного ключа, необходимые и достаточные функции аппаратного средства криптозащиты.
2. Пароли и ключи, организация хранения ключей. Методы и средства ограничения доступа к компонентам ЭВМ.
3. Оформить отчет по проведенному исследованию.

Лабораторная работа 4.

Тема: Защита программ от несанкционированного копирования. Защита программ от изучения; защита от отладки, защита от дизассемблирования, защита от трассировки по прерываниям. Защита от разрушающих программных воздействий (РПВ). Компьютерные вирусы как особый класс РПВ. Необходимые и достаточные условия недопущения разрушающего воздействия. Понятие изолированной программной среды.

Цель занятия:

Продолжительность занятия – 4 ч.

Задание:

1. Защита программ от несанкционированного копирования. Защита программ от изучения; защита от отладки, защита от дизассемблирования, защита от трассировки по прерываниям.
2. Защита от разрушающих программных воздействий (РПВ). Компьютерные вирусы как особый класс РПВ.
3. Необходимые и достаточные условия недопущения разрушающего воздействия. Понятие изолированной программной среды.
4. Оформить отчет по проведенному исследованию.

6. Перечень основной и дополнительной учебной литературы

Основная:

1. А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков и др.: под редакцией А.П. Зайцева и А.А. Шелупанова. Технические средства и методы защиты информации. Учебное пособие для вузов. – 4-е издание исправленное и дополненное. - М.: Горячая линия – Телеком, 2012. - 616с
2. Рябко Б.Я., Фионов А.Н. Основы современной криптографии и стеганографии – 2-е издание- М.: Горячая линия – Телеком, 2013. – 232с.
3. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах: Учебное пособие для вузов. – 4-е издание, стереотип- М.: Горячая линия – Телеком, 2011. - 146с.
4. А.И. Баранчиков, П.А. Баранчиков, А.Н. Пылькин Алгоритмы и модели ограничения доступа к записям баз данных. - М. Горячая линия – Телеком, 2011 – 182с.
5. А.Ф. Чепига Информационная безопасность автоматизированных систем. М.: «Гелиос АРВ», 2010. -336с.
6. В.Ф. Шаньгин Комплексная защита информации в корпоративных системах. М.: ИД «Форум»: ИНФРА-М., 2010.-592с.
7. О.А.Романов, С.А. Бабин, С.Г. Жданов Организационное обеспечение информационной безопасности М.: Издательский центр «Академия», 2008,-192.
8. Васильков А.В., Васильков А.А., Васильков И.А. Информационные системы и их безопасность М.: ФОРУМ, 2011,-528с.

Дополнительная:

1. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей. Учебное пособие. 2008. Москва, «ИД ФОРУМ – ИНФРА-М».
2. Малюк А.А. Теория защиты информации.-М.:Горячая линия-Телеком,2012.
3. Хорев П.Б. Программно-аппаратная защита информации. М.: ФОРУМ, 2009г.-352с.
4. В.А.Северин. Комплексная защита информации на предприятии. М.: Издательский дом «Городец»,2008.- 368с.
5. Мельников В.П. идр Информационная безопасность.М.: Издателский центр «Академия» , 2008.-336с.
6. Шепитько Г.Е. Теория информационной безопасности и методология защиты информации. – М.: РГСУ, 2012

7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

Интернет-ресурсы:

1. http://eup.ru/catalog/all-all.asp – научно-образовательный портал.
2. http://informika.ru/ – образовательный портал.
3. www.wikIsec.ru - Энциклопедия информационной безопасности. – Публикации, статьи.
4. www.biblioclub.ru - Универсальная библиотека онлайн.
5. www.rucont.ru - ЭБС «Руконт».
6. http://www.academy.it.ru/ – академия АЙТИ.
7. http://www.minfin.ru - Официальный сайт Министерства финансов Российской Федерации
8. http://www.gov.ru/ - Официальный сервер органов государственной власти Российской Федерации**.**
9. http://www.fsb.ru/ - Официальный сайт Федеральной Службы Безопасности

http://www.fstec.ru/ - Официальный сайт Федеральной Службы по Техническому Экспортному контролю

8. Перечень информационных технологий

Перечень программного обеспечения: *MSOffice, Multisim.*

Информационные справочные системы:

1. Ресурсы информационно-образовательной среды МГОТУ
2. Рабочая программа и методическое обеспечение по дисциплине «Программно – аппаратные средства защиты информации».