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

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ»

Направление подготовки: 10.03.01 Информационная безопасность

Профиль: Информационно-аналитические системы финансового мониторинга

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Королев
2020

Автор: к.т.н. Журавлев С.И. Рабочая программа дисциплины: «Информационная безопасность автоматизированных систем». – 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			

2

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

Целью изучения дисциплины является закрепление базовых положений по защите информации в процессе её передачи, обработки и хранения с применением существующих и перспективных информационных систем.

В процессе обучения студент приобретает и совершенствует следующие компетенции.

Общепрофессиональные компетенции:

- ОПК-2: способность применять соответствующий математический аппарат для решения профессиональных задач;
- ОПК-3: способность применять положения электротехники, электроники и схемотехники для решения профессиональных задач;

Профессиональные компетенции:

- ПК-2: - способность применять программные средства системного, прикладного и специального назначения;
- ПК-5: способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации;
- ПК-8: способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов;
- ПК-15: способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.

Основными **задачами** дисциплины являются:

- определение общей методологии защиты информации в информационных системах;
- освоение методических подходов в выборе способов и средств защиты информации;
- установление основных тенденций развития, направлений совершенствования информационных систем (ИС) и технологических операций, используемых при обработке данных;
- приобретение знаний по основам проектирования автоматизированных информационных систем (АИС), базирующимся на применении современных технических и программных средств с учётом требований безопасности;

- оценка степени защищённости информационных систем и алгоритмов их безопасного функционирования;
- приобретение навыков в решении задач сбора, хранения и обработки защищаемой информации, а также овладении приёмами работы с современными пакетами прикладных программ;
- определение основных угроз информационной безопасности информационных систем и факторов, влияющих на требуемый уровень их защищённости;
- определение путей совершенствования информационных систем с учётом требований по защите информации;
- определение методологических подходов к оценке эффективности информационных систем.

После завершения освоения данной дисциплины студент должен:

Знать:

- основные положения теоретических основ в области создания информационных систем;
- состав, структуру и функциональные возможности современных информационных систем;
- источники угроз информационной безопасности;
- методы обработки конфиденциальной информации в информационных системах;
- критерии, условия и принципы обеспечения защиты информации информационных системах;
- технологию обеспечения защиты информации;
- каналы и методы несанкционированного доступа к конфиденциальной информации;

Уметь:

- выявлять угрозы информационной безопасности применительно к системам обработки информации;
- устанавливать применительно к информационным системам каналы и методы несанкционированного доступа к конфиденциальной информации;
- пользоваться методами моделирования системы защиты информации;
- организовывать комплексный подход по защите информации и др.

Владеть навыками:

- определения требований и состава средств, методов и мероприятий по организации защиты информации в информационных системах;
- использования методов контроля функционирования систем обработки и передачи данных с учётом требований информационной безопасности;

• разработки организационно-функциональной структуры и комплекса нормативно-методического обеспечения по защите информации в системах обработки и передачи данных;

• проведения количественной и качественной оценки эффективности функционирования средств защиты информации в информационных системах и др.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Информационная безопасность автоматизированных систем» относится к обязательным дисциплинам вариативной 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: «Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности», «Техническая защита информации», «Основы управления в корпорациях» и компетенциях: ОК-4,5, ОПК-4,5 и ПК-3,5,6,8,9,10,12,15.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Стандарты информационной безопасности в банковской сфере», «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 и виды учебной работы

Общая трудоемкость дисциплины для студентов очной формы составляет 3 зачетные единицы, 108 часов.

Таблица1

Виды занятий	**Всего часов**	**Семестр** 7	**Семестр** 8	**Семестр** 9	**Семестр …**
Общая трудоемкость	108	108			
ОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	48	48			
Лекции (Л)	16	16			
Практические занятия (ПЗ)	16	16			
Лабораторные работы (ЛР)	16	16			
Самостоятельная работа	60	60			
КСР	-	-			

Курсовые работы (проекты)	-	-			
Расчетно-графические работы	-	-			
Контрольная работа, домашнее задание	+	+			
Текущий контроль знаний (7 - 8, 15 - 16 недели)- 2ч.	Т1; Т2	Т1; Т2			
Вид итогового контроля	Зачет	Зачет			

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
Седьмой семестр					
Тема 1: Введение. Информационный ресурс. Информатизация общества. Классификация информационных систем. Операционная схема процедуры восприятия и измерение информации	1	1	-	2	**ОПК-2,3 ПК-2**
Тема 2: Обнаружение и распознавание информации. Принципы построения и основы применения информационных систем	2	2	2	2	**ОПК-2,3 ПК-2**
Тема 3: Автоматизированные информационные технологии и их классификация. Структурная и функциональная организация информационных систем и технологий	2	2	2	1	**ОПК-2,3 ПК-2**
Тема 4: Стадии и этапы создания автоматизированных информационных систем и технологий. Особенности проектирования автоматизированных информационных технологий	2	2	2	1	**ОПК-2,3 ПК-2,-5,-8;**
Тема 5: Структура и содержание информационного обеспечения. Технология применения электронного докумен-	2	2	2	2	**ОПК-2,3 ПК-2,-5,-8;**

тооборота					
Тема 6: Информационные базы и банки данных. Базы знаний. Цели и задачи технологического обеспечения. Режимы обработки информации	2	2	2	2	**ОПК-2,3 ПК-2,-5,-8;**
Тема 7: Экспертные информационные системы. Проблемы безопасности информационных систем	2	2	2	1	**ОПК-2,3 ПК-2,-5,-8;**
Тема 8: Организационно-правовые аспекты обеспечения информационной безопасности информационных систем. Комплексный (системный) подход в обеспечении информационной безопасности информационных систем	2	2	2	1	**ОПК-2,3 ПК-2,-5,-8,-15;**
Тема 9: Методы и средства обеспечения информационной безопасности информационных систем	1	1	2	1	**ОПК-2,3 ПК-2,-5,-8,-15;**
Итого:	16	16	16	12	

4.2. Содержание тем дисциплины

Тема 1. Введение. Информационный ресурс. Информатизация общества. Классификация информационных систем. Операционная схема процедуры восприятия и измерение информации

Предмет и задачи курса. Значение и место курса в подготовке специалистов по защите информации. Научная и учебная взаимосвязь курса с другими дисциплинами.

Разделы и темы, их распределение по видам аудиторных занятий. Формы проведения практических занятий. Состав и методика самостоятельной работы студентов по изучению дисциплины. Формы проверки знаний.

Анализ нормативных источников, научной и учебной литературы.

Знания и умения студентов, которые должны быть получены в результате изучения курса.

Становление и развитие понятия "информационные процессы". Современные подходы к определению понятия «информатизация».

Две стороны задачи восприятия. Цель измерительного преобразования. Угловая и временная формы представления параметров передаваемой информации. Операционная схема процедуры восприятия. Первичное воспри-

тие и измерение информации.

Тема 2. Обнаружение и распознавание информации. Принципы построения и основы применения информационных систем

Задачи обнаружения и распознавания информации. Характеристика пространства признаков и его разбиение. Вероятностный подход при рассмотрении зависимости реализаций от состояний. Характерные случаи расположения условных распределений. Качество распознавания и его параметры.

Структура информационных ресурсов. Основные свойства информационных систем. Структурированность информационных систем. Принципы построения информационных систем. Многоуровневость и распределённость информационных систем. Особенности применения информационных систем в различных областях. Интегрированные информационные системы.

Тема 3. Автоматизированные информационные технологии и их классификация. Структурная и функциональная организация информационных систем и технологий

Определение автоматизированных информационных технологий (АИТ). Основные компоненты АИТ. Виды классификаций АИТ. Основные тенденции развития АИТ в современных условиях. Интегрированные информационные системы обработки данных и способы защиты информации. Многоуровневые и распределённые информационные системы организационного управления.

Система управления и её роль в процессе получения информации и её обработки с помощью заданных алгоритмов. Технологические процессы при обработке данных. Основные задачи автоматизированных информационных систем (АИС). Структура и составные элементы АИС и АИТ. Функции АИТ. Процедуры преобразования информации в АИС. Технология функционирования элементов АИТ.

Тема 4. Стадии и этапы создания автоматизированных информационных систем и технологий. Особенности проектирования автоматизированных информационных технологий

Цель и задачи проектирования АИТ и АИС. Основополагающие принципы создания АИС. Принцип системности – важнейший принцип при создании, функционировании и развитии АИС. Стадии жизненного цикла АИС и АИТ. Модели жизненного цикла АИС и АИТ. Особенности разработки АИС и АИТ.

Особенности создания АИТ. Основные требования к АИТ с учётом информационной безопасности. Аппаратно-программные комплексы, используемые при создании АИТ. Классы пользователей АИТ.

Тема 5. Структура и содержание информационного обеспечения. Технология применения электронного документооборота

Определение информационного обеспечения. Организация информационного обеспечения. Классификаторы, коды и технология их применения. Выбор системы кодирования. Последовательность разработки позиционных и комбинированных систем кодирования.

Последовательность прохождения документов. Автоматизация движения информационных потоков. Система поиска. Механизм установления паролей на вход в информационную систему и выбор способа шифрования данных.

Тема 6. Информационные базы и банки данных. Базы знаний. Цели и задачи технологического обеспечения. Режимы обработки информации

Технология информационных баз и банков данных. Требования, предъявляемые к информационным базам данных. Распределённая система информационных баз и банков данных. Этапы создания информационных баз и банков данных. Система управления базами данных (СУБД). Управленческие стандарты информационной безопасности.

Техническое обеспечение. Средства обработки информации. Распределённая система обработки информации. Условия разработки и выбора программного обеспечения. Классификация программного обеспечения. Диалоговый режим обработки информации. Сетевой режим обработки информации.

Тема 7. Экспертные информационные системы. Проблемы безопасности информационных систем

Определение экспертной системы. Технология применения экспертных систем. Разработка экспертных систем. Преимущества использования экспертных систем. Отличительные особенности экспертных систем. Области применения экспертных систем. Уязвимость экспертных систем.

Причины, способствующие уязвимости информационных систем. Источники, виды и анализ угроз. Мероприятия по предотвращению угроз безопасности информационных систем. Проблемы обеспечения безопасности информационных систем. Основные подходы в создании защищённых информационных систем.

Тема 8. Организационно-правовые аспекты обеспечения информационной безопасности информационных систем. Комплексный (системный) подход в обеспечении информационной безопасности информационных систем

Глобальные информационные сети и системы, их свойства. Правовые аспекты информационного обмена в глобальных сетях. Особенности отношений субъектов информационного обмена в сетях. Обеспечение совместимости в информационных сетях и системах. Протоколы совместимости. Роль стандартов информационной безопасности при создании информационных систем.

Основные стадии жизненного цикла системы защиты информации. Общая методология в выборе средств и способов защиты информации в информационных системах. Модель построения системы защиты информации. Комплексный (системный) подход в обеспечении информационной безопасности информационных систем.

Тема 9. Методы и средства обеспечения информационной безопасности информационных систем

Методы и средства защиты информации в информационных системах. Два подхода к проблеме обеспечения информационной безопасности информационных систем. Пути решения проблем защиты информации в информационных системах. Задачи управления средствами информационной безопасности. Политики безопасности. Протоколы безопасной передачи данных.

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

«Методические указания для самостоятельной работы обучающихся по освоению дисциплины» представлены 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 «Информационная безопасность автоматизированных систем» приведена в Приложении 1.

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

Основная литература:

1. Цирлов В.Л. Основы информационной безопасности: краткий курс, Ростов-на-Дону, «Феникс», 2008.
2. Торокин А.А. Инженерно-техническая защита информации. Учебное пособие, М.: «Гелиос АРВ». 2005.
3. Титоренко Г.А. Автоматизированные информационные технологии в экономике, учебник, М.: «ЮНИТИ», 1998.
4. Темников Ф.Е. и другие Теоретические основы информационной техники, учебник, М.: «Энергия», 1971.

Дополнительная литература:

1. Литвинская О.С. Основы теории передачи информации. Учебное пособие, М.: «КНОРУС», 2010.
2. Завгородний В.И. Комплексная защита информации в компьютерных сис-темах. Учебное пособие, М.: Логос; ПБОЮЛ Н.А.Егоров, 2001.

3. Романец Ю.В. и др. Защита информации в компьютерных системах и сетях. - 2-е изд., М.: Радио и связь, 2001.

4. Сидак А.А. Формирование требований безопасности современных сетевых информационных технологий, М.: МГУЛ, 2001.

Рекомендуемая литература:

1. Васильков А.В. Информационные системы и их безопасность. Учебное пособие, М.: «Форум», 2010.

2. Цирлов В.Л. Основы информационной безопасности: краткий курс, Ростов-на-Дону, «Феникс», 2008.

3. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей, М.: «Форум»-Инфра-М. 2008.

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

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

9. Методические указания для обучающихся, по освоению дисциплины

Методические указания для обучающихся, по освоению дисциплины (модуля) приведены в Приложении 2 к настоящей рабочей программе.

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

- **Перечень программного обеспечения:** MSOffice, PowerPoint.

- **Информационные справочные системы:**

1. Ресурсы информационно-образовательной среды «МГОТУ».
2. Рабочая программа и методическое обеспечение по дисциплине: «Информационная безопасность автоматизированных систем»

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

Лекционные занятия:

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

Практические занятия:

- компьютерный класс с проектором для интерактивного обучения и проведения лекций в форме слайд-презентаций, оборудованный современными лицензионными программно-техническими средствами: операционная система не ниже WindowsXP; офисные программы MSOffice 7;
- 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

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ»
(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 компетенции	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	Темы 1,2,3, 4, 5,6, 7, 8, 9	критерии, условия и принципы обеспечения защиты информации информационных системах;	устанавливать применительно к информационным системам каналы и методы несанкционированного доступа к конфиденциальной информации;	определения требований и состава средств, методов и мероприятий по организации защиты информации в информационных системах;
2.	ОПК-3	способность применять положения электротехники, электроники и схемотехники для решения профессиональных задач	Темы 1,2,3, 4, 5,6, 7, 8, 9	критерии, условия и принципы обеспечения защиты информации информационных системах;	устанавливать применительно к информационным системам каналы и методы несанкционированного доступа к конфиденциальной информации;	определения требований и состава средств, методов и мероприятий по организации защиты информации в информационных системах;
3.	ПК-2	способность применять программные средства системного, прикладного и специального назначения	Темы 1,2,3, 4, 5,6, 7, 8, 9	критерии, условия и принципы обеспечения защиты информации информационных системах;	устанавливать применительно к информационным системам каналы и методы несанкционированного доступа к конфиденциальной информации;	определения требований и состава средств, методов и мероприятий по организации защиты информации в информационных системах;
4.	ПК-5	способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	Темы 4, 5,6, 7, 8, 9	каналы и методы несанкционированного доступа к конфиденциальной информации.	выявлять угрозы информационной безопасности применительно к системам обработки информации.	разработки организационно-функциональной структуры и комплекса нормативно-методического обеспечения по защите информации в системах обработки и передачи данных.

5.	ПК-8	способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	Темы 4, 5,6, 7, 8, 9	каналы и методы несанкционированного доступа к конфиденциальной информации.	выявлять угрозы информационной безопасности применительно к системам обработки информации.	разработки организационно-функциональной структуры и комплекса нормативно-методического обеспечения по защите информации в системах обработки и передачи данных.
6.	ПК-15	способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	Темы 8, 9	каналы и методы несанкционированного доступа к конфиденциальной информации.	выявлять угрозы информационной безопасности применительно к системам обработки информации.	разработки организационно-функциональной структуры и комплекса нормативно-методического обеспечения по защите информации в системах обработки и передачи данных.

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	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.
ОПК-3	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-2	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-5	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-8	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-15	Контрольная работа	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 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 презентационной форме:

1. Виды атак на сетевые информационные системы и методы борьбы с ними.
2. Скорость передачи информации дискретных каналов с помехами.
3. Современные системы электронного документооборота и показатели их защищённости.
4. Информационная безопасность электронного бизнеса.
5. Оптимальные алгоритмы обработки конфиденциальной информации в сетевых информационных системах.
6. Методы оценки эффективности функционирования современных информационных систем.
7. Перспективные информационные системы, технологии управления и обеспечение их безопасности.
8. Методы разграничения доступа в информационных системах.
9. Интегрированные и корпоративные информационные системы, проблемы их защищённости.
10. Статистические критерии обнаружения и распознавания информации.

Примерная тематика заданий на контрольную работу:

1. Задача стандартизации при разработке систем защиты информации.
2. Правовая основа защиты информации на объектах информатизации.
3. Криптографические методы защиты информации в современных информационных системах.
4. Компьютерные вирусы и проблемы антивирусной защиты.
5. Организация защиты при обмене данными в информационных системах.
6. Протоколы, применяемые для защиты информации в сетевых информационных системах.
7. Проблемы обеспечения информационной безопасности беспроводных информационных систем.
8. Общая методология выбора средств и способов защиты информации в информационных системах.
9. Организация парольной защиты в информационных системах.

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

Формой контроля знаний по дисциплине «Информационная безопасность автоматизированных систем» являются две текущие аттестации в виде тестов и итоговая аттестация в виде зачета.

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 ОПК-3 ПК-2 ПК-5 ПК-8 ПК-15	20-40 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 ОПК-3 ПК-2 ПК-5 ПК-8 ПК-15	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	Зачет	ОПК-2 ОПК-3 ПК-2 ПК-5 ПК-8 ПК-15	2 теоретических вопроса + практическое задание	Зачет проводится в письменной форме, путем ответа на вопросы. Время, отведенное на процедуру – 25 минут.	Результаты предоставляются в день проведения зачета	Критерии оценки: **«Зачтено»:** • знание основных понятий предмета; • умение использовать и применять полученные знания на практике; • работа на семинарских занятиях; • знание основных научных теорий, изучае-

						мых предметов; • ответ на вопросы билета. **«Не зачтено»**: • демонстрирует частичные знания по темам дисциплин; • незнание основных понятий предмета; • неумение использовать и применять полученные знания на практике; • не работал на семинарских занятиях; не отвечает на вопросы.

4.1. Типовые вопросы, выносимые на тестирование

Тесты используются в режиме промежуточного контроля. По форме заданий выбраны открытые тесты.

1. Перечислите возможные каналы утечки информации в офисном помещении?

2. Изобразите модель системы защиты информации?

3. Поясните организацию обмена данными в информационных системах?

4. Дайте определение системы защиты информации от несанкционированного доступа?

5. Что подразумевается под безопасностью информационной системы (ИС)?

6. Изобразить структуру информационных ресурсов?

7. Перечислить основные виды угроз безопасности?

8. Перечислить наиболее распространенные пути НСД к информации?

9. Назвать задачи, решаемые при проектировании автоматизированных информационных технологий?

10. Перечислить организационные меры по защите информации?

11. Дайте определение идентификации и аутентификации?

12. Назвать особенности парольных систем аутентификации и угрозы их безопасности?

13. Перечислить рекомендации по практической реализации парольных систем?

14. Какие методы хранения паролей существуют?

15. Назвать методы разграничения доступа и их отличительные особенности?

16. Пояснить схему симметричного криптошифрования?

17. Пояснить схему асимметричного криптошифрования?

18. Пояснить назначение механизма регистрации и аудита?

19. Куда и как помещаются протоколируемые данные?

20. Изобразить схему отношения субъектов информационного обмена в сети Internet?

21. В чем сущность главной задачи, решаемой при создании сетевых ИС?

22. Что представляет собой модель OSI?

23. Что такое стек коммуникационных протоколов и межуровневый интерфейс?

24. Что используют в компьютерных сетях для подслушивания?

25. В чем сущность подмены доверенного субъекта?

26. С какой целью осуществляется посредничество в обмене информационными ключами?

27. Чем характеризуется отказ в обслуживании?

28. Дайте характеристику парольным атакам?

29. Что представляет собой сетевая разведка?

30. Какие подходы к проблеме обеспечения безопасности ИС и сетей существуют?

31. Перечислить группы административно-организационных мер?

32. Какие механизмы безопасности используют современные ИС?

33. Назовите области ИБ, на которые должны опираться создатели электронного бизнеса?

34. Перечислите основные методы и средства защиты информации в рамках общей системы ИБ?

35. По каким признакам классифицируются компьютерные вирусы?

36. Дайте характеристику сетевым компьютерным вирусам?

37. Что такое «Троянские программы» и «Логические бомбы»?

38. Перечислить основные каналы распространения компьютерных вирусов?

39. Назовите основные методы защиты от компьютерных вирусов?

40. В чем сущность концепции глобального управления безопасностью?

41. Назвать структурные элементы системы управления средствами безопасности?

42. Дайте краткую характеристику отечественным стандартам ИБ?

43. Какие стандарты ИБ для беспроводных сетей существуют?

44. Дайте общую характеристику стандарту ISO/IEC 15408-1999?

45. Дайте общую характеристику стандарту ISO/IEC 15408-1999?

46. Перечислите международные стандарты ИБ?

4.2. Типовые вопросы, выносимые на зачет

1. Понятие "информационный процесс". Восприятие информации.
2. Операционная схема процедуры восприятия информации.
3. Две стороны задачи восприятия. Цель измерительного преобразования.
4. Угловая и временная формы представления параметров передаваемой информации.

5. Первичное восприятие и измерение информации.
6. Задачи обнаружения и распознавания информации.
7. Характеристика пространства признаков и его разбиение.
8. Качество распознавания и его параметры.
9. Свойства информационных систем. Структурированность информационных систем.
10. Принципы построения защищённых информационных систем.
11. Интегрированные информационные системы и их защищённость.
12. Основные тенденции развития АИТ в современных условиях.
13. Интегрированные информационные системы обработки данных и способы защиты информации.
14. Многоуровневые и распределённые информационные системы организационного управления.
15. Структура и составные элементы АИС и АИТ. Функции АИТ.
16. Процедуры преобразования информации в АИС. Технология функционирования элементов АИТ.
17. Определение информационного обеспечения. Организация информационного обеспечения.
18. Выбор системы кодирования. Последовательность разработки позиционных и комбинированных систем кодирования.
19. Автоматизация движения информационных потоков. Система поиска.
20. Механизм установления паролей на вход в информационную систему и выбор способа шифрования данных.
21. Требования, предъявляемые к информационным базам данных.
22. Распределённая система информационных баз и банков данных.
23. Система управления базами данных (СУБД). Управленческие стандарты информационной безопасности.
24. Техническое обеспечение. Средства обработки информации.
25. Распределённая система обработки информации.
26. Диалоговый режим обработки информации.
27. Сетевой режим обработки информации.
28. Причины, способствующие уязвимости информационных систем. Источники, виды и анализ угроз.
29. Мероприятия по предотвращению угроз безопасности информационных систем.
30. Проблемы обеспечения безопасности информационных систем. Основные подходы в создании защищённых информационных систем.
31. Глобальные информационные сети и системы, их свойства.

32. Правовые аспекты информационного обмена в глобальных сетях.

33. Обеспечение совместимости в информационных сетях и системах. Протоколы совместимости.

34. Роль стандартов информационной безопасности при создании информационных систем.

35. Основные стадии жизненного цикла системы защиты информации.

36. Общая методология в выборе средств и способов защиты информации в информационных системах.

37. Модель построения системы защиты информации.

38. Комплексный (системный) подход в обеспечении информационной безопасности информационных систем.

39. Методы и средства защиты информации в информационных системах.

40. Два подхода к проблеме обеспечения информационной безопасности информационных систем.

41. Пути решения проблем защиты информации в информационных системах.

42. Задачи управления средствами информационной безопасности. Политики безопасности.

43. Протоколы безопасной передачи данных.

44. Свойства и параметры сложных информационных систем.

45. Механизм установления паролей на вход в информационную систему и выбор способа шифрования данных.

Приложение 2

ИНСТИТУТ ТЕХНИКИ И ЦИФРОВЫХ ТЕХНОЛОГИЙ

ФАКУЛЬТЕТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ»

(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

Целью изучения дисциплины является:

1. Формирование у студентов специализированной базы знаний по фундаментальным проблемам информационной безопасности в условиях становления современного информационного общества.
2. закрепление базовых положений по защите информации в процессе её передачи, обработки и хранения с применением существующих и перспективных информационных систем.
3. Получение первичных навыков в применении защищённых технологий при обеспечении информационной безопасности различных объектов.

Задачи дисциплины:

- ознакомление студентов с информационными процессами на предприятии с точки зрения информационной безопасности;
- формирование у студентов способности самостоятельно проводить классификацию автоматизированных систем и средств защиты информации по требованиям безопасности;
- формирование студентами предложений по совершенствованию, модернизации, унификации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами.

2. Указания по проведению практических занятий

Тема 1: Введение. Информационный ресурс. Информатизация общества. Классификация информационных систем. Операционная схема процедуры восприятия и измерение информации

Практическое занятие 1.

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Ознакомиться с основными понятиями.

Основные положения темы занятия:

1. Становление и развитие понятия "информационные процессы".
2. Современные подходы к определению понятия «информатизация».

Вопросы для обсуждения:

Основной доклад (реферат) по теме занятия.

1. Две стороны задачи восприятия.
2. Цель измерительного преобразования.
3. Угловая и временная формы представления параметров передаваемой информации.
4. Операционная схема процедуры восприятия.
5. Первичное восприятие и измерение информации.

Продолжительность занятия – 1 ч.

Тема 2: Обнаружение и распознавание информации. Принципы построения и основы применения информационных систем

Практическое занятие 2.

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Ознакомиться с принципами построения информационных систем

Основные положения темы занятия:

1. Основные свойства информационных систем.
2. Принципы построения информационных систем.

Вопросы для обсуждения:

Основной доклад (реферат) по теме занятия.

1. Задачи обнаружения и распознавания информации
2. Многоуровневость и распределённость информационных систем.
3. Особенности применения информационных систем в различных областях.

Продолжительность занятия – 2 ч.

Тема 3: Автоматизированные информационные технологии и их классификация. Структурная и функциональная организация информационных систем и технологий

Практическое занятие 3.

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Ознакомиться с организацией информационных систем и технологий.

Основные положения темы занятия:

1. Многоуровневые и распределённые информационные системы организационного управления.
2. Система управления и её роль в процессе получения информации и её обработки с помощью заданных алгоритмов

Вопросы для обсуждения:

Основной доклад (реферат) по теме занятия.

1. Основные компоненты АИТ. Виды классификаций АИТ.
2. Основные задачи автоматизированных информационных систем (АИС).

Продолжительность занятия – 2 ч.

Тема 4: Стадии и этапы создания автоматизированных информационных систем и технологий. Особенности проектирования автоматизированных информационных технологий

Практическое занятие 4.

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить базовые знания о проектировании и построении автоматизированных информационных систем.

Основные положения темы занятия:

1. Цель и задачи проектирования АИТ и АИС
2. Особенности создания АИТ

Вопросы для обсуждения:

Основной доклад (реферат) по теме занятия.

1. Стадии жизненного цикла АИС и АИТ.
2. Особенности разработки АИС и АИТ.
3. Классы пользователей АИТ.

Продолжительность занятия – 2 ч.

Тема 5: Структура и содержание информационного обеспечения. Технология применения электронного документооборота

Практическое занятие 5.

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить представление об информационном обеспечении и электронном документообороте.

Основные положения темы занятия:

1. Ознакомиться с организацией информационного обеспечения
2. Ознакомиться с автоматизацией движения информационных потоков

Вопросы для обсуждения:

Основной доклад (реферат) по теме занятия.

1. Последовательность разработки позиционных и комбинированных систем кодирования.
2. Механизм установления паролей на вход в информационную систему и выбор способа шифрования данных.

Продолжительность занятия – 2 ч.

Тема 6: Информационные базы и банки данных. Базы знаний. Цели и задачи технологического обеспечения. Режимы обработки информации

Практическое занятие 6.

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические навыки в предоставлении технологического обеспечения.

Основные положения темы занятия:

1. Технология информационных баз и банков данных.
2. Средства обработки информации.

Вопросы для обсуждения:

Основной доклад (реферат) по теме занятия.

1. Требования, предъявляемые к информационным базам данных.
2. Система управления базами данных (СУБД).
3. Условия разработки и выбора программного обеспечения.

Продолжительность занятия – 2 ч.

Тема 7: Экспертные информационные системы. Проблемы безопасности информационных систем

Практическое занятие 7.

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Ознакомиться с проблемами информационных систем.

Основные положения темы занятия:

1. Разработка экспертных систем и Технология их применения.
2. Мероприятия по предотвращению угроз безопасности информационных систем *Вопросы для обсуждения:*

Основной доклад (реферат) по теме занятия.

1. Области применения экспертных систем.
2. Уязвимость экспертных систем.
3. Проблемы обеспечения безопасности информационных систем.
4. Основные подходы в создании защищённых информационных систем.

Продолжительность занятия – 2 ч.

Тема 8: Организационно-правовые аспекты обеспечения информационной безопасности информационных систем. Комплексный (системный) подход в обеспечении информационной безопасности информационных систем

Практическое занятие 8.

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические навыки в обеспечении информационной безопасности информационных систем.

Основные положения темы занятия:

1. Правовые аспекты информационного обмена в глобальных сетях.
2. Основные стадии жизненного цикла системы защиты информации.

Вопросы для обсуждения:

Основной доклад (реферат) по теме занятия.

1. Глобальные информационные сети и системы, их свойства
2. Роль стандартов информационной безопасности при создании информационных систем.
3. Комплексный (системный) подход в обеспечении информационной безопасности информационных систем.

Продолжительность занятия – 2 ч.

Тема 9: Методы и средства обеспечения информационной безопасности информационных систем

Практическое занятие 9.

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Ознакомиться с методами и средствами обеспечения информационной безопасности информационных систем.

Основные положения темы занятия:

1. Методы и средства защиты информации в информационных системах
2. Пути решения проблем защиты информации в информационных системах.

Вопросы для обсуждения:

Основной доклад (реферат) по теме занятия.

1. Два подхода к проблеме обеспечения информационной безопасности информационных систем
2. Задачи управления средствами информационной безопасности.
3. Политики безопасности.
4. Протоколы безопасной передачи данных.

Продолжительность занятия – 1 ч.

3. Указания по проведению лабораторных работ

Цель проведения лабораторных работ – ознакомление студентов с комплексом показателей для оценки защищённости информационных объектов, систем и ознакомление с программной средой, используемой для моделирования процессов оптимизации применения систем физической защиты.

Задачи выполнения лабораторных работ:

- определение положения механизмов защиты, включение которых в иерархию системы физической защиты информационных объектов повышает уровень их защищённости;
- мониторинг защищённости охраняемых информационных объектов, базирующийся на решении оптимизационных задач на основе рейтинговых показателей, учитывающий разноплановые экспертные оценки, включая экономические;
- анализ существующих систем физической защиты предприятий на предмет определения эффективности их применения исходя из предполагаемых затрат на создание таких систем, их эксплуатацию и реализацию для предотвращения ущерба от выявленных и потенциальных угроз;
- формирование потенциальной структуры защищённых информационных систем и технологий, путём задания иерархии эшелонов и перечня механизмов защиты для нейтрализации требуемого поля угроз и предотвращённого ущерба;

- формирование динамической модели физической защиты информационных систем для анализа последствий реализации угроз, приводящих к ущербу, близкому или превышающему допустимое для данного хозяйствующего субъекта значение.

Методика проведения лабораторных работ определяется моделью решаемых задач по обеспечению физической защиты информационных объектов, исследуемых студентами на занятии по заданию преподавателя.

Средства выполнения лабораторных работ:

- программный комплекс «Эксперт - 2.0»;
- программный комплекс «EASI»;
- инструменты интегрального метода оценки рисков при распределении ограниченных ресурсов;
- программный комплекс «Adobe Photoshop».

Этапы выполнения лабораторных работ:

1. Постановка задачи лабораторной работы.
2. Ознакомление обучаемых с содержанием и объёмом лабораторной работы.
3. Порядок выполнения лабораторной работы.
4. Регистрация результатов и оформление отчёта о лабораторной работе.
5. Заключительная часть лабораторной работы.

Тематика лабораторных работ и задания к ним

Лабораторная работа 1.

Тема: **Выявление и анализ угроз охраняемым объектам с помощью программного комплекса «Эксперт - 2.0».**

Цель занятия: Ознакомление с программным комплексом оценки защищённости информационных систем «Эксперт - 2.0» и получение практических навыков в моделировании и оптимизации определения угроз безопасности информационным объектам, применения механизмов защиты в ходе осуществления мониторинга деятельности предприятий.

Учебные вопросы.

1. Формирование матрицы экспертных оценок с полями «механизмы защиты-угрозы» и «угрозы-эшелоны» для оценки достоверности активируемых механизмов защиты.
2. Формирование рейтинговых показателей в разрезе использования конкретных механизмов защиты и эшелонов для системы физической защиты в целом, а также показателей активности отдельных эшелонов и механизмов защиты.
3. Анализ активности системы физической защиты в разрезе использования конкретных механизмов и эшелонов защиты, формулирование предложений по улучшению рейтинга исследуемой системы.

Продолжительность занятия – 4 часа.

Задание на лабораторную работу №1:

1. Ознакомиться с системой показателей для оценки информационной защищённости исследуемых объектов.
2. Запустить программу «Эксперт - 2.0» и в интерактивном режиме сформировать перечень известных угроз, механизмов защиты и расставить их в иерархии эшелонов защиты для исследуемых объектов.
3. Сформировать матрицы экспертных оценок «Механизмы защиты – Угрозы» и «Угрозы – Эшелоны защиты» для повышения достоверности исходных данных и активации механизмов защиты.
4. Провести расчёт матрицы, определяющей распределение относительного потенциального ущерба по механизмам защиты и эшелонам безопасности на заданном множестве известных угроз.
5. Проанализировать активность системы информационной безопасности в разрезе использования конкретных механизмов защиты и эшелонов безопасности исследуемого предприятия.
6. Действия пунктов 3-5 повторить для различных частот активизации угроз безопасности.
7. Сформировать рейтинговые показатели при использовании конкретных механизмов защиты и эшелонов информационной безопасности для указанных информационных объектов, а также показатели активности отдельных эшелонов и механизмов защиты.
8. Создать отчёт по лабораторной работе и сформулировать выводы.

Лабораторная работа 2.

Тема: **Исследование системы физической защиты с помощью программного комплекса «Эксперт – 2.0».**

Цель занятия: Ознакомление с программным комплексом оценки защищённости информационных систем «Эксперт - 2.0» и получение практических навыков в моделировании и оптимизации применения механизмов защиты для деятельности отдельных предприятий с учётом рисков и неопределённости внешней среды.

Учебные вопросы.

1. Корректировка матрицы экспертных оценок для достоверности активации механизмов защиты с расчётом матрицы, определяющей распределение достоверности активации по механизмам защиты и эшелонам безопасности для системы физической защиты на заданном множестве известных угроз.
2. Формирование рейтинговых показателей в разрезе использования конкретных механизмов защиты и эшелонов безопасности для системы физической защиты в целом, а также показателей активности отдельных эшелонов и механизмов защиты.

3. Анализ информационной защищенности исследуемых объектов с определением конкретных механизмов защиты, обеспечивающих наибольшую динамику рейтинговых показателей.

Продолжительность занятия – 4 часа.

Задание на лабораторную работу №2:

1. Ознакомиться с системой показателей для оценки защищённости исследуемых объектов в деятельности отдельных предприятий с учётом рисков и неопределённости внешней среды.

2. Запустить программу «Эксперт - 2.0» в интерактивном режиме, получить от преподавателя вариант многоуровневой системы защиты исследуемого объекта предприятия с индивидуальным распределением конкретных механизмов защиты по эшелонам безопасности.

3. Провести расчёт матрицы, определяющей распределение относительного ущерба по механизмам защиты и уровням адаптивной системы защищённости исследуемых объектов предприятия на заданном множестве известных угроз.

4. Проанализировать активность адаптивной защиты в разрезе использования конкретных механизмов защиты и эшелонов безопасности исследуемых объектов предприятия.

5. Сформировать рейтинговые показатели в разрезе использования конкретных механизмов защиты и эшелонов безопасности исследуемых объектов предприятия.

6. Проанализировать существующую защищённость и сформулировать предложения по улучшению рейтинга системы физической защиты исследуемых объектов предприятия в рамках реализации адаптивной системы защиты.

7. Создать отчёт по лабораторной работе и сформулировать выводы.

Лабораторная работа 3.

Тема: **Исследование эффективности системы физической защиты предприятия по предполагаемым действиям нарушителя при определённых угрозах и состоянии элементов защиты с помощью программного комплекса оценки враждебных проникновений и действий “EASI”.**

Цель занятия: Ознакомление студентов с комплексом показателей для оценки защищённости объектов предприятий и программным комплексом оценки враждебных проникновений и действий “Estimate of Adversary Sequence Interruption” (EASI), а так же получение практических навыков в моделировании применения механизмов физической защиты и оценки их эффективности на заданном пути нарушителя при определённых угрозах и состоянии самой системы защиты предприятия.

Учебные вопросы.

1. Анализ пути нарушителя при продвижении к охраняемому объекту.

2. Определение критической точки обнаружения и её влияние на параметры оценки прерывания последовательности действий нарушителя.
3. Построение и исследование диаграммы последовательности действий нарушителя для конкретной зоны охраняемого объекта.

Продолжительность занятия – 4 часа.

Задание на лабораторную работу №3:

1. Ознакомиться с краткими теоретическими сведениями по оценке физической защищённости охраняемых объектов и основными способами действий злоумышленников.

2. Ознакомиться с методикой применения модели “EASI” по оценке враждебных проникновений и действий нарушителя на охраняемых объектах.

3. Запустить модель “EASI” на персональном компьютере и смоделировать в интерактивном режиме возможные действия нарушителя на предложенном охраняемом объекте с выбором определённых процедур и механизмов защиты.

4. Рассчитать основные показатели эффективности по введённым данным для выбранного пути проникновения нарушителя и сформированной системы защиты охраняемого объекта, оценить её значение.

5. Проанализировать эффективность исходной системы физической защиты охраняемого объекта, выявить её недостатки и сформировать дополнительные мероприятия и средства защиты на пути проникновения нарушителя для повышения основных критериев безопасности все данные занести в рабочую таблицу модели.

6. Оценить эффективность усовершенствованной системы защиты на основе добавленных элементов на охраняемом объекте, обосновать Ваши решения расчётами с занесением данных в рабочую таблицу модели и сформировать итоговые показатели эффективности системы физической защиты.

7. Создать отчёт по лабораторной работе и сформулировать выводы.

Лабораторная работа 4.

Тема: **Исследование системы физической защиты и охраняемых объектов с помощью интегрального метода оценки рисков при распределении ограниченных ресурсов, имеющихся в распоряжении службы безопасности.**

Цель занятия: Изучение принципов компьютерного моделирования эффективности системы физической защиты на основе общего уравнения для расчёта рисков охраняемого объекта и получение практических навыков в работе со специализированными программными средствами защиты.

Учебные вопросы.

1. Использование общего уравнения для расчёта рисков охраняемого объекта как важного инструмента количественной оценки системы физической защиты.
2. Анализ и оценка рисков для выбора оптимального варианта защиты, допустимого для охраняемого объекта по критерию затраты-прибыль в исследуемой системе физической защиты.

Продолжительность занятия – 4 часа.

Задание на лабораторную работу №4:

1. Ознакомиться с инструментом количественной оценки системы физической защиты на основе общего уравнения для расчёта рисков охраняемого объекта.

2. Сформировать рейтинговые показатели риска в разрезе использования выбранных механизмов защиты для охраняемых объектов и для системы в целом, а также показатели активности отдельных элементов защиты.

3. Воспользовавшись инструментом количественной оценки системы физиической защиты на основе общего уравнения расчёта рисков проанализировать исходную защищенность исследуемого объекта, выделить конкретные механизмы защиты, обеспечивающие наибольшую динамику рейтинговых показателей риска.

4. Сохранить в файле текущее состояние адаптивной системы физической защиты и показатели риска для дальнейших исследований.

5. Сравнить разнородную структуру системы физической защиты и рейтинговые показатели риска для заданных вариантов адаптивной защиты охраняемых объектов.

6. Результаты работы и итогового анализа сравнения поместить в Вашу папку на ПК.

7. Создать отчёт по лабораторной работе и сформулировать выводы.

4. Указания по проведению самостоятельной работы студентов

Цель самостоятельной работы: подготовить студентов к самостоятельному научному творчеству.

Задачи самостоятельной работы:

1) расширить представление в области защиты информационных процессов;

2) привить навыки самостоятельного решения задач в области создания безопасной среды функционирования предприятия.

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	10
Подготовка к практическим занятиям	16
Подготовка к лабораторным занятиям	16
Подготовка докладов	10
Выполнение практических заданий	8

Вопросы, выносимые на самостоятельное изучение:

1. Задача стандартизации при разработке систем защиты информации.

2. Правовая основа защиты информации на объектах информатизации.

3. Криптографические методы защиты информации в современных информационных системах.

4. Компьютерные вирусы и проблемы антивирусной защиты.

5. Организация защиты при обмене данными в информационных системах.

6. Протоколы, применяемые для защиты информации в сетевых информационных системах.

7. Проблемы обеспечения информационной безопасности беспроводных информационных систем.

8. Общая методология выбора средств и способов защиты информации в информационных системах.

9. Организация парольной защиты в информационных системах.

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	10	Изучение открытых источников

2.	Подготовка к практическим занятиям	16	Изучение открытых источников при подготовке доклада на выбранную тему.
3.	Подготовка к лабораторным занятиям	16	Изучение открытых источников
4.	Тематика докладов	10	см. примерные темы докладов
5.	Выполнение практических заданий	8	

Примерные темы докладов

1. Виды атак на сетевые информационные системы и методы борьбы с ними.
2. Скорость передачи информации дискретных каналов с помехами.
3. Современные системы электронного документооборота и показатели их защищённости.
4. Информационная безопасность электронного бизнеса.
5. Оптимальные алгоритмы обработки конфиденциальной информации в сетевых информационных системах.
6. Методы оценки эффективности функционирования современных информационных систем.
7. Перспективные информационные системы, технологии управления и обеспечение их безопасности.
8. Методы разграничения доступа в информационных системах.
9. Интегрированные и корпоративные информационные системы, проблемы их защищённости.
10. Статистические критерии обнаружения и распознавания информации.

6. Перечень основной и дополнительной учебной литературы

Основная литература:

1. Васильков А.В. Информационные системы и их безопасность. Учебное пособие, М.: «Форум», 2010.
2. Цирлов В.Л. Основы информационной безопасности: краткий курс, Ростов-на-Дону, «Феникс», 2008.
3. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей, М.: «Форум»-Инфра-М. 2008.

Дополнительная литература:

1. Литвинская О.С. Основы теории передачи информации. Учебное пособие, М.: «КНОРУС», 2010.

2. Завгородний В.И. Комплексная защита информации в компьютерных сис-темах. Учебное пособие, М.: Логос; ПБОЮЛ Н.А.Егоров, 2001.
3. Романец Ю.В. и др. Защита информации в ком¬пьютерных системах и сетях. - 2-е изд., М.: Радио и связь, 2001.
4. Сидак А.А. Формирование требований безопасности современных сетевых информационных технологий, М.: МГУЛ, 2001.

Рекомендуемая литература:

1. Васильков А.В. Информационные системы и их безопасность. Учебное пособие, М.: «Форум», 2010.
2. Цирлов В.Л. Основы информационной безопасности: краткий курс, Ростов-на-Дону, «Феникс», 2008.
3. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей, М.: «Форум»-Инфра-М. 2008.

Электронные книги:

1. Иванов М.А., Чугунов И.В. криптографические методы защиты информации в компьютерных системах и сетях: Учебное пособие/ под редакцией М.А. Иванова .М.: НИЯУ МИФИ,2012.
http://biblioclub.ru/index.php?page=book_view&book_id=231673
2. В.А. Галатенко Стандарты информационной безопасности: Учебное пособие .М.: ИНТУИТ,2006
http://www.intuit.ru/goods_store/ebooks/8172
3. Д.С. Кулябов Защита информации в сетях. Уч. пос.ч1.2004.
http://telesys.pfu.edu.ru/sites/telesys.pfu.edu.ru/files/imported/studies/book/net-sec-p1.pdf
4. Международные стандарты по оценке безопасности информационных технологий. Гармонизированные критерии Европейских стран ITSEC.
http://dehack.ru/mezhdunarodnye_standarty_po_otsenke_bezopasnosti_informatsio/
5. Андрианов В.В. Обеспечение информационной безопасности бизнеса. 2-е издание, переработанное и дополненное. 2011
http://fanread.ru/book/8496757/?page=1
6. Блинов А.М. Информационная безопасность: Учебное пособие. Часть1.-СПб.:Изд-во СПГУЭФ,2010.
http://elibrary.unecon.ru/materials_files/341423666.pdf
7. Скотт Бармен. Разработка правил информационной безопасности. Учебное пособие: Изд-во: Вильямс. 2002
http://bookimir.ru/loads/kompyuteryiinternet/aznoe37/501266-razrabotka-pravil-informacionnoy-bezopasnosti-skott-barmen.html

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

8. Перечень информационных технологий

Перечень программного обеспечения: MSOffice, PowerPoint.

Информационные справочные системы:

1. Ресурсы информационно-образовательной среды «МГОТУ».
2. Рабочая программа и методическое обеспечение по дисциплине: «Информационная безопасность автоматизированных систем».