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

«КОМПЛЕКСНОЕ ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ ОБЪЕКТА ИНФОРМАТИЗАЦИИ (ПРЕДПРИЯТИЯ)»

Направление подготовки: 10.03.01 Информационная безопасность
Профиль: Информационно-аналитические системы финансового мониторинга
Квалификация (степень) выпускника: бакалавр
Форма обучения: очная

Королев
2020

Автор: к.в.н., доцент Соляной В.Н. Рабочая программа дисциплины: «Комплексное обеспечение защиты информации объекта информатизации (предприятия)». – Королев МО: «Технологический университет», 2020.

Рецензент: **к.в.н., доцент Сухотерин А.И.**

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

Целями изучения дисциплины являются:

1. Дать студентам знания по организации целесообразных мероприятий по защите информации на предприятиях (организациях и учреждений) с различными формами собственности с учетом современных требований в области теории обеспечения информационной безопасности на основе комплексного подхода.

2. Выработать и закрепить у студентов базовые умения и навыки по практической организации и реализации современных технологий защиты информации на предприятиях (организациях и учреждений) с различными формами собственности с учетом современных международных и отечественных стандартов обеспечения информационной безопасности.

В процессе обучения студент приобретает и совершенствует следующие компетенции.

Общекультурные компетенции:

- ОК-5: способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики;

Общепрофессиональные компетенции:

- ОПК-7: способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты

Профессиональные компетенции:

- ПК-10: способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности;

Профильно-специализированные компетенции:

- ПСК-1: способность решать задачи первичного финансового мониторинга в рамках функционирования служб внутреннего контроля субъектов финансового мониторинга;
- ПСК-3: способность участвовать в разработке информационно-аналитических систем финансового мониторинга.

Основными задачами дисциплины являются:

- раскрытие сущности, целей и задач обеспечения информационной безопасности на предприятии;
- определение принципов и этапов разработки современных систем информационной безопасности предприятия;
- освоение технологии установления состава защищаемой информации и выявления объектов защиты;
- **выявление актуальных информационных угроз и опасных** нарушителей (злоумышленников);
- овладение методами оценки уязвимости защищаемой информации;
- определение параметров и структуры потребных систем информационной безопасности современного предприятия;
- установление состава целесообразных мероприятий (технологий) по обеспечению по обеспечению информационной безопасности различных предприятий;
- раскрытие структуры и методов управления информационной безопасностью;
- определение показателей эффективности системы информационной безопасности и методики ее оценки.

После завершения освоения данной дисциплины студент должен;

Знать:

- основные понятия, цели и задачи обеспечения информационной безопасности предприятия;
- сущность и составляющие современной системы обеспечения информационной безопасности предприятия;
- принципы организации и этапы разработки системы обеспечения информационной безопасности предприятия;
- факторы, влияющие на организацию обеспечения информационной безопасности предприятия;
- технологию определения состава защищаемой информации и объектов информационной безопасности;
- методы анализа и оценки информационных угроз и уязвимостей информационных объектов;
- технологическое и организационное построение потребной системы информационной безопасности;
- состав мероприятий и условия, обеспечивающие функционирование

системы информационной безопасности;

- технологию управления системой информационной безопасности;
- методику проведения анализа эффективности функционирования системы информационной безопасности;

Уметь:

- выявлять угрозы и уязвимости информационной безопасности применительно к объектам защиты;
- определять состав конфиденциальной информации применительно к видам тайны;

- выявлять причины, обстоятельства и условия дестабилизирующего воздействия на защищаемую информацию со стороны различных источников воздействия;
- выявлять применительно к объекту защиты каналы и методы несанкционированного доступа к конфиденциальной информации;
- определять направления и виды защиты информации с учетом характера информации и задач по ее защите;
- организовывать комплексный подход по защите информации;

Владеть навыками:

- определения требований и состава средств, методов и мероприятий по организации защиты информации;
- использования методов (технологий) организации, планирования и контроля функционирования систем информационной безопасности;
- разработки организационно-функциональной структуры и комплекса нормативно-методического обеспечения систем информационной безопасности;
- проведения количественной и качественной оценки эффективности функционирования различных компонентов систем информационной безопасности.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Комплексное обеспечение защиты информации объекта информатизации (предприятия)» 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 прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

3. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 8 зачетных единиц, 288 часов.

Таблица 1

Наименование параметров	**Очное обучение**					
	Всего часов	**Семестр 7**	**Семестр 8**			
Общая трудоемкость	**288**	**144**	**144**			
Аудиторные занятия	**88**	**64**	**24**			
Лекции (Л)	44	32	12			
Практические занятия (ПЗ)	44	32	12			
Лабораторные работы(ЛР)	-	-	-			
Самостоятельная работа	**200**	**78**	**122**			
КСР	-	-	-			
Курсовые работы (проекты)	-	-	+			
Контрольная работа, домашнее задание	-	+	-			
Текущий контроль знаний (7-8 и 15-16 неделя)	+	+	+			
КонтрольСРС	-	-	-			
Вид итогового контроля	**Зачёт/ Экзамен**	**Зачет**	**Экзамен**			

4. Содержание дисциплины
4.1. Темы дисциплины и виды занятий

Таблица 2

Наименование тем	Очное обучение, час.						Код компетенций
	Лекции	Практические занятия	Занятие в интерак. форме				
1	2	3	4	5	6	7	8
	Семестр 7						
I раздел. Теоретико-прикладные основы ИБ предприятия							
Тема 1.Введение в дисциплину	2	2	1				ОК-5 ОПК-7 ПК-10 ПСК-1,3
Тема 2.Сущность и задачи системы обеспечения информационной безопасности предприятия (СИБ)	2	2	1				ОК-5 ОПК-7 ПК-10 ПСК-1,3
Тема 3. Принципы организации и этапы функционирования СИБ предприятия	2	2	1				ОК-5 ОПК-7 ПК-10 ПСК-1,3
Тема 4.Факторы, влияющие на организацию СИБ современного предприятия	2	2	1				ОК-5 ОПК-7 ПК-10 ПСК-1,3
Тема 5.Определение и нормативное закрепление состава защищаемой информации	2	2	1				ОК-5 ОПК-7 ПК-10 ПСК-1,3
Тема 6.Выявление объектов информационной защиты на предприятии	2	2	1				ОК-5 ОПК-7 ПК-10 ПСК-1,3
II раздел. Базовые организационно - аналитические технологии ИБ							
Тема 7.Выявление, оценка источников, способов и результатов дестабилизирующего воздействия	2	2	1				ОК-5 ОПК-7 ПК-10 ПСК-1,3
Тема 8.Определение потенциальных каналов и методов противоправных действий	2	2	1				ОК-5 ОПК-7 ПК-10 ПСК-1,3
Тема 9.Выявление нарушителей, определение уязвимостей информационных объектов и последствий противоправных действий	4	4	1				ОК-5 ОПК-7 ПК-10 ПСК-1,3
Тема 10.Определение потребных компонентов целесообразной СИБ	4	4	2				ОК-5 ОПК-7 ПК-10 ПСК-1,3
Тема 11.Определение условий функционирования СИБ	4	4	2				ОК-5 ОПК-7

							ПК-10 ПСК-1,3
Тема 12.Разработка моделей СИБ предприятия	4	4	2				ОК-5 ОПК-7 ПК-10 ПСК-1,3
Всего (за семестр)	**32**	**32**	**15**				

Продолжение табл.2

1	2	3	4	5	6	7	8
	Семестр 8						
III раздел. Виды обеспечения функционирования системы ИБ							
Тема 13.Технологическое построение СИБ	1	1	1				ОК-5 ОПК-7 ПК-10 ПСК-1,3
Тема 14.Организационно - кадровое обеспечение функционирования СИБ	1	1	1				ОК-5 ОПК-7 ПК-10 ПСК-1,3
Тема 15.Материально-техническое обеспечение СИБ	1	1	1				ОК-5 ОПК-7 ПК-10 ПСК-1,3
Тема 16.Нормативно-методическое обеспечение СИБ	1	1	2				ОК-5 ОПК-7 ПК-10 ПСК-1,3
Тема 17.Назначение, структура и содержание управления СИБ	1	1	2				ОК-5 ОПК-7 ПК-10 ПСК-1,3
Тема 18.Планирование функционирования СИБ	1	1	2				ОК-5 ОПК-7 ПК-10 ПСК-1,3
IV раздел. Ключевые управленческие аспекты обеспечения ИБ предприятия							
Тема 19.Сущность и содержание контроля (аудита) функционирования СИБ	1	1	1				ОК-5 ОПК-7 ПК-10 ПСК-1,3
Тема 20.Управление СИБ в условиях чрезвычайных ситуаций	1	1	1				ОК-5 ОПК-7 ПК-10 ПСК-1,3
Тема 21.Общая характеристика подходов по оценки эффективности систем информационной безопасности	1	1	1				ОК-5 ОПК-7 ПК-10 ПСК-1,3
Тема 22.Методы и модели функциональной оценки эффективности СИБ предприятия	1	1	1				ОК-5 ОПК-7 ПК-10 ПСК-1,3
Тема 23.Компьютерное моделирование функциональной оценки эффективности СИБ	1	1	1				ОК-5 ОПК-7 ПК-10 ПСК-1,3
Тема 24.Экономическая оценка эффективности СИБ предприятия	1	1	1				ОК-5 ОПК-7 ПК-10 ПСК-1,3
Всего (за семестр)	**12**	**12**	**15**				
Итого (за дисциплину)	**44**	**44**	**30**				

4.2. Содержание тем дисциплины

Тема 1. Введение в дисциплину

Предмет, задачи и содержание курса. Значение и место курса в подготовке кадров в области информационной безопасности по направлению «Бакалавр» с профилем подготовки "Организация и технология защиты информации". Взаимосвязь курса с другими дисциплинами направления.

Структура курса. Распределение тем по видам аудиторных занятий. Формы проведения практических занятий. Формы проверки знаний.

Анализ источников, научной и учебной литературы по курсу. Самостоятельная работа студентов. Знания и умения студентов, которые должны быть получены в результате изучения курса.

Тема 2. Сущность и задачи системы обеспечения информационной безопасности предприятия

Понятие и сущность системы обеспечения информационной безопасности предприятия (СИБ). Назначение и задачи СИБ предприятия.

СИБ предприятия как средство выражения концептуальных основ теории и практики современной защиты информации. Методология защиты информации как теоретический базис построения СИБ предприятия.

Тема 3. Принципы организации и этапы функционирования системы информационной безопасности

Методологические основы организации СИБ современного предприятия как сложная человеко-машинная система. Основные положения теории систем.

Принципы организации СИБ предприятия. Основные требования, предъявляемые к обеспечению информационной безопасности.

Содержательная характеристика этапов разработки (проектирования) современных систем обеспечения информационной безопасности предприятия.

Тема 4. Факторы, влияющие на организацию обеспечения информационной безопасности современного предприятия

Основные факторы, влияющие на организацию обеспечения информационную безопасность предприятия: организационно-правовая форма и характер основной деятельности предприятия; состав, объем и степень конфиденциальности защищаемой информации; структура и территориальное расположение предприятия; режим функционирования предприятия; конструктивные особенности предприятия; количественные и качественные параметры ресурс обеспечения; степень автоматизации основных процедур обработки защищаемой информации.

Характер и степень влияния различных факторов на организацию обеспечения информационную безопасность.

Тема 5. Определение и нормативное Закрепление состава защищаемой информации

Методика определения состава защищаемой информации и этапы работы по выявлению состава защищаемой информации.

Функции руководства предприятия и подразделений предприятия, экспертной комиссии, службы защиты информации по определению и закреплению защищаемой информации.

Классификация информации по видам тайны и степеням конфиденциальности/секретности.

Нормативное закрепление состава защищаемой информации и структура перечней сведений, относимых к различным видам тайны. Порядок внедрения перечней, внесения в них изменений и дополнений.

Тема 6. Выявление объектов информационной защиты на предприятии

Факторы, определяющие состав носителей информации. Методика выявления состава носителей защищаемой информации. Носители защищаемой информации на предприятии как объекты информационной защиты.

Хранилища носителей информации на предприятии как объекты защиты. Особенности помещений (защищенных и выделенных) для работы с закрытой информацией как объекты защиты.

Состав технических средств обработки, передачи, транспортировки и защиты информации, являющихся объектами защиты. Состав средств обеспечения функционирования предприятия, подлежащих защите.

Факторы, определяющие необходимость защиты периметра и здания предприятия.

Специфика персонала предприятия как объекта защиты.

Тема 7. Выявление, оценка источников, способов и результатов дестабилизирующего воздействия

Определение источников дестабилизирующего воздействия на информацию и видов их воздействия.

Методика выявления способов воздействия на информацию.

Определение причин, обстоятельств и условий дестабилизирующего воздействия на информацию.

Оценка ущерба от потенциального дестабилизирующего воздействия на информацию.

Тема 8. Определение потенциальных каналов и методов противоправных действий

Соотношение между каналами противоправных действий и источниками воздействий на защищаемую информацию на предприятии.

Определение возможных методов противоправных действий к защищаемой информации.

Методика выявления каналов противоправных действий к защищаемой информации.

Тема 9. Выявление нарушителей, определение уязвимостей информационных объектов и последствий противоправных действий

Методика выявления нарушителей (незаконных пользователей). Определение уязвимостей информационных объектов и возможностей доступа нарушителей к защищаемой информации.

Оценка степени уязвимости информации в результате действий нарушителей различных категорий. Потенциальные последствия реализаций противоправных действий.

Тема 10. Определение потребных компонентов целесообразной системы информационной безопасности

Факторы, влияющие на выбор компонентов целесообразной СИБ предприятия. Объекты защиты как основной фактор, определяющий потребный состав компонентов СИБ предприятия.

Основные требования, предъявляемые к выбору методов и средств защиты, зависимость их от структуры предприятия, защищаемых элементов объектов, условий функционирования СИБ.

Тема 11. Определение условий функционирования системы информационной безопасности

Обеспечение полноты составляющих защиты информации на предприятии. Учет всех факторов и обстоятельств, оказывающих влияние на качество обеспечение информационной безопасности.

Обеспечение безопасности всей совокупности подлежащей защите информации: во всех компонентах ее сбора, хранения, передачи и использования; во все время и при всех режимах функционирования систем обработки информации на предприятии.

Тема 12. Разработка моделей системы информационной безопасности предприятия

Понятие модели объекта информационной безопасности, основные виды моделей и их характеристика.

Модель как инструмент количественного и качественного анализа функционирования СИБ предприятия. Значение моделирования отдельных процессов функционирования СИБ.

Выбор различных функциональных структуры СИБ, зависимость их от объектов информационной защиты, характера и условий функционирования предприятия: структурно-функциональная модель СИБ; организационная модель СИБ; информационная модель СИБ.

Тема 13. Технологическое построение системы информационной безопасности

Общее содержание работ по организации системы информационной безопасности (состав и характеристика стадий и этапов построения СИБ на предприятии).

Привлекаемые силы и средства проектирования потребной СИБ для предприятия.

Виды проектирования СИБ: индивидуальное, типовое и смешанное.

Тема 14. Организационно - кадровое обеспечение функционирование системы информационной безопасности

Определение состава кадрового обеспечения функционирования СИБ.

Распределение функций по защите информации между руководством предприятия, службой защиты информации, специальными комиссиями и пользователями защищаемой информации, обеспечение взаимодействия между ними.

Разработка нормативных документов, регламентирующих деятельность персонала по защите информации.

Подбор и обучение персонала предприятия по вопросам обеспечения информационной безопасности.

Тема 15. Материально-техническое обеспечение системы информационной безопасности

Значение материально-технического обеспечения (МТО) функционирования СИБ на предприятии. Решаемые задачи МТО СИБ.

Определение сил и средств материально-технического обеспечения СИБ.

Организация материально-технического обеспечения СИБ на предприятии. Профилактические виды работ на технических системах и средствах информационной безопасности. Ремонтные виды работ и их содержание.

Тема 16. Нормативно-методическое обеспечение системы информационной безопасности

Значение нормативно-методического обеспечения функционирования СИБ предприятия.

Перечень вопросов по функционированию системы защиты информации на предприятии, требующих документационного закрепления.

Состав нормативно-методических документов по обеспечению функционирования СЗИ, их назначение, структура и содержание.

Порядок разработки и внедрения потребных документов в СИБ.

Тема 17. Назначение, структура и содержание управления системой информационной безопасности

Понятие, цели, функции и задачи управления СИБ предприятия.

Сущность и содержание процессов управления СИБ.

Принципы управления СИБ. Основные стили (вид и формы) управления СИБ.

Структура и содержание общей технологии управления СИБ.

Привлекаемые силы и средства управления СИБ современного предприятия.

Тема 18. Планирования функционирования системы информационной безопасности

Понятие, задачи и виды планирования функционирования СИБ.

Способы и стадии планирования. Факторы, влияющие на выбор принципов и способов планирования.

Структура и общее содержание планов организации и функционирования СИБ. Методы сбора, обработки и изучения информации, необходимой для планирования.

Организация выполнения планов функционирования СИБ предприятия.

Особенности планирование функционирования СИБ предприятия в чрезвычайных условиях.

Тема 19. Сущность и содержание контроля (аудита) функционирования системы информационной безопасности

Понятие и цель проведения контрольных мероприятий в СИБ.

Виды и методы контроля функционирования СИБ.

Анализ и использование результатов проведения контрольных мероприятий в СИБ предприятия.

Особенности проведения аудита отдельных составляющих СИБ в различных условиях их функционирования.

Тема 20. Управление системой информационной безопасности предприятия в условиях чрезвычайных ситуаций

Понятие и основные виды чрезвычайных ситуаций на современном предприятии.

Технология принятия решений по обеспечению информационной безопасности в условиях чрезвычайной ситуации.

Факторы, влияющие на принятие решений в СИБ в условиях чрезвычайной ситуации.

Подготовка мероприятий по обеспечению ИБ на случай возникновения чрезвычайных ситуаций.

Тема 21. Общая характеристика подходов по оценки эффективности систем информационной безопасности

Классификация подходов к оценке эффективности систем зашиты информации.

Вероятностный подход: структуризация предметной области оценки; анализ вероятности реализации угроз безопасности; расчетные соотношения.

Оценочный подход на основе формирования требований к защищенности объекта: классы защищенности и их характеристика; контрольно-испытательные процедуры определения соответствия защиты установленным требованиям.

Содержание и особенности экспертной оценки эффективности защиты: выбор системы измерений (вербальные и вербально-числовые шкалы); организация процедуры экспертного оценивания (подбор экспертов, составление вопросников, обработка результатов).

Сравнительный анализ подходов к оценке эффективности СИБ.

Тема 22. Методы и модели функциональной оценки эффективности системы информационной безопасности предприятия

Классификационная структура методов и моделей оценки. Базовые понятия и определения, используемые в моделях. Системы показателей защищенности (эффективности).

Метод оценки уровня безопасности и аналитические модели определения базовых и обобщенных показателей уязвимости. Метод анализа риска. Метод оценки на основе структурных вопросников.

Области применения и анализ приемлемости различных методов и моделей для решения задачи оценки эффективности СИБ.

Тема 23. Компьютерное моделирование функциональной оценки эффективности системы информационной безопасности

Особенности компьютерного моделирования функциональной (технической) оценки эффективности СИБ. Показатели и возможные критерии компьютерной оценки эффективности функционирования

СИБ. Возможные методы и виды компьютерных моделей оценки эффективности СИБ.

Решаемые задачи и основные структурные компоненты компьютерной модели Домарева. Математический метод реализации модели Домарева. Исходные и выходные данные модели Домарева. Порядок применения компьютерной модели Домарева для оценки эффективности отдельных подсистем и всей СИБ на предприятии.

Тема 24. Экономическая оценка эффективности СИБ предприятия

Общая характеристика существующих подходов экономической оценки эффективности системы информационной безопасности.

Существующие методы (двухфакторный и трехфакторный) оценки информационных рисков в СИБ.

Особенности применения метода совокупной стоимости владения (определения затрат) СИБ.

Основы обоснования возврата инвестиций (оценка доходной части) для СИБ.

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

1. «Методические указания для обучающихся по освоению дисциплины».

2. «Методические указания для обучающихся по выполнению курсовых работ».

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

Структура фонда оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине приведена в Приложении 1.

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

Основная литература:

1. Грибунин В.Г. Комплексная система защиты информации на предприятии. Учебное пособие – М.: «Академия», 2009.

2. Северин В.А. Комплексная защита информации на предприятии. Учебник для вузов. – М.: «Городец», 2008

Дополнительная литература:

1. Гришина Н.В. Организация комплексной защиты информации. – М.: Гелиос АРВ, 2007.

2. Ярочкин В.И. Информационная безопасность. М.: Международные отношения, 2008.

Рекомендуемая литература:

1. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. К.: ООО "ТИД "СД", 2001.

2. Завгородний В.И. Комплексная защита информации в компьютерных системах. М., 2001.

3. Игнатьева А.В., Максимцов М.М. Исследование систем управления. М.: ЮНИТИ-ДАНА, 2000.

4. Семкин С.Н., Семкин А.Н. Основы безопасности объектов обработки информации. - Орел, 2000.

5. Устинов Г.Н. Основы информационной безопасности систем и сетей передачи данных. М.: СИНТЕГ, 2000.

Электронные книги:

1. Тайна предприятия: что и как защищать
http://fanread.ru/book/4624607/?page=1

2. Информационная безопасность в режиме «сетевой войны»
http://fanread.ru/book/3731798/?page=1

3. Секреты и ложь. Безопасность данных в цифровом мире.

http://fanread.ru/book/4628219/?page=1

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. http://www.academy.it.ru/ – академия АЙТИ.
4. http://www.iso27000.ru/ - портал по управлению информационной безопасностью.

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: *MS Office.*

Информационные справочные системы:

1. Справочно-правовая система «Консультант плюс».
2. Ресурсы информационно-образовательной среды МГОТУ
3. Рабочая программа и методическое обеспечение по дисциплине «Комплексное обеспечение защиты информации объекта информатизации (предприятия)».

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 лекций в форме слайд-презентаций, оборудованный современными лицензионными программно-техническими средствами: операционная система не ниже Windows XP; офисные программы MS Office 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

«КОМПЛЕКСНОЕ ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ ОБЪЕКТА ИНФОРМАТИЗАЦИИ (ПРЕДПРИЯТИЯ)»

(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.	ОК-5	способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	Темы 1, 2,3, 4, 5,6	основные экономические категории и закономерности, методы анализа экономических явлений и процессов, специфические черты функционирования хозяйственной системы на (микро- и макро-) уровнях, основные понятия экономической и финансовой деятельности отрасли и ее структурных подразделений	оценивать эффективность управленческих решений и анализировать экономические показатели деятельности подразделения	навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности;
2.	ОПК-7	способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей	Темы 1,2,3, 4, 5,6	основы: российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации; характеристику основных отраслей российского	анализировать и составлять правовые акты и осуществлять правовую оценку информации, используемой в профессиональной деятельности, предпринимать необходимые меры по восстановлению нарушенных прав осуществлять	навыками обоснования, выбора, реализации и контроля результатов управленческого решения

		функционирования объекта защиты		права; правовые основы обеспечения национальной безопасности Российской Федерации	планирование и организацию работы рабочего коллектива при выполнении поставленных задач	
3.	ПК-10	способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	Темы 1, 2,3, 4, 5,6		анализировать и составлять правовые акты и осуществлять правовую оценку информации, используемой в профессиональной деятельности, предпринимать необходимые меры по восстановлению нарушенных прав	навыками публичной речи, аргументации, ведения дискуссии и полемики, практического анализа логики различного рода рассуждений; навыками критического восприятия информации; навыками письменного аргументированного изложения собственной точки зрения
4.	ПСК-1	способность решать задачи первичного финансового мониторинга в рамках функционирования служб внутреннего контроля субъектов финансового мониторинга	Темы 1, 2,3, 4, 5,6	типовые структуры и принципы организации компьютерных сетей; последовательность и содержание этапов построения компьютерных сетей;	пользоваться сетевыми средствами для обмена данными, в том числе с использованием глобальной информационной сети Интернет	навыками работы с технической документацией на ЭВМ и вычислительные системы
5.	ПСК-3	способность участвовать в разработке информационно-аналитических систем финансового мониторинга	Темы 1, 2,3, 4, 5,6	Основные нормативные документы в области информационной безопасности	Выбирать методические и нормативные документы в соответствии с решаемой задачей	Навыками по работе с технической документацией, требуемой или рекомендуемой по соответствующему тематическому вопросу

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
ОК-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.
ОПК-7	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-10	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.
ПСК-1	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.
ПСК-3	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.

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. Анализ существующих подходов построения СИБ в системе информационной безопасности на типовом предприятии.
2. Анализ существующих подходов определения состава защищаемой информации в системе информационной безопасности на типовом предприятии.

3. Анализ существующих подходов определения степеней конфиденциальности защищаемой информации в системе информационной безопасности на типовом предприятии.
4. Анализ существующих подходов определения ценности защищаемого информационного ресурса в системе информационной безопасности на типовом предприятии.
5. Анализ существующих подходов выявления информационных угроз в системе информационной безопасности на типовом предприятии.
6. Анализ существующих подходов выявления уязвимостей информационных объектов в системе информационной безопасности на типовом предприятии.
7. Анализ существующих подходов определения важнейших объектов защиты в системе информационной безопасности на типовом предприятии.
8. Анализ существующих подходов выявления возможных нарушителей (злоумышленников) в системе информационной безопасности на типовом предприятии.
9. Анализ существующих подходов определения возможных технических каналов утечки информации в системе информационной безопасности на типовом предприятии.
10 Анализ существующих подходов выявления каналов несанкционированного доступа к защищаемой информации в системе информационной безопасности на типовом предприятии.
10. Обоснование потребного подхода к выявлению факторов, влияющих на организацию СИБ построения СИБ на типовом предприятии.
11. Обоснование потребного подхода к стратегии информационной безопасности на типовом предприятии.
12. Обоснование потребного подхода к требуемому уровню защиты информационных ресурсов в системе информационной безопасности на типовом предприятии.
13. Обоснование потребного подхода к определению состава защищаемой информации в системе информационной безопасности на типовом предприятии.
14. Обоснование потребного подхода к определению степеней конфиденциальности защищаемой информации в системе информационной безопасности на типовом предприятии.
15. Обоснование потребного подхода к определению ценности защищаемого информационного ресурса в системе информационной безопасности на типовом предприятии.
16. Обоснование потребного подхода к определению важнейших объектов защиты в системе информационной безопасности на типовом предприятии.
17. Обоснование потребного подхода к определению структурных компонентов в системе информационной безопасности на типовом предприятии.

18. Обоснование потребного подхода к выявлению информационных угроз в системе информационной безопасности на типовом предприятии.
19. Обоснование потребного подхода к выявлению уязвимостей информационных объектов в системе информационной безопасности на типовом предприятии.
20. Обоснование потребного подхода выявления возможных нарушителей (злоумышленников) информации в системе информационной безопасности на типовом предприятии.

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

Формой контроля знаний по дисциплине «Комплексное обеспечение защиты информации объекта информатизации (предприятия)» являются две текущие аттестации в виде тестов и итоговая аттестация в виде зачета/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	ОК-5 ОПК-7 ПК-10 ПК-8 ПСК-1 ПСК-3	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	ОК-5 ОПК-7 ПК-10 ПК-8 ПСК-1 ПСК-3	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/Экзамен	ОК-5 ОПК-7 ПК-10 ПК-8 ПСК-1 ПСК-3	3теоретических вопроса + практическое задание	Зачет /Экзамен проводится в письменной форме, путем ответа на вопросы.	Результаты предоставляются в день проведения зачета/экзамена	Критерии оценки: «Зачтено»: • знание основных понятий предмета; • умение

				Время, отведенное на процедуру – 15 минут.		использовать и применять полученные знания на практике; • работа на практических занятиях; • знание основных научных теорий, изучаемых 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 практических занятиях; • не отвечает на вопросы. Критерии оценки: «**Отлично**»: 1. знание основных понятий предмета; 2. умение использовать и применять полученные знания на практике; 3. работа на практических 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**»: • демонстрирует частичные знания по темам дисциплин; • незнание неумение использовать и применять полученные знания на практике; • не работал на практических занятиях; «**Неудовлетвори-тельно**»: • демонстрирует частичные знания по темам дисциплин; • незнание основных понятий предмета; • неумение использовать и применять полученные знания на практике; • не работал на практических занятиях; • 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.

4.1.1 Вопросы 7 семестр

1-ое промежуточное тестирование (Т1)

1. Незаконный сбор, присвоение и передача сведений составляющих коммерческую тайну, наносящий ее владельцу ущерб, - это...
(?) политическая разведка;
(!) промышленный шпионаж;
(?) добросовестная конкуренция;
(?) конфиденциальная информация;
(?) правильного ответа нет.
2. Какая информация является охраняемой внутригосударственным законодательством или международными соглашениями как объект интеллектуальной собственности?
(?) любая информация;
(?) только открытая информация;
(!) запатентованная информация;
(?) закрываемая собственником информация;
(?) коммерческая тайна.
3. Кто может быть владельцем защищаемой информации?
(?) только государство и его структуры;
(?) только предприятия, акционерные общества, фирмы;
(?) только общественные организации;
(!) все вышеперечисленные организационные структуры;
(?) кто угодно.
4. Какие сведения на территории РФ могут составлять коммерческую тайну?
(?) учредительные документы и устав предприятия;
(?) сведенья о численности работающих, их заработной плате и условиях труда;
(!) документы о платежеспособности, об уплате налогов, о финансово-хозяйственной деятельности;
(?) другие;
(?) любые.
5. Какие закрытые сведения входят в понятие «коммерческая тайна»?
(?) только связанные с производством;
(?) только связанные с планированием производства и сбытом продукции;
(?) только технические и технологические решения предприятия;

(?) только 1 и 2 вариант ответа;
(!) три первых варианта ответа.

6. Что называют источником конфиденциальной информации?

(!) объект, обладающий определенными охраняемыми сведениями, представляющими интерес для злоумышленников;
(?) сведения о предметах, объектах, явлениях и процессах, отображаемые на каком-либо носителе;
(?) доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники;
(?) это защищаемые предприятием сведения в области производства и коммерческой деятельности;
(?) способ, позволяющий нарушителю получить доступ к обрабатываемой или хранящейся в ПЭВМ информации.

7. Как называют процессы обмена информацией с помощью официальных, деловых документов?

(?) непосредственные**;**
(?) межличностные;
(?) формальные**;**
(?) неформальные**;**
(!) конфиденциальные.

8. Какое наиболее распространенное действие владельца конфиденциальной информации, приводит к неправомерному овладению ею при минимальных усилиях со стороны злоумышленника?

(?) хищение носителей информации;
(?) использование технических средств для перехвата электромагнитных ПЭВМ;
(!) разглашение;
(?) копирование программой информации с носителей;
(?) другое.

9. Каким образом происходит разглашение конфиденциальной информации?

(?) утеря документов и других материалов, или пересылка их посредством почты, посыльного, курьера;
(?) опубликование материалов в печати;
(?) сообщение, передача, предоставление в ходе информационного обмена;
(!) все вышеперечисленные способы;
(?) правильного варианта ответа нет.

10. Какие основные цели преследует злоумышленник при несанкционированном доступе к информации?

(?) получить, изменить, а затем передать ее конкурентам;
(?) размножить или уничтожить ее;
(!) получить, изменить или уничтожить;
(?) изменить и уничтожить ее;
(?) изменить, повредить или ее уничтожить.

11. Какой самый прямой и эффективный способ склонения к сотрудничеству?
(?) психическое давление;
(!) подкуп;
(?) преследование;
(?) шантаж;
(?) угрозы.
12. Наиболее сложный и дорогостоящий процесс несанкционированного доступа к источникам конфиденциальной информации?
(?) инициативное сотрудничество;
(?) выпытывание;
(?) наблюдение;
(!) хищение;
(?) копирование.
13. Какое из утверждений неверно?
(?) подкуп — сложный процесс, требует долгой и кропотливой работы;
(?) выпытывание — это стремление путем внешне наивных вопросов получить определенные сведения;
(!) процесс наблюдения не сложен, так как не требует затрат сил и средств;
(?) под незаконным подключением понимают контактное или бесконтактное подсоединение к линиям и проводам с целью несанкционированного доступа к информации, образующейся или передаваемой в них;
(?) негласное ознакомление — способ получения информации, к которой субъект не допущен, но при определенных условиях он может получить возможность кое-что узнать.
14. Завершающим этапом любого сбора конфиденциальной информации является
(?) копирование;
(?) подделка;
(!) аналитическая обработка;
(?) фотографирование;
(?) наблюдение.
15. Как называются реальные или потенциально возможные действия или условия, приводящие к овладению, хищению, искажению, изменению или уничтожению информации?
(?) ненадежность;
(!) угроза;
(?) несчастный случай;
(?) авария;
(?) правильного ответа среди перечисленных нет.
16. Что в скором времени будет являться главной причиной информационных потерь?
(?) материальный ущерб, связанный с несчастными случаями;
(?) кража и преднамеренная порча материальных средств;
(!) информационные инфекции;

(?) аварии и выход из строя аппаратуры, программ и баз данных;
(?) ошибки эксплуатации.

17. В каком варианте ответа инфекции расположены от более простого к более сложному, по возрастанию?

(?) логические бомбы, троянский конь, червь, вирус;
(?) червь, вирус, логические бомбы, троянский конь;
(?) червь, логические бомбы, вирус, троянский конь;
(?) логические бомбы, вирус, троянский конь, червь;
(!) вирус, логические бомбы, троянский конь, червь.

18. Причины связанные с информационным обменом приносящие наибольшие убытки?

(?) остановка или выход из строя информационных систем;
(?) потери информации;
(?) неискренность;
(?) проникновение в информационную систему;
(!) перехват информации.

19. Какие цели преследуются при активном вторжении в линии связи?

(?) анализ информации (содержание сообщений, частоту их следования и факты прохождения, пароли, идентификаторы коды) и системно-структурный анализ;
(?) воздействие на поток сообщений (модификация, удаление и посылка ложных сообщений) или воспрепятствие передаче сообщений;
(?) инициализация ложных соединений;
(!) варианты 1 и 2;
(?) варианты 2 и 3.

20. Что определяет модель нарушителя?

(?) категории лиц, в числе которых может оказаться нарушитель;
(?) возможные цели нарушителя и их градации по степени важности и опасности;
(?) предположения о его квалификации и оценка его технической вооруженности;
(?) ограничения и предположения о характере его действий;
(!) все выше перечисленные.

21. Выберите наиболее полный список мотивов, которые преследуют компьютерные пираты (хакеры), пытаясь получить несанкционированный доступ к информационной системе или вычислительной сети.

(?) ознакомление с информационной системой или вычислительной сетью;
(?) похитить программу или иную информацию;
(?) оставить записку, выполнить, уничтожить или изменить программу;
(?) вариант 2 и 3;
(!) вариант 1, 2 и 3.

22. Какое из утверждений неверно?

(?) наблюдается тенденция к стремительному росту попыток получить несанкционированный доступ к информационным системам или вычислительным сетям;
(?) недовольный руководителем служащий создает одну из самых больших угроз вычислительным системам коллективного пользования;
(?) считается, что компьютерные преступления, более легкий путь добывания денег, чем ограбление банков;
(!) очень малое число фирм могут пострадать от хакеров;
(?) к категории хакеров-профессионалов обычно относят: преступные группировки, преследующие политические цели.

23. Какое из утверждений неверно?

(?) хакеры могут почерпнуть много полезной информации из газеты и других периодических изданий;
(?) хакерами часто используется завязывание знакомств для получения информации о вычислительной системе или выявления служебных паролей;
(?) один из наиболее эффективных и наименее рискованных путей получения конфиденциальной информации и доступа к ЭВМ — просто изучая черновые распечатки;
(!) о перехвате сообщений в каналах связи речь может идти лишь в связи с деятельностью военных или секретных служб;
(?) после получения необходимого объема предварительной информации, компьютерный хакер-профессионал осуществляет непосредственное вторжение в систему.

24. Какое из утверждений неверно?

(!) наибольшие убытки (в среднем) приносит саботаж в нематериальной сфере;
(?) убытки, связанные с забастовками не превышают убытков связанных с аварией оборудования;
(?) уход ведущих специалистов опасен для малых центров;
(?) хищения, в первую очередь осуществляются сотрудниками предприятия или пользователями;
(?) аварии оборудования или основных элементов системы являются мало распространенными и определяются надежностью аппаратуры.

25. Метод скрытие — это...

(?) максимальное ограничение числа секретов, из-за допускаемых к ним лиц;
(!) максимального ограничения числа лиц, допускаемых к секретам;
(?) уменьшение числа секретов неизвестных большинству сотрудников;
(?) выбор правильного места, для утаивания секретов от конкурентов;
(?) поиск максимального числа лиц, допущенных к секретам.

26. Что включает в себя ранжирование как метод защиты информации?

(?) регламентацию допуска и разграничение доступа к защищаемой информации***;***
(?) деление засекречиваемой информации по степени секретности;
(?) наделять полномочиями назначать вышестоящими нижестоящих на соответствующие посты;

(!) вариант ответа 1 и 2;
(?) вариант ответа 1, 2 и 3.

27. К какому методу относятся следующие действия: имитация или искажение признаков и свойств отдельных элементов объектов защиты, создания ложных объектов?

(!) скрытие;
(?) дезинформация;
(?) дробление;
(?) кодирование;
(?) шифрование.

28. Что в себя включают морально-нравственные методы защиты информации?

(?) воспитание у сотрудника, допущенного к секретам, определенных качеств, взглядов и убеждений;
(?) контроль работы сотрудников, допущенных к работе с секретной информацией;
(?) обучение сотрудника, допущенного к секретам, правилам и методам защиты информации, и навыкам работы с ней;
(?) вариант ответа 1 и 3;
(!) вариант ответа 1, 2 и 3.

29. Какое из выражений не верно?

(?) страхование — как метод защиты информации пока еще не получил признания;
(?) кодирование — это метод защиты информации, преследующий цель скрыть от соперника содержание защищаемой информации;
(?) шифрование может быть предварительное и линейное;
(!) дирекция очень часто не может понять необходимость финансирования безопасности;
(?) безопасность предприятия — не стабильное состояние предприятия, не поддающееся прогнозированию во времени.

30. Что является одним из основных признаков защищаемой информации?

(!) ограничения, вводимые собственником информации на ее распространение и использование
(?) в каком виде эта информация представлена (электронном, печатном, письменном и т.д.)
(?) все вышеперечисленное

2-ое промежуточное тестирование (Т2)

1. Какой должна быть защита информации с позиции системного подхода?

(?) безопасной для сотрудников;
(?) активной;
(?) универсальной;

(!) надежной;
(?) непрерывной.

2. Что такое «служба информационной безопасности»?

(?) система внештатных формирований, предназначенных для обеспечения безопасности объекта;
(?) структурное подразделение, предназначенное для охраны помещений и территорий предприятия;
(!) система штатных органов управления и организационных формирований, предназначенных для обеспечения безопасности и защиты конфиденциальной информации;
(?) структурное подразделение, предназначенное для хранения и выдачи документов, носителей конфиденциальной информации;
(?) структурное подразделение, задача которого: подбор персонала и работа с сотрудниками.

3. Кому непосредственно подчиняется служба информационной безопасности?

(?) владельцу предприятия;
(?) владельцу предприятия и лицу которому тот подчиняется;
(?) руководителю предприятия, либо лицу, которому тот делегировал свои права по руководству ее деятельностью;
(?) заместителю руководителя предприятия по организационным вопросам;
(!) начальнику службы безопасности.

4. Какие задачи не входят в круг обязанностей службы информационной безопасности?

(!) внедрение в деятельность предприятия новейших достижений науки и техники, передового опыта в области обеспечения экономической безопасности предприятия;
(?) определение участков сосредоточения сведений, составляющих коммерческую тайну;
(?) определение на предприятии технологического оборудования, выход из строя которого может привести к большим экономическим потерям;
(?) ограничение круга сторонних предприятий, работающих с данным предприятием, на которых возможен выход из-под контроля сведений составляющих коммерческую тайну предприятия;
(?) определение круга сведений, составляющих коммерческую тайну.

5. Какие средства использует инженерно-техническая защита (по функциональному назначению)?

(?) программные, аппаратные, криптографические, технические;
(?) программные, физические, шифровальные, криптографические;
(?) программные, аппаратные, криптографические, физические;
(?) физические, аппаратные, материальные, криптографические;
(!) аппаратные, физические, программные, материальные.

6. В каком нормативном акте говорится о формировании и защите информационных ресурсов как национального достояния?

(?) в Конституции РФ;

(?) в Законе об оперативно розыскной деятельности;
(?) в Законе об частной охране и детективной деятельности;
(!) в Законе об информации, информационных технологиях и защите информации;
(?) в Указе Президента РФ № 170 от 20 января 1994 г. «Об основах государственной политики в сфере информатизации».

7. Владельцами (собственниками) защищаемой информации могут быть…

(?) государство и его структуры; предприятия, товарищества, акционерные общества;
(?) общественные организации; граждане государства: их права (тайна переписки, телефонных и телеграфных разговоров, врачебная тайна и др.)
(!) все вышеперечисленное

8. На каком уровне защиты информации создаются комплексные системы защиты информации?

(?) на организационно-правовом;
(?) на социально-политическом;
(?) на тактическом*;*
(?) на инженерно-техническом;
(!) на всех вышеперечисленных.

9. Какие существуют наиболее общие задачи защиты информации на предприятии?

(?) снабжение всех служб, подразделений и должностных лиц необходимой информацией, как засекреченной, так и несекретной*;*
(?) предотвращение утечки защищаемой информации и предупреждение любого несанкционированного доступа к носителям засекреченной информации;
(?) документирование процессов защиты информации, с целью получения соответствующих доказательств в случае обращения в правоохранительные органы;
(?) создание условий и возможностей для коммерческого использования секретной и конфиденциальной информации предприятия;
(!) все вышеперечисленные.

10. Какие меры и методы защиты секретной или конфиденциальной информации в памяти людей не являются основными?

(?) воспитание понимания важности сохранения в тайне доверенных им секретных или конфиденциальных сведений;
(?) подбор людей, допускаемых к секретным работам;
(?) обучение лиц, допущенных к секретам, правилам их сохранения;
(!) добровольное согласие на запрет работы по совместительству у конкурентов;
(?) стимулирование заинтересованности работы с засекреченной информацией и сохранения этих сведений в тайне.

11. В каком документе содержаться основные требования к безопасности информационных систем в США?

(?) в красной книге;
(?) в желтой прессе;
(!) в оранжевой книге;
(?) в черном списке;
(?) в красном блокноте.

12. Какое определение соответствует термину «Аутентификация»?

(?) набор норм, правил и практических приемов, которые регулируют управление, защиту и распределение ценной информации в данной организации;
(?) распознавание имени объекта;
(!) подтверждение того, что предъявленное имя соответствует объекту;
(?) регистрация событий, позволяющая восстановить и доказать факт происшествия событий;
(?) правильного определения нет.

13. Какое требование относится к термину «Подотчетность»?

(?) субъекты индивидуально должны быть идентифицированы;
(?) гарантированно защищенные механизмы, реализующие указанные базовые требования, должны быть постоянно защищены от "взламывания";
(?) необходимо иметь явную и хорошо определенную политику обеспечения безопасности;
(?) аудиторская информация должна храниться и защищаться так, чтобы имелась возможность отслеживать действия, влияющие на безопасность;
(!) метки, управляющие доступом, должны быть установлены и связаны с объектами.

14. Какой уровень безопасности системы соответствует низшему?

1) A;
2) B;
3) C;
4) D;
(!) E.

15. Какой класс присваивается системам которые не прошли испытания?

(?) A1;
(?) B2:
(?) B3;
(?) C4;
(!) D.

16. Что включают в себя технические мероприятия по защите информации?

(?) поиск и уничтожение технических средств разведки;
(?) кодирование информации или передаваемого сигнала;
(?) подавление технических средств постановкой помехи;
(?) применение детекторов лжи;
(!) все вышеперечисленное.

17. Какие устройства поиска технических средств разведки не относятся к устройствам поиска пассивного типа?
(!) металлоискатели;
(?) тепловизоры;
(?) устройства и системы поиска по электромагнитному излучению;
(?) детекторы записывающей аппаратуры
18. Какие устройства не относятся к устройствам поиска по электромагнитному излучению?
(?) частотомер;
(?) шумомер;
(?) сканер;
(!) нелинейный локатор;
(?) анализатор спектра.
19. С какого расстояния можно считать информацию с монитора компьютера?
(?) 200 м.
(!) менее 200 м.
(?) 500 м.
(?) 750 м.
(?) 1 км.
20. Какие материалы не применяются при экранировании помещения?
(?) листовая сталь;
(?) медная сетка;
(?) алюминиевая фольга;
(!) фтористая сетка.
21. Какое устройство позволяет обеспечивать защищенность от разного рода сигналов генерируемых устройствами, которые могут служить источником утечки информации?
(?) приемник-сканер;
(?) телефонный адаптер;
(?) скремблер;
(!) сетевой фильтр;
(?) все вышеперечисленные.
22. Какие основные направления в защите персональных компьютеров от несанкционированного доступа Вы знаете?
(?) недопущение нарушителя к вычислительной среде;
(?) защита вычислительной среды;
(?) использование специальных средств защиты информации ПК от несанкционированного доступа;
(!) все вышеперечисленные;
(?) правильного ответа нет.
23. Какие средства защиты информации в ПК наиболее распространены?
(?) применение различных средств шифрования, не зависящих от контекста информации;

(?) средства защиты от копирования коммерческих программных продуктов;
(?) средства защиты вычислительных ресурсов, использующие парольную идентификацию и ограничивающие доступ несанкционированного пользователя;
(?) средства защита от компьютерных вирусов и создание архивов;
(!) все вышеперечисленные.

24. Какое утверждение неверно?

(?) чтобы уменьшить потери по эксплуатационным причинам, следует иметь архивные копии используемых файлов и систематически обновлять копии изменяемых файлов;
(?) программы-архиваторы позволяют не только сэкономить место на архивных дискетах, но и объединять группы совместно используемых файлов в один архивный файл, что заметно облегчает ведение архивов:
(?) информация на жестком диске может разрушиться только вследствие действия компьютерного вируса или злого умысла вашего недоброжелателя;
(?) единственно надежным способом уберечь информацию от любых разрушительных случайностей является четкая, неукоснительно соблюдаемая система резервного копирования;
(!) одним из основных симптомов, возникновения серьезных дефектов на диске, является замедление работы дисковода.

25. Кто является собственником защищаемой информации?

(?) юридическое лицо, которое по своему усмотрению владеет, пользуется и распоряжается принадлежащей ему информацией
(!) юридическое или физическое лицо, которое по своему усмотрению владеет, пользуется и распоряжается принадлежащей ему информацией
(?) физическое лицо, которое по своему усмотрению владеет, пользуется и распоряжается принадлежащей ему информацией

26. На какие группы делятся информационные ресурсы государства?

(!) информация открытая, информация запатентованная и информация, «закрываемая» ее собственником, владельцем и защищаемая им с помощью отработанных механизмов защиты государственной, коммерческой или другой охраняемой тайны
(?) информация открытая и информация запатентованная
(?) информация запатентованная и информация, «закрываемая» ее собственником, владельцем и защищаемая им с помощью отработанных механизмов защиты государственной, коммерческой или другой охраняемой тайны

27. Что такое запатентованная информация?

(?) на распространение и использование которой не имеется никаких ограничений
(!) охраняется внутригосударственным законодательством или международными соглашениями как объект интеллектуальной собственности;
(?) информация, которая принадлежит одному единственному собственнику

28. К защищаемой информации относят…

(?) секретную информацию и конфиденциальную информацию

(?) личную тайну

(!) все вышеперечисленное

29. Применительно к органам государственной власти и управления под тайной понимается…

(!) то, что скрывается от других, что известно строго определенному кругу людей

(?) секретная переписка

(?) секретные переговоры

30. Какие из ниже перечисленных сведений, согласно Постановлению Правительства РФ от 5 декабря 1991 г. № 35, не могут составлять коммерческую тайну?

(?) учредительные документы и устав предприятия; документы, дающие право заниматься предпринимательской деятельностью; сведения по установленным формам отчетности о финансово-хозяйственной деятельности, необходимые для проверки уплаты налогов; документы о платежеспособности

(?) сведения о численности, заработной плате и условиях труда, о наличии свободных рабочих мест; документы об уплате налогов; сведения о загрязнении окружающей среды, нарушении антимонопольного законодательства, несоблюдении безопасности условий труда, а также других нарушениях законодательства РФ

(!) все вышеперечисленное

4.1.2 Вопросы 8 семестр

1-ое промежуточное тестирование (Т1)

1. Одной из проблем защиты информации является…

1. классификация возможных каналов утечки информации
2. ее разнообразие
3. ее доступность

2. Известно, что информация — это сведения о…

1. предметах, объектах
2. явлениях и процессах, отображаемые в сознании человека или на каком-либо носителе, для последующего их восприятия человеком
3. все вышеперечисленное

3. Назовите категории источников, обладающие и владеющие конфиденциальной информацией или содержащие ее в себе?

1. люди, документы, публикации, технические носители, технические средства обеспечения производственной и трудовой деятельности
2. продукция, промышленные и производственные отходы
3. все вышеперечисленное

4. Как называются процессы обмена информацией, осуществляемые самими специалистами, учеными, производителями, маркетологами и другими путем личного общения при непосредственных контактах или переписки?

1. неформальными
2. формальными
3. глобальными

5. Принято считать, что первичные документы содержат непосредственные результаты…

1. разработок, исследований, учетно-статистической информации и т.п.
2. анализа и обобщения, полученные в результате аналитико-синтетической и логистической обработки исходных данных нескольких первичных документов или сведений о них
3. все выше перечисленное

6. Стремление путем внешне наивных вопросов получить определенные сведения называется …

1. выпытыванием
2. преследованием
3. шантажом

7. Постоянное или выборочное активное и целенаправленное исследование предметов, явлений или людей в естественных условиях или с помощью технических средств с последующим обобщением и анализом данных наблюдения называется…

1. подслушиванием
2. наблюдением
3. преследованием

8. Как могут классифицироваться угрозы?

1. по природе возникновения
2. по ориентации на угрозы персоналу, материальным и финансовым ресурсам и информации, как составным элементам информационной системы
3. все вышеперечисленное

9. К факторам, приводящим к информационным потерям и, как следствие, к различным видам убытков или ущерба можно отнести следующие причины и действия…

1. материальный ущерб, связанный с несчастными случаями, кража и преднамеренная порча материальных средств, аварии и выход из строя аппаратуры, программ и баз данных, убытки, связанные с ошибками накопления, хранения, передачи и использования информации
2. ошибки эксплуатации, концептуальные ошибки и ошибки внедрения, убытки от злонамеренных действий в нематериальной сфере, болтливость и разглашение, убытки социального характера
3. все вышеперечисленное

10. Какие расходы можно отнести к категории дополнительных?

1. поддержка информационных ресурсов и средств удаленного доступа;

2. стоимость ремонтно-восстановительных работ;
3. все вышеперечисленное

11. Какие потери можно отнести к категории эксплуатационных?

1. потеря клиентуры;
2. расходы на анализ и исследование причин и величины ущерба;
3. все вышеперечисленное

12. Различные виды злонамеренных действий в нематериальной сфере (разрушение или изменение данных или программ) могут быть подразделены на два крупных класса…

1. физические и материальные разрушения
2. физический саботаж и информационные инфекции
3. физический саботаж и материальные разрушения

13. Установить информационный обмен между несколькими партнерами — это значит договориться…

1. о технических и юридических передачи данных, к этому следует добавить еще и требования сокращения времени передачи документов, снижение стоимости, улучшение качества информационного обслуживания
2. договориться о технических условиях передачи данных
3. договориться о технических и материальных условиях передачи данных

14. Убытки в системе обмена данными могут иметь…

1. внешние причины
2. внешние и внутренние причины
3. внутренние причины

15. По своему характеру вторжения в линии связи информационных систем по отношению к информационному обмену могут быть…

1. пассивными или активными.
2. частыми или редкими
3. все вышеперечисленное

16. Основными методами, используемыми в защите информации, являются следующие…

1. скрытие, ранжирование, дезинформация
2. дробление, страхование, морально-нравственные, учет, кодирование, шифрование
3. все вышеперечисленное

17. Скрытие — как метод защиты информации является в основе своей реализацией на практике одного из основных организационных принципов защиты информации — …

1. максимального ограничения числа лиц, допускаемых к секретам
2. расчленение информации на части с таким условием, что знание какой-то одной части информации не позволяет восстановить всю картину, всю технологию в целом
3. все вышеперечисленное

18. Средства защиты информации — это …

1. совокупность инженерно-технических, электрических, электронных, оптических и других устройств и приспособлений, приборов и технических систем, а также иных элементов, используемых для решения различных задач по защите информации
2. средства, используемые для предупреждения утечки и обеспечения безопасности защищаемой информации.
3. все вышеперечисленное

19. Что такое СИБ?

1. система информационной безопасности
2. способы информационной боеготовности
3. сумма информационных блоков

20. С позиции системного подхода к защите информации предъявляются определенные требования. Защита информации должна быть:

1. непрерывной, плановой, централизованной, активной
2. надежной, целенаправленной, универсальной, комплексной
3. все вышеперечисленное

21. Какие требования предъявляются к СИБ?

1. четкость определения полномочий и прав пользователей к доступу на определенные виды информации; предоставление пользователю минимальных полномочий, необходимых ему для работы; сведение к минимуму числа общих для нескольких пользователей средств защиты
2. учет случаев и попыток несанкционированного доступа к конфиденциальной информации; обеспечение оценки степени конфиденциальности информации; обеспечение контроля целостности средств защиты и немедленное реагирование на их выход из строя
3. все вышеперечисленное

22. Основными задачами обеспечения безопасности персонала является…

1. охрана личности от любых противоправных посягательств на его жизнь
2. охрана личности от любых противоправных посягательств на его жизнь, материальные ценности и личную информацию.
3. охрана личности и его близких от любых противоправных посягательств на его жизнь и материальные ценности

23. Какие существуют уровни защиты в государстве?

1. социально-политический уровень и материально – технический уровень защиты информации
2. социально-политический, организационно-правовой (стратегический) и тактический уровень защиты информации
3. социально-политический, тактический и материально – технический уровень защиты информации

24. Какие существуют отношения субординации для системы защиты государственной тайны?

1. государственный уровень (высший); отраслевой (средний); предприятие, фирма, акционерное общество и др. (низший).

2. государственный уровень (высший), должностной средний и персональный (низший)
3. государственный уровень (высший), министерский (средний), должностной (низший)

25. Основные положения современной концепции защиты информации можно свести к следующим положениям:

1. защита информации в государстве должна обеспечить информационную безопасность личности, общества и государства
2. защита должна обеспечить охрану информационных ресурсов страны
3. все вышеперечисленное

26. За счет чего организуется защита информационных ресурсов.

1. на основе различных законодательных и других нормативных актов, различных организационных мерах
2. на основе электронной защиты
3. на основе архивных данных

27. Конкретизация стратегических целей защиты информации может состоять в том, чтобы были четко сформулированы цели…

1. обеспечения информационной безопасности личности, общества и государства; надежного режимного информационного обеспечения разработки и реализации стратегических проблем управления государством
2. постановки преград на путях безвозмездного использования информационных ресурсов страны, растаскивания ее интеллектуального потенциала, объектов интеллектуальной собственности
3. все вышеперечисленное

28. Что является основой защиты целостности?

1. является своевременное регулярное копирование ценной информации, помехозащищенное кодирование информации и создание системной избыточности
2. защита от вмешательства посторонних лиц и архивирование информации
3. все вышеперечисленное

29. Комплексная система защиты информации (КСЗИ) — это…

1. использование современных электронных методов защиты системы
2. совокупность сил, средств, методов и мероприятий, используемых во взаимодействии и дополнении друг друга и предназначенных для обеспечения на регулярной основе и на заданном уровне защиты информации на этом объекте.
3. все вышеперечисленное

30. Объектом защиты информации являются …

1. различные категории сведений, имеющихся на данном предприятии, и отнесенные в соответствии с установленными законодательными и другими нормативными актами к составляющим государственную или коммерческую тайну.
2. определенный объект, обладающий какой либо информацией
3. все вышеперечисленное

31. Предметом защиты информации являются…

1. носители информации, на которых зафиксированы, отображены защищаемые сведения: секретные документы; специзделия; материалы; излучения, несущие и отображающие защищаемую информацию
2. персонал
3. все вышеперечисленное

32. Основные методы защиты секретной и конфиденциальной информации, «переносимой» указанными носителями информации:

1. скрытие; дезинформация;
2. кодирование и шифрование, а также организационные и инженерно-технические меры
3. все вышеперечисленное

33. В каком случае система безопасности считается надежной и не требует дополнительных мер?

1. если реальное состояние перекрывает угрозы в полной мере
2. если персонал правильно выполняет свои служебные обязанности
3. если техническое оснащение объекта отвечает современным требованиям

34. Политика безопасности — это…

1. набор норм, правил и практических приемов, которые регулируют управление, защиту и распределение ценной информации в данной организации.
2. это подтверждение того, что предъявленное имя соответствует объекту.
3. это регистрация событий, позволяющая восстановить и доказать факт происшествия этих событий.

35. Сколько классов защищенности установлено в Российской системе безопасности нформационных систем?

1. три
2. семь
3. девять

36. Защита информации или противодействие технической коммерческой разведке в общем случае представляет собой…

1. комплекс мероприятий организационного и технического характера
2. использование электронных средств защиты
3. все вышеперечисленное

2-ое промежуточное тестирование (Т2)

1. Устойчивая защита информации на жестком диске может быть достигнута посредством…

1. шифрования системной информации, пароля и всего содержимого диска
2. системы контроля
3. все вышеперечисленное

2. Какие основные группы шифрования можно условно выделить?

1. подстановка; перестановка; аналитическое преобразование; комбинированное преобразование
2. замена, перестановка, упаковка, монтировка
3. аналитическое преобразование, расстановка, замена, перестановка

3. Какими способами может быть выполнена следующая задача: с одной стороны - разрешать чтение программы для её выполнения, а с другой — запретить операцию чтения для предотвращения несанкционированного копирования?

1. можно разрешить операцию чтения (копирования), но делать скопированные программы неработоспособными (неузнаваемыми);
2. сделать информацию "трудночитаемой" стандартными средствами, но доступной для специальных программных средств
3. все вышеперечисленное

4. Какие средства можно использовать для копирования файлов?

1. программные средства, например, утилиты UnErase и DiskEdit (входящими в состав Norton Utilities) или UnDelet, входящей в состав дистрибутива DOS.
2. стандартные команды Copy, Xcopy, Diskcopy; программные средства PCtools, Norton Commander, Windows; программы непрерывного копирования Backup и Restore.
3. все вышеперечисленное

5. Вирусы условно подразделяются на классы по следующим признакам:

1. по среде обитания; по способу заражения; по возможностям:
2. по среде обитания, по скорости распространения, по названию
3. по способу заражения, по названию

6. Наиболее типичные симптомы, предшествующие возникновению серьезных дефектов на диске — следующие:

1. отсутствие доступа к отдельному файлу или появление в текстовых файлах посторонних символов; замедление работы дисковода;
2. появление при записи и чтении информации звука, напоминающего фырканье насоса; неустойчивость процесса загрузки DOS.
3. все вышеперечисленное

7. Основные угрозы доступности информации:

1. непреднамеренные ошибки пользователей

2. злонамеренное изменение данных

3. хакерская атака

4. отказ программного и аппаратного обеспечения

5. разрушение или повреждение помещений

6. перехват данных

8. Суть компрометации информации:

1. внесение изменений в базу данных, в результате чего пользователь лишается доступа к информации

2. несанкционированный доступ к передаваемой информации по каналам связи и уничтожения содержания передаваемых сообщений
3. внесение несанкционированных изменений в базу данных, в результате чего потребитель вынужден либо отказаться от неё, либо предпринимать 4. дополнительные усилия для выявления изменений и восстановления истинных сведений

9. **Информационная безопасность автоматизированной системы – это состояние автоматизированной системы, при котором она:**
1. с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой – ее наличие и функционирование не создает информационных угроз для элементов самой системы и внешней среды
2. с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой – затраты на её функционирование ниже, чем предполагаемый ущерб от утечки защищаемой информации
3. способна противостоять только информационным угрозам, как внешним так и внутренним
4. способна противостоять только внешним информационным угрозам
10. **Методы повышения достоверности входных данных:**
1. Замена процесса ввода значения процессом выбора значения из предлагаемого множества
2. Отказ от использования данных
3. Проведение комплекса регламентных работ
4. Использование вместо ввода значения его считывание с машиночитаемого носителя
5. Введение избыточности в документ первоисточник
6. Многократный ввод данных и сличение введенных значений
11. **Принципиальное отличие межсетевых экранов (МЭ) от систем обнаружения атак (СОВ):**
1. МЭ были разработаны для активной или пассивной защиты, а СОВ – для активного или пассивного обнаружения
2. МЭ были разработаны для активного или пассивного обнаружения, а СОВ – для активной или пассивной защиты
3. МЭ работают только на сетевом уровне, а СОВ – еще и на физическом
12. **Сервисы безопасности:**
1. идентификация и аутентификация
2. шифрование
3. инверсия паролей

4. контроль целостности
5. регулирование конфликтов
6. экранирование
7. обеспечение безопасного восстановления
8. кэширование записей

13. Под угрозой удаленного администрирования в компьютерной сети понимается угроза:

1. несанкционированного управления удаленным компьютером
2. внедрения агрессивного программного кода в рамках активных объектов Web-страниц
3. перехвата или подмены данных на путях транспортировки
4. вмешательства в личную жизнь
5. поставки неприемлемого содержания

14. Причины возникновения ошибки в данных:

1. Погрешность измерений
2. Ошибка при записи результатов измерений в промежуточный документ
3. Неверная интерпретация данных
4. Ошибки при переносе данных с промежуточного документа в компьютер
5. Использование недопустимых методов анализа данных
6. Неустранимые причины природного характера
7. Преднамеренное искажение данных
8. Ошибки при идентификации объекта или субъекта хозяйственной деятельности

15. К формам защиты информации не относится:

1. аналитическая
2. правовая
3. организационно-техническая
4. страховая

16. Наиболее эффективное средство для защиты от сетевых атак:

1. использование сетевых экранов или «firewall»
2. использование антивирусных программ
3. посещение только «надёжных» Интернет-узлов
4. использование только сертифицированных программ-броузеров при доступе к сети Интернет

17. Информация, составляющая государственную тайну не может иметь гриф:

1. «для служебного пользования»
2. «секретно»

3. «совершенно секретно»
4. «особой важности»

18. Разделы современной криптографии:

1. Симметричные криптосистемы
2. Криптосистемы с открытым ключом
3. Криптосистемы с дублированием защиты
4. **Системы электронной подписи**
5. Управление паролями

19. Документ, определивший важнейшие сервисы безопасности и предложивший метод классификации информационных систем по требованиям безопасности:

1. рекомендации X.800
2. Оранжевая книга
3. Закону «Об информации, информационных технологиях и о защите информации»

20. Утечка информации – это:

1. несанкционированный процесс **переноса** информации от источника к злоумышленнику
2. процесс раскрытия секретной информации
3. процесс уничтожения информации
4. непреднамеренная утрата носителя информации

21. Основные угрозы конфиденциальности информации:

1. маскарад
2. карнавал
3. переадресовка
5. перехват данных
6. блокирование
7. злоупотребления полномочиями

22. Элементы знака охраны авторского права:

1. буквы С в окружности или круглых скобках
2. буквы Р в окружности или круглых скобках
3. наименования (имени) правообладателя
4. наименование охраняемого объекта
5. года первого выпуска программы

23. Защита информации обеспечивается применением антивирусных средств:

1. да
2. нет
3. не всегда

24. Средства защиты объектов файловой системы основаны на:

1. определении прав пользователя на операции с файлами и каталогами
2. задании атрибутов файлов и каталогов, независящих от прав пользователей

25. Вид угрозы действия, направленного на несанкционированное использование информационных ресурсов, не оказывающего при этом влияния на её функционирование:

1. активная
2. пассивная

26. Преднамеренная угроза безопасности информации:

1. кража
2. наводнение
3. повреждение кабеля, по которому идет передача, в связи с погодными условиями
4. ошибка разработчика

27. Концепция системы защиты от информационного оружия не должна включать:

1. средства нанесения контратаки с помощью информационного оружия
2. механизмы защиты пользователей от различных типов и уровней угроз для национальной информационной инфраструктуры
3. признаки, сигнализирующие о возможном нападении
4. процедуры оценки уровня и особенностей атаки против национальной инфраструктуры в целом и отдельных пользователей

28. В соответствии с нормами российского законодательства защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

1. обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации
2. реализацию права на доступ к информации»
3. соблюдение норм международного права в сфере информационной безопасности
4. выявление нарушителей и привлечение их к ответственности
5. соблюдение конфиденциальности информации ограниченного доступа
6. разработку методов и усовершенствование средств информационной безопасности.

4.2 Примерная тематика контрольных и домашних работ

1. Анализ существующих подходов построения СИБ в системе информационной безопасности на типовом предприятии.
2. Анализ существующих подходов определения состава защищаемой информации в системе информационной безопасности на типовом предприятии.
3. Анализ существующих подходов определения степеней конфиденциальности защищаемой информации в системе информационной безопасности на типовом предприятии.
4. Анализ существующих подходов определения ценности защищаемого информационного ресурса в системе информационной безопасности на типовом предприятии.
5. Анализ существующих подходов выявления информационных угроз в системе информационной безопасности на типовом предприятии.
6. Анализ существующих подходов выявления уязвимостей информационных объектов в системе информационной безопасности на типовом предприятии.
7. Анализ существующих подходов определения важнейших объектов защиты в системе информационной безопасности на типовом предприятии.
8. Анализ существующих подходов выявления возможных нарушителей (злоумышленников) в системе информационной безопасности на типовом предприятии.
9. Анализ существующих подходов определения возможных технических каналов утечки информации в системе информационной безопасности на типовом предприятии.

11 Анализ существующих подходов выявления каналов несанкционированного доступа к защищаемой информации в системе информационной безопасности на типовом предприятии.

10. Обоснование потребного подхода к выявлению факторов, влияющих на организацию СИБ построения СИБ на типовом предприятии.
11. Обоснование потребного подхода к стратегии информационной безопасности на типовом предприятии.
12. Обоснование потребного подхода к требуемому уровню защиты информационных ресурсов в системе информационной безопасности на типовом предприятии.
13. Обоснование потребного подхода к определению состава защищаемой информации в системе информационной безопасности на типовом предприятии.
14. Обоснование потребного подхода к определению степеней конфиденциальности защищаемой информации в системе информационной безопасности на типовом предприятии.

15. Обоснование потребного подхода к определению ценности защищаемого информационного ресурса в системе информационной безопасности на типовом предприятии.
16. Обоснование потребного подхода к определению важнейших объектов защиты в системе информационной безопасности на типовом предприятии.
17. Обоснование потребного подхода к определению структурных компонентов в системе информационной безопасности на типовом предприятии.
18. Обоснование потребного подхода к выявлению информационных угроз в системе информационной безопасности на типовом предприятии.
19. Обоснование потребного подхода к выявлению уязвимостей информационных объектов в системе информационной безопасности на типовом предприятии.
20. Обоснование потребного подхода выявления возможных нарушителей (злоумышленников) информации в системе информационной безопасности на типовом предприятии.

4.3. Типовые вопросы, выносимые на зачет

1. Сущность и назначение системы информационной безопасности (СИБ) предприятия.
2. Задачи, возлагаемые на систему информационной безопасности предприятия.
3. Методология защиты информации как теоретический базис построения СИБ предприятия.
4. Методологические основы организации СИБ предприятия.
5. Принципы организации СИБ предприятия.
6. Основные требования, предъявляемые к СИБ предприятия.
7. Содержательная характеристика этапов разработки СИБ предприятия.
8. Основные факторы, влияющие на организацию обеспечения ИБ предприятия.
9. Характер и степень влияния различных факторов на организацию СИБ предприятия.
10. Методика определения состава защищаемой информации на предприятии.
11. Этапы работы по выявлению состава защищаемой информации на

предприятии.

12. Функции руководства предприятия и руководителей подразделений по обеспечению информационной безопасности.

13. Функции экспертной комиссии по защите информации на предприятии.

14. Функции и структура службы информационной безопасности на предприятии.

15. Классификация защищаемой информации по видам тайн и степеням конфиденциальности (секретности) в системе информационной безопасности на предприятии.

16. Нормативное закрепление состава защищаемой информации и структура перечня сведений, относимых к различным видам тайны при реализации СИБ на предприятии.

17. Внедрение перечня защищаемых сведений и порядок внесения в них изменений (дополнений) в СИБ на предприятии.

18. Факторы, определяющие состав носителей с защищаемой информацией в СИБ на предприятии.

19. Методика выявления состава носителей защищаемой информации в СИБ на предприятии.

20. Хранилища носителей с защищаемой информацией в СИБ на предприятии.

21. Особенности помещений для работы с защищаемой информацией как объекты СИБ предприятия.

22. Состав технических средств обработки, передачи, транспортировки и защиты информации, являющихся объектами СИБ предприятия.

23. Факторы, определяющие необходимость защиты периметра и здания предприятия в СИБ предприятия.

24. Персонал предприятия как объект защиты в СИБ.

25. Определение дестабилизирующих воздействий на защищаемую информацию в СИБ предприятия.

26. Выявление способов воздействия на защищаемую информацию в СИБ

предприятия.

27. Оценка ущерба от потенциального дестабилизирующего воздействия на защищаемую информацию в СИБ предприятия.

28. Методика выявления каналов несанкционированного доступа к защищаемой информации в СИБ предприятия.

29. Определение возможных методов несанкционированного доступа к защищаемой информации в СИБ предприятия.

30. Оценка степени опасности применения различных методов НСД в СИБ предприятия.

31. Виды потенциальных последствий несанкционированного доступа в СИБ предприятия.

32. Методика выявления нарушителей (злоумышленников) в СИБ предприятия.

33. Определение возможностей несанкционированного доступа нарушителей (злоумышленников) в СИБ предприятия.

34. Оценка степени уязвимости защищаемой информации в СИБ предприятия.

35. Факторы, влияющие на выбор потребных компонентов СИБ предприятия.

36. Объекты защиты, определяющие потребный состав компонентов СИБ предприятия.

37. Требования, предъявляемые к выбору методов и средств защиты информации в СИБ предприятия

38. Факторы и обстоятельства, влияющие на качество защиты информации в СИБ предприятия.

39. Виды обеспечения функционирования СИБ предприятия.

40. Выбор структуры СИБ в зависимости от объектов защиты, характера и условий функционирования предприятия.

41. Функциональная модель СИБ предприятия.

42. Организационная модель СИБ предприятия.

43. Информационная модель СИБ предприятия.
44. Кибернетическая модель СИБ предприятия.

4.4 Примерная тематика курсовых проектов (работ)

1. Разработка правового обеспечения СИБ на малом (среднем, большом или корпоративном) предприятии.
2. Разработка организационного обеспечения СИБ на малом (среднем, большом или корпоративном) предприятии.
3. Построение программно-аппаратного обеспечения СИБ в коммерческих производственных структурах.
4. Построение инженерно-техническое обеспечение СИБ на малом (среднем, большом или корпоративном) предприятии.
5. Разработка методического обеспечения СИБ на государственном (коммерческом) предприятии.
6. Построение материально-технического обеспечения СИБ на предприятии.
7. Разработка подсистемы физической защиты информационных объектов в СИБ современного предприятия.
8. Построение СИБ для автоматизированных систем обработки информации на предприятии.
9. Построение подсистемы управление СИБ на малом (среднем, большом или корпоративном) предприятии.
10. Разработка подсистемы управление СИБ предприятия в условиях чрезвычайных ситуаций.
11. Разработка и внедрение политики информационной безопасности при реализации СИБ на предприятии.
12. Разработка подсистемы автоматизированного планирование в СИБ на предприятии.
13. Организация и проведение аудита СИБ на малом (среднем, большом или корпоративном) предприятии.
14. Анализ и управление рисками при проектировании СИБ предприятия.
15. Разработка моделей угроз и нарушителей при проектировании СИБ на малом (среднем, большом или корпоративном) предприятии.
16. Разработка моделей оценки эффективности проектирования СИБ на малом (среднем, большом или корпоративном) предприятии.
17. Разработка технологии делового планирования при организации СИБ предпринимательских структур.
18. Определение возможностей несанкционированного доступа к защищаемой информации в СИБ предприятия.

19. Определение основных компонентов СИБ предприятия.
20. Определение условий функционирования СИБ предприятия.
21. Разработка модели СИБ современного предприятия.
22. Организационное построение СИБ типового предприятия.
23. Управление СИБ в условиях чрезвычайных ситуаций на предприятии.
24. Методы и модели оценки эффективности СИБ типового предприятия.

4.5 Типовые вопросы, выносимые на экзамен

1. Сущность и задачи системы информационной безопасности современного предприятия.
2. Принципы организации современной системы информационной безопасности предприятия.
3. Этапы разработки системы информационной безопасности современного предприятия.
4. Сущность и назначение СИБ предприятия.
5. Методологические основы организации СИБ предприятия.
6. Факторы, влияющие на организацию СИБ предприятия.
7. Определение и нормативное закрепление состава защищаемой информации в СИБ предприятия.
8. Определение объектов защиты при организации СИБ предприятия.
9. Выявления состава носителей защищаемой информации в СИБ предприятия.
10. Выявление и оценка дестабилизирующего воздействия на защищаемую информацию в СИБ предприятия.
11. Определение потенциальных каналов и методов несанкционированного доступа к информации при организации СИБ.
12. Определение возможностей несанкционированного доступа к защищаемой информации в СИБ предприятия.
13. Определение потребных компонентов СИБ предприятия.
14. Определение условий функционирования СИБ современного предприятия.

15. Разработка структурно-функциональной модели СИБ предприятия.
16. Содержание организации функционирования СИБ предприятия.
17. Характеристика основных стадий создания (проектирования) СИБ предприятия.
18. Основы проектирования СИБ предприятия: характеристика предпроектного обследования объектов защиты.
19. Назначение и структура технико-экономического обоснования на проектирование СИБ предприятия.
20. Назначение и структура технического задания на проектирование СИБ предприятия.
21. Основы проектирования СИБ предприятия: характеристика технического проекта.
22. Основы проектирования СИБ предприятия: характеристика рабочего проекта.
23. Основы проектирования СИБ предприятия: характеристика этапа апробации и ввода в эксплуатацию.
24. Кадровое обеспечение функционирования СИБ предприятия: определение кадрового состава.
25. Кадровое обеспечение функционирования СИБ предприятия: распределение функций по защите информации между должностными лицами.
26. Кадровое обеспечение функционирования СИБ предприятия: разработка нормативных документов, регламентирующих деятельность персонала по защите информации.
27. Потребный состав материально-технического обеспечения СИБ предприятия.
28. Зависимость материально-технического обеспечения СИБ предприятия от структуры предприятия.
29. Нормативно-методическое обеспечение СИБ предприятия: вопросы, требующие документационного закрепления.

30. Состав потребных нормативно-методических документов по функционированию СИБ предприятия.
31. Порядок разработки и внедрения документов по нормативно-методическому обеспечению СИБ предприятия
32. Понятие и цели управления СИБ предприятия.
33. Сущность процессов и принципы управления СИБ предприятия.
34. Структура и содержание общей технологии управления СИБ предприятия.
35. Понятие и задачи планирования функционирования СИБ современного предприятия.
36. Способы и стадии планирования СИБ предприятия.
37. Структура и общее содержание планов функционирования СИБ предприятия.
38. Методы сбора, обработки и изучения информации для планирования работы СИБ предприятия.
39. Организация выполнения планов СИБ современного предприятия.
40. Понятие и виды контроля функционирования СИБ предприятия.
41. Цель, методы и особенности проведения контрольных мероприятий в СИБ предприятия.
42. Анализ и использование результатов проведения контрольных мероприятий в СИБ предприятия.
43. Технология принятия решений в СИБ предприятия в условиях чрезвычайной ситуации.
44. Факторы, влияющие на принятие решений в СИБ при условиях чрезвычайной ситуации на предприятии.
45. Подготовка мероприятий в СИБ предприятия на случай возникновения чрезвычайных ситуаций.
46. Классификация существующих подходов по оценке эффективности СИБ предприятия и их сравнительный анализ.
47. Характеристика вероятностного подхода по оценке эффективности

СИБ предприятия.

48. Характеристика оценочного подхода по оценке эффективности СИБ предприятия.
49. Содержание и особенности экспертной оценки эффективности СИБ предприятия.
50. Классификационная структура методов и моделей оценки эффективности СИБ предприятия.
51. Системы показателей защищенности (эффективности) СИБ предприятия.
52. Аналитические модели определения базовых и обобщенных показателей уязвимости в СИБ предприятия.
53. Метод оценки эффективности СИБ предприятия: построение диаграмм безопасности.
54. Метод оценки эффективности СИБ предприятия: анализ информационных рисков.
55. Метод оценки эффективности СИБ предприятия: на основе структурных вопросников.
56. Характеристика компьютерного моделирования функциональной оценки эффективности СИБ на предприятии (модель Домарева).
57. Области применения (анализ приемлемости) различных методов и моделей для функциональной оценки эффективности СИБ предприятия.
58. Общая характеристика методов экономической оценки эффективности СИБ предприятия.
59. Характеристика методики оценки затрат (совокупной стоимости владения) в СИБ предприятия.
60. Характеристика методики обоснования возврата инвестиций в СИБ предприятия.

Приложение 2

ИНСТИТУТ ТЕХНИКИ И ЦИФРОВЫХ ТЕХНОЛОГИЙ

ФАКУЛЬТЕТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

«КОМПЛЕКСНОЕ ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ ОБЪЕКТА ИНФОРМАТИЗАЦИИ (ПРЕДПРИЯТИЯ)»

(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: изучение и закрепление базовых знаний, умений и навыков по организации и реализации современных технологий защиты информации на предприятиях (организациях и учреждений) с различными формами собственности с учетом современных требований в области теории и практики по обеспечению информационной безопасности на основе комплексного подхода.

В процессе обучения студент приобретает и совершенствует следующие компетенции.

Задачи дисциплины:

- раскрытие сущности, целей и задач обеспечения информационной безопасности на предприятии;
- определение принципов и этапов разработки современных систем информационной безопасности предприятия;
- освоение технологии установления состава защищаемой информации и выявления объектов защиты;
- выявление актуальных информационных угроз и опасных нарушителей (злоумышленников);
- овладение методами оценки уязвимости защищаемой информации;
- определение параметров и структуры потребных систем информационной безопасности современного предприятия;
- установление состава целесообразных мероприятий (технологий) по обеспечению по обеспечению информационной безопасности различных предприятий;
- раскрытие структуры и методов управления информационной безопасностью;
- определение показателей эффективности системы информационной безопасности и методики ее оценки.

2. Указания по проведению практических занятий

Практическое занятие №1
Тема: Введение в дисциплину
Учебные вопросы

1. Значение и место курса в подготовке кадров в области «Информационная безопасность» по направлению «Бакалавр» с профилем "Организация и технология защиты информации".
2. Структура курса.
3. Формы проведения практических занятий.
4. Формы проверки знаний.
5. Самостоятельная работа студентов.
6. Знания и умения студентов, которые должны быть получены в результате изучения курса.

Продолжительность занятия – 2 ч.

Практическое занятие №2
Тема: Сущность и задачи системы обеспечения информационной безопасности предприятия

Учебные вопросы

1. Понятие и сущность системы обеспечения информационной безопасности предприятия (СИБ).
2. Назначение и задачи СИБ предприятия.
3. СИБ предприятия как средство выражения концептуальных основ теории и практики современной защиты информации.
4. Методология защиты информации как теоретический базис построения СИБ предприятия.

Продолжительность занятия – 2 ч.

Практическое занятие №3
Тема: Принципы организации и этапы разработки системы информационной безопасности

Учебные вопросы

1. Методологические основы организации СИБ современного предприятия как сложная человеко-машинная система.
2. Принципы организации СИБ предприятия.
3. Основные требования, предъявляемые к обеспечению информационной безопасности.
4. Содержательная характеристика этапов разработки (проектирования) современных систем обеспечения информационной безопасности предприятия.

Продолжительность занятия – 2 ч.

Практическое занятие №4
Тема: Факторы, влияющие на организацию обеспечения информационной безопасности современного предприятия

Учебные вопросы

1. Основные факторы, влияющие на организацию обеспечения информационную безопасность предприятия:

1.1. организационно-правовая форма и характер основной деятельности предприятия;

1.2. состав, объем и степень конфиденциальности защищаемой информации;

1.3. структура и территориальное расположение предприятия;

1.4. режим функционирования предприятия;

1.5. конструктивные особенности предприятия;

1.6. количественные и качественные параметры ресурс обеспечения;

1.7. степень автоматизации основных процедур обработки защищаемой информации.

2. Характер и степень влияния различных факторов на организацию обеспечения информационную безопасность.

Продолжительность занятия – 2 ч.

Практическое занятие №5
Тема: Определение и нормативное закрепление состава защищаемой информации

Учебные вопросы

1. Методика определения состава защищаемой информации.
2. Этапы работы по выявлению состава защищаемой информации.
3. Функции руководства предприятия и подразделений предприятия, экспертной комиссии, службы защиты информации.
4. Классификация информации по видам тайны и степеням конфиденциальности.
5. Нормативное закрепление состава защищаемой информации; структура перечней сведений, относимых к различным видам тайны.
6. Порядок внедрения перечней, внесения в них изменений и дополнений.

Продолжительность занятия – 2 ч.

Практическое занятие №6
Тема: Определение объектов информационной безопасности

Учебные вопросы

1. Факторы, определяющие состав носителей информации.
2. Методика выявления состава носителей защищаемой информации.
3. Хранилища носителей информации на предприятии как объекты защиты. Особенности помещений (защищенных и выделенных) для работы с закрытой информацией как объекты защиты.
4. Состав технических средств обработки, передачи, транспортировки и защиты информации, являющихся объектами защиты. Факторы, определяющие необходимость защиты периметра и здания предприятия.
5. Специфика персонала предприятия как объекта защиты.

Продолжительность занятия – 2 ч.

Практическое занятие №7
Тема: Выявление и оценка источников, способов и результатов дестабилизирующего воздействия на информацию
Учебные вопросы

1. Определение источников дестабилизирующего воздействия на информацию и видов их воздействия.
2. Методика выявления способов воздействия на информацию.
3. Определение причин, обстоятельств и условий дестабилизирующего воздействия на информацию.
4. Оценка ущерба от потенциального дестабилизирующего воздействия на информацию.

Продолжительность занятия – 2 ч.

Практическое занятие №8
Тема: Определение потенциальных каналов и методов несанкционированного доступа к информации

Учебные вопросы

1. Соотношение между каналами несанкционированного доступа (НСД) и источниками воздействия на защищаемую информацию на предприятии.
2. Определение возможных методов несанкционированного доступа к защищаемой информации.
3. Методика выявления каналов несанкционированного доступа к информации.
4. Оценка степени опасности реализации различных методов НСД.

Продолжительность занятия – 2 ч.

Практическое занятие №9
Тема: Определение возможностей несанкционированного доступа к информации

Учебные вопросы

1. Методика выявления нарушителей (незаконных пользователей).
2. Определение направлений и возможностей доступа нарушителей к защищаемой информации.
3. Оценка степени опасности применения различных методов НСД.
4. Оценка степени уязвимости информации в результате действий нарушителей различных категорий.
5. Анализ потенциальных последствий реализации несанкционированного доступа.

Продолжительность занятия – 4 ч.

Практическое занятие №10
Тема: Определение потребных компонентов целесообразной системы информационной безопасности

Учебные вопросы

1. Факторы, влияющие на выбор компонентов КСЗИ.
2. Объекты защиты как основной фактор, определяющий потребный состав компонентов СИБ предприятия.
3. Основные требования, предъявляемые к выбору методов и средств защиты, зависимость их от структуры предприятия, защищаемых элементов объектов, условий функционирования СИБ.

Продолжительность занятия – 4 ч.

Практическое занятие №11
Тема: Определение условий функционирования системы информационной безопасности

Учебные вопросы

1. Обеспечение полноты составляющих защиты информации на предприятии.

2. Учет всех факторов и обстоятельств, оказывающих влияние на качество обеспечение информационной безопасности.
3. Обеспечение безопасности всей совокупности подлежащей защите информации: во всех компонентах ее сбора, хранения, передачи и использования; во все время и при всех режимах функционирования систем обработки информации на предприятии.

Продолжительность занятия – 4 ч.

Практическое занятие №12
Тема: Разработка моделей системы информационной безопасности предприятия

Учебные вопросы

1. Понятие модели объекта информационной безопасности, основные виды моделей и их характеристика.
2. Модель как инструмент количественного и качественного анализа функционирования СИБ предприятия. Значение моделирования отдельных процессов функционирования СИБ.
3. Выбор различных функциональных структуры СИБ, зависимость их от объектов информационной защиты, характера и условий функционирования предприятия: структурно-функциональная модель СИБ; организационная модель СИБ; информационная модель СИБ.

Продолжительность занятия – 4 ч.

Практическое занятие №13
Тема: Технологическое построение системы информационной безопасности

Учебные вопросы

1. Общее содержание работ по организации системы информационной безопасности (состав и характеристика стадий и этапов построения СИБ на предприятии).

2. Привлекаемые силы и средства проектирования потребной СИБ для предприятия.
3. Виды проектирования СИБ: индивидуальное, типовое и смешанное.

Продолжительность занятия – 1 ч.

Практическое занятие №14
Тема: Организационно - кадровое обеспечение функционирование системы информационной безопасности

Учебные вопросы

1. Определение состава кадрового обеспечения функционирования СИБ.
2. Распределение функций по защите информации между руководством предприятия, службой защиты информации, специальными комиссиями и пользователями защищаемой информации, обеспечение взаимодействия между ними.
3. Разработка нормативных документов, регламентирующих деятельность персонала по защите информации.
4. Подбор и обучение персонала.

Продолжительность занятия – 1 ч.

Практическое занятие №15
Тема: Материально-техническое обеспечение системы информационной безопасности

Учебные вопросы

1. Значение материально-технического обеспечения (МТО) функционирования СИБ на предприятии. Решаемые задачи МТО СИБ.
2. Определение сил и средств материально-технического обеспечения СИБ.

3. Организация материально-технического обеспечения СИБ на предприятии.

Продолжительность занятия – 1 ч.

Практическое занятие №16
Тема: Нормативно-методическое обеспечение системы информационной безопасности

Учебные вопросы

1. Значение нормативно-методического обеспечения функционирования СЗИ предприятия.
2. Перечень вопросов по функционированию системы защиты информации на предприятии, требующих документационного закрепления.
3. Состав нормативно-методических документов по обеспечению функционирования СЗИ, их назначение, структура и содержание.
4. Порядок разработки и внедрения потребных документов в СИБ.

Продолжительность занятия – 1 ч.

Практическое занятие №17
Тема: Назначение, структура и содержание управления системой информационной безопасности

Учебные вопросы

1. Понятие, цели, функции и задачи управления СИБ предприятия.
2. Сущность и содержание процессов управления СИБ.
3. Принципы управления СИБ. Основные стили (вид и формы) управления СИБ.
4. Структура и содержание общей технологии управления СИБ.
5. Привлекаемые силы и средства управления СИБ современного предприятия.

Продолжительность занятия – 1 ч.

Практическое занятие №18
Тема: Планирования функционирования системы информационной безопасности

Учебные вопросы

1. Понятие и задачи планирования функционирования СИБ.
2. Способы и стадии планирования.
3. Факторы, влияющие на выбор принципов и способов планирования.
4. Структура и общее содержание планов организации и функционирования СИБ.
5. Методы сбора, обработки и изучения информации, необходимой для планирования.
6. Организация выполнения планов функционирования СИБ предприятия.

Продолжительность занятия – 1 ч.

Практическое занятие №19
Тема: Сущность и содержание контроля функционирования системы информационной безопасности

Учебные вопросы

1. Понятие и цель проведения контрольных мероприятий в СИБ.
2. Виды и методы контроля функционирования СИБ.
3. Особенности проведения контроля функционирования СИБ.
4. Анализ и использование результатов проведения контрольных мероприятий в СИБ предприятия.

Продолжительность занятия – 1 ч.

Практическое занятие №20
Тема: Управление системой информационной безопасности предприятия в условиях чрезвычайных ситуаций

Учебные вопросы

1. Понятие и основные виды чрезвычайных ситуаций на современном предприятии.
2. Технология принятия решений по обеспечению информационной безопасности в условиях чрезвычайной ситуации.
3. Факторы, влияющие на принятие решений в СИБ в условиях чрезвычайной ситуации.
4. Подготовка мероприятий по обеспечению ИБ на случай возникновения чрезвычайных ситуаций.

Продолжительность занятия – 1 ч.

Практическое занятие №21
Тема: Общая характеристика подходов к оценке эффективности систем защиты информации

Учебные вопросы

1. Классификация подходов к оценке эффективности систем зашиты информации.

2. Вероятностный подход:

структуризация предметной области оценки;

анализ вероятности реализации угроз безопасности;

расчетные соотношения.

3. Оценочный подход на основе формирования требований к защищенности объекта:

классы защищенности и их характеристика;

контрольно-испытательные процедуры определения соответствия защиты установленным требованиям.

4. Содержание и особенности экспертной оценки эффективности защиты:

выбор системы измерений (вербальные и вербально-числовые шкалы);

организация процедуры экспертного оценивания (подбор экспертов, составление вопросников, обработка результатов).

5. Сравнительный анализ подходов.

Продолжительность занятия – 1 ч.

Практическое занятие №22
Тема: Методы и модели оценки эффективности системы информационной безопасности предприятия

Учебные вопросы

1. Классификационная структура методов и моделей оценки.
2. Базовые понятия и определения, используемые в моделях.
3. Системы показателей защищенности (эффективности).
4. Метод оценки уровня безопасности и аналитические модели определения базовых и обобщенных показателей уязвимости.
5. Метод анализа риска
6. Метод оценки на основе структурных вопросников.
7. Области применения и анализ приемлемости различных методов и моделей для решения задачи оценки эффективности СИБ

Продолжительность занятия – 1 ч.

Практическое занятие №23
Тема: Компьютерное моделирование функциональной оценки эффективности системы информационной безопасности

Учебные вопросы

1. Особенности компьютерного моделирования функциональной (технической) оценки эффективности СИБ.
2. Показатели и возможные критерии компьютерной оценки эффективности функционирования СИБ.
3. Возможные методы и виды компьютерных моделей оценки эффективности СИБ.
4. Решаемые задачи и основные структурные компоненты компьютерной модели Домарева.
5. Математический метод реализации модели Домарева.
6. Исходные и выходные данные модели Домарева.

7. Порядок применения компьютерной модели Домарева для оценки эффективности отдельных подсистем и всей СИБ на предприятии.

Продолжительность занятия – 1 ч.

Практическое занятие №24
Тема: Экономическая оценка эффективности СИБ

Учебные вопросы

1. Общая характеристика существующих подходов экономической оценки эффективности системы информационной безопасности.
2. Существующие методы (двухфакторный и трехфакторный) оценки информационных рисков в СИБ.
3. Особенности применения метода совокупной стоимости владения (определения затрат) СИБ.
4. Основы обоснования возврата инвестиций (оценка доходной части) для СИБ.

Продолжительность занятия – 1 ч.

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. Методология защиты информации как теоретический базис построения СИБ предприятия. Методологические основы организации СИБ предприятия.
2. Принципы организации СИБ предприятия. Основные требования, предъявляемые к СИБ предприятия.
3. Содержательная характеристика этапов разработки СИБ предприятия.

Основные факторы, влияющие на организацию обеспечения ИБ предприятия.

4. Характер и степень влияния различных факторов на организацию СИБ предприятия.
5. Методика определения состава защищаемой информации на предприятии.
6. Этапы работы по выявлению состава защищаемой информации на предприятии.
7. Функции руководства предприятия и руководителей подразделений по обеспечению информационной безопасности.
8. Функции экспертной комиссии по защите информации на предприятии.
9. Функции и структура службы информационной безопасности на предприятии.
10. Классификация защищаемой информации по видам тайн и степеням конфиденциальности (секретности) в системе информационной безопасности на предприятии.
11. Нормативное закрепление состава защищаемой информации и структура перечня сведений, относимых к различным видам тайны при реализации СИБ на предприятии.
12. Внедрение перечня защищаемых сведений и порядок внесения в них изменений (дополнений) в СИБ на предприятии.
13. Факторы, определяющие состав носителей с защищаемой информацией в СИБ на предприятии.
14. Методика выявления состава носителей защищаемой информации в СИБ на предприятии.
15. Хранилища носителей с защищаемой информацией в СИБ на предприятии.
16. Особенности помещений для работы с защищаемой информацией как объекты СИБ предприятия.
17. Состав технических средств обработки, передачи, транспортировки и защиты информации, являющихся объектами СИБ предприятия.
18. Факторы, определяющие необходимость защиты периметра и здания предприятия в СИБ предприятия.
19. Персонал предприятия как объект защиты в СИБ.
20. Определение дестабилизирующих воздействий на защищаемую информацию в СИБ предприятия.
21. Выявление способов воздействия на защищаемую информацию в СИБ предприятия.
22. Оценка ущерба от потенциального дестабилизирующего воздействия на защищаемую информацию в СИБ предприятия.
23. Методика выявления каналов несанкционированного доступа к защищаемой информации в СИБ предприятия.
24. Определение возможных методов несанкционированного доступа к защищаемой информации в СИБ предприятия.
25. Оценка степени опасности применения различных методов НСД в СИБ

предприятия.

26. Виды потенциальных последствий несанкционированного доступа в СИБ предприятия.
27. Методика выявления нарушителей (злоумышленников) в СИБ предприятия.
28. Определение возможностей несанкционированного доступа нарушителей (злоумышленников) в СИБ предприятия.
29. Оценка степени уязвимости защищаемой информации в СИБ предприятия.
30. Факторы, влияющие на выбор потребных компонентов СИБ предприятия.
31. Объекты защиты, определяющие потребный состав компонентов СИБ предприятия.
32. Требования, предъявляемые к выбору методов и средств защиты информации в СИБ предприятия
33. Факторы и обстоятельства, влияющие на качество защиты информации в СИБ предприятия.
34. Виды обеспечения функционирования СИБ предприятия.
35. Выбор структуры СИБ в зависимости от объектов защиты, характера и условий функционирования предприятия.
36. Функциональная модель СИБ предприятия.
37. Организационная модель СИБ предприятия.
38. Информационная модель СИБ предприятия.
39. Кибернетическая модель СИБ предприятия.

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

Цель самостоятельной работы: подготовить студентов к самостоятельному научному творчеству.

Задачи самостоятельной работы:

1) расширить представление в области информационной безопасности предприятия;

2) привить навыки самостоятельного решения задач в области организации защиты информационной безопасности ан предприятии.

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	**200**
Вопросы, выносимые на самостоятельное изучение	110
Подготовка к практическим занятиям	30
Подготовка к лабораторным занятиям	-
Подготовка докладов	30
Выполнение практических заданий	30

Вопросы, выносимые на самостоятельное изучение:
для очной формы обучения:

1. Предмет комплексной СЗИ в организации.
2. Методы комплексной СЗИ в организации.
3. Характеристика угроз безопасности коммерческой организации.
4. Организационные аспекты осуществления мониторинга безопасности коммерческой организации.
5. Деятельность органов государственной власти и управления в области защиты государственных секретов.
6. Концептуальные основы установления режима коммерческой тайны в организации.
7. Управление системой обеспечения безопасности организации.
8. Факторы, влияющие на степень охраны конфиденциальной информации.
9. Понятие и содержание мер по установлению режима коммерческой тайны.
10. Понятие характеристики нарушений режима конфиденциальности информации.
11. Характеристика обстоятельств организационно-управленческого характера.
12. Нравственно-психологические черты лиц, нарушающих режим коммерческой тайны.
13. Субъекты профилактики правонарушений в сфере обращения КЗИ.
14. Система мер по предупреждению правонарушений в сфере обращения КЗИ.
15. Аналитическая работа в сфере обращения КЗИ.

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	110	Изучение открытых источников
2.	Подготовка к практическим занятиям	30	Изучение открытых источников при подготовке доклада на выбранную тему.
3.	Подготовка к лабораторным занятиям	-	Изучение открытых источников
4.	Тематика докладов	30	см. примерные темы докладов
5.	Выполнение практических заданий	30	

Примерные темы докладов

1. Основные направления деятельности министерств и ведомств по защите государственных секретов.
2. Деятельность администрации предприятий и общественных организаций по обеспечению режима секретности.
3. Оптимальный выбор организационной структуры безопасности коммерческой организации.
4. Концептуальные аспекты установления категорий сведений, составляющих коммерческую тайну.
5. Основные направления деятельности организаций по установлению режима коммерческой тайны.
6. Сущность разрешительной системы доступа лиц к коммерческой тайне.
7. Классификация возможных каналов утечки информации и их характеристика.
8. Понятие и классификация причин нарушения режима конфиденциальности информации.
9. Проблема изучения личности нарушителя режима конфиденциальности информации.
10. Социально-демографические признаки лиц, нарушающих режим конфиденциальности информации.
11. Понятие, принципы и система предупреждения правонарушений в сфере обращения КЗИ.
12. Меры предупреждения обстоятельств организационно-управленческого характера.
13. Предупредительные меры воспитательного характера.
14. Меры правового характера.
15. Сущность и содержание контроля в сфере обращения КЗИ.
16. Характеристика систем контроля на предприятиях.

5. Указания по проведению контрольных работ для студентов факультета заочного обучения

Не предусмотрено учебным планом.

6. Перечень основной и дополнительной учебной литературы

Основная литература:

1. Грибунин В.Г. Комплексная система защиты информации на предприятии. Учебное пособие – М.: «Академия», 2009.
2. Гришина Н.В. Организация комплексной защиты информации. – М.: Гелиос АРВ, 2007.
3. Северин В.А. Комплексная защита информации на предприятии. Учебник для вузов. – М.: «Городец», 2008.

Дополнительная литература:

1. Бурков В.Н., Е.В.Грацианский, С.И.Длобко, А.В.Щепкин. Модели и механизмы управления безопасностью. М.:СИНТЕГ, 2001.
2. Гришина Н.В., Морозова Е.В., Хмелевская Н.В. Современные модели и методы оценки защищенности информационно-вычислительных систем // Безопасность информационных технологий, 2002, №3.
3. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. К.: ООО "ТИД "СД", 2001.
4. Завгородний В.И. Комплексная защита информации в компьютерных системах. М., 2001.
5. Игнатьева А.В., Максимцов М.М. Исследование систем управления. М.: ЮНИТИ-ДАНА, 2000.
6. Морозова Е.В. К определению степени защищенности локальной информационно-вычислительной сети // Мир безопасности, №7-8, 2000.
7. Прангишвили И.В. Системный подход и общесистемные закономерности. М..СИНТЕГ, 2000.
8. Проблемы управления информационной безопасностью: Сборник трудов института

системного анализа Российской академии наук / Под ред. д.т.н., проф. Д.С. Черешкина.- М.: Едиториал УРСС, 2002.

9. Семкин С.Н., Семкин А.Н. Основы безопасности объектов обработки информации. - Орел, 2000.
10. Спиркин Г.Н. Юшков Е. С. Харьков С А. Концептуальные направления защиты конфиденциальной информации. Сборник трудов научно-практической конференции "Информационная безопасность". -Таганрог.: Изд-во ТРТУ, 2001. с.2
11. Устинов Г.Н. Основы информационной безопасности систем и сетей передачи данных. М.: СИНТЕГ, 2000.
12. ХаляпинД.Б. Вас подслушивают? Защищайтесь! М.: "Мир безопасности", 2001.
13. Ярочкин В.И. Информационная безопасность. М.: Международные отношения 2003.

Электронные книги:
Электронные ресурсы библиотеки МГОТУ

1. Портал с электронно-методическими комплексами (do.kimes).
2. Универсальная библиотека онлайн (www.biblioclub.ru).
3. Polpred.com www.polpred.com.
4. Единое окно доступа (www.window.edu.ru)/
5. Издательский дом «Гребенников» (http://grebennikon.ru/).

Интернет-ресурсы:

1. **minfin.ru** - официальный сайт Министерства финансов Российской Федерации.
2. **gov.ru** - сервер органов государственной власти Российской Федерации.
3. **Anti-Malware** (информационно-аналитический сайт по ИБ, основная тема - антивирусы и их исследования).
4. **AuditNet** (все об аудите ИТ и ИБ).
5. **CCCure** (обучение по ИБ, сертификация, тестирование, аналитика, лучшие практики, документы).

6. **CERT** (информация об уязвимостях, аналитика, исследования, лучшие практики, проведение расследований).
7. **Datum** (сайт Ассоциации защиты прав операторов и субъектов персональных данных).
8. **Information Security Forum** (лучшие практики, исследования, отчеты, методологии).
9. **ISO27000.ru** (портал по ИБ, аналитика, информация по законодательству и стандартам, блоги, каталоги ресурсов и ПО).
10. **NIST -** Национальный институт стандартов и технологий США (лучшие практики, публикации на тему ИБ, материалы исследований).
11. **SANS** (лучшие практики, статьи, исследования, информация об угрозах и уязвимостях).
12. **Secunia** (информация об уязвимостях).

8. Перечень информационных технологий

Перечень программного обеспечения: *MSOffice*

Информационные справочные системы:

1. Ресурсы информационно-образовательной среды «МГОТУ»
2. Рабочая программа и методическое обеспечение по дисциплине «Комплексное обеспечение защиты информации объекта информатизации (предприятия)».