Частное образовательное учреждение высшего образования

«ИНСТИТУТ БИЗНЕСА И ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ»

УТВРЖДАЮ
Ректор Института бизнеса и инновационных технологий

Одобрено
решением Ученого совета
от «29» июля 2023г.
протокол № 2

А.И. Садыкова

«29» июля 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Информационная безопасность

Специальность: **38.05.01 Экономическая безопасность**

Специализация: **Экономическая безопасность хозяйствующих субъектов**

Квалификация: **Экономист**

Вологда
2023

Рабочая программа дисциплины составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по специальности 38.05.01 Экономическая безопасность, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 14.04.2021 № 293, профессионального стандарта 08.043 ЭКОНОМИСТ ПРЕДПРИЯТИЯ, зарегистрированого в Министерстве юстиции РФ 2021.04.29 №63289.

Оглавление

1. Организационно-методический раздел. Аннотация

Целью освоения дисциплины «Информационная безопасность» является формирований у обучающегося профессиональных компетенций в области обеспечения безопасности информационных систем с учетом установленных нормативных правовых актов в области защиты государственной тайны и информационной безопасности.

Освоение дисциплины способствует подготовке выпускника к решению следующих типов задач профессиональной деятельности: расчетно-экономический, информационно-аналитический, а именно:

– защита частной, государственной, муниципальной и иных форм собственности;

– проведение работ по описанию информационного обеспечения и реализации бизнес-процессов предприятия заказчика;

– освоения базовых методов организации информационной безопасности;

– организация методического, организационно-правового и технического обеспечения информационной безопасности;

– разработка и реализация стратегий, моделей и систем предотвращения несанкционированного доступа в информационную систему организаций и предприятий, защиты государственной тайны, соблюдения режима секретности.

Дисциплина «Информационная безопасность» относится к части учебного плана, формируемой участниками образовательных отношений и является дисциплиной по выбору.

Изучение дисциплины базируется на знаниях и умениях, полученных при изучении дисциплин и прохождении практик: Экономическая безопасность, Практика по профилю профессиональной деятельности.

Освоение дисциплины необходимо как предшествующее при изучении следующих дисциплин и прохождении практик: Проекты и проектная деятельность, Бухгалтерские информационные системы, выполнение выпускной квалификационной работы.

2. Перечень планируемых результатов обучения

Результаты освоения ООП: код и формулировка компетенции (в соответствии с учебным планом) или ее части	Код и формулировка индикатора достижения компетенций	Планируемые результаты обучения по дисциплине
ПК-2 Способен проводить анализ возможных экономических рисков и давать им оценку, составлять и обосновывать прогнозы динамики развития основных угроз экономической безопасности	ПК-2.2 Проводит комплексный анализ угроз экономической безопасности при планировании и осуществлении инновационных проектов	**Знает:** -основные принципы обеспечения безопасности информационной системы -основные угрозы информационной безопасности и их классификацию -сущности информационной безопасности и защиты информации, их места в системе национальной безопасности; нормативных правовых актов в области защиты государственной тайны и информационной безопасности; режимы секретности. **Умеет:** -применять нормативные правовые акты в области защиты информации и учитывать их при создании систем экономической безопасности хозяйствующих субъектов -разрабатывать и применять нормативно-методические материалы по регламентации процессов обработки, хранения и защиты конфиденциальных документов с учетом нормативных правовых актов в области защиты государственной тайны и информационной безопасности с учетом соблюдения необходимого режима секретности -строить модель актуальных угроз на основе предоставленных сведениях и процессах информационной системы организации.
ПК-5 Способен проводить оценку и интерпретацию полученных, в ходе экономического обоснования финансовых результатов	ПК-5.2 Разрабатывает аналитические материалы (отчеты) о финансово-хозяйственной деятельности по результатам оценки финансовых показателей	**Знает:** -автоматизированные методы формирования финансовых показателей организации с точки зрения информационной безопасности. **Умеет:** -подготавливать и анализировать отчеты о финансово-хозяйственной деятельности организации с точки зрения

		информационной безопасности.

3. Примерный тематический план дисциплины

Очная форма обучения - 9 семестр

Вид занятия	Часов по учебному плану
Контактная работа с преподавателем:	44
-занятия лекционного типа, в том числе:	16
практическая подготовка	0
-занятия семинарского типа:	
-семинарские/практические, в том числе:	0
практическая подготовка	0
-лабораторные, в том числе:	26
практическая подготовка	0
-консультации, в том числе по курсовой работе (проекту)	2
Самостоятельная работа:	64
в т.ч. курсовая работа (проект)	
Промежуточная аттестация:	
зачет	
Общая трудоемкость	108

Заочная форма обучения - 6 курс

Вид занятия	Часов по учебному плану
Контактная работа с преподавателем:	16
-занятия лекционного типа, в том числе:	6
практическая подготовка	0
-занятия семинарского типа:	
-семинарские/практические, в том числе:	0
практическая подготовка	0
-лабораторные, в том числе:	6
практическая подготовка	0
-консультации, в том числе по курсовой работе (проекту)	4
Самостоятельная работа:	88
в т.ч. курсовая работа (проект)	

контрольная работа	+
Промежуточная аттестация:	
зачет	4
Общая трудоемкость	108

Очная форма обучения

		Количество часов по видам учебной работы					
				контактная работа с преподавателем			
					занятия семинарского типа:		
№	Раздел / Тема дисциплины	ВСЕГО	СР	занятия лекционного типа	семи-нарские/ практи-ческие	лабора-торные	консультации, в том числе по курсовой работе (проекту)
1	Информационная безопасность. Основные положения, понятия и определения	12	8	2	0	2	
2	Методология обеспечения информационной безопасности деятельности общества.	16	10	2	0	4	
3	Организационно-правовое обеспечение информационной безопасности	26	16	4	0	6	
4	Модели и системы обеспечения информационной безопасности деятельности организаций	28	16	4	0	8	
5	Техническое и методическое обеспечение информационной безопасности	24	14	4	0	6	

Подготовка и защита курсовой работы (проекта)						
Промежуточная аттестация (зачет)	0	0				0
ИТОГО	**108**	**64**	**16**	**0**	**26**	**2**
В том числе: практическая подготовка	0		0	0	0	

Заочная форма обучения

		Количество часов по видам учебной работы					
				контактная работа с преподавателем			
					занятия семинарского типа:		
№	Раздел / Тема дисциплины	ВСЕГО	СР	занятия лекционного типа	семи-нарские/ практи-ческие	лабора-торные	консультации, в том числе по курсовой работе (проекту)
1	Информационная безопасность. Основные положения, понятия и определения	11	10	1	0	0	
2	Методология обеспечения информационной безопасности деятельности общества.	17	16	1	0	0	
3	Организационно-правовое обеспечение информационной безопасности	26	22	2	0	2	
4	Модели и системы обеспечения информационной безопасности деятельности организаций	23	20	1	0	2	
5	Техническое и методическое обеспечение информационной безопасности	23	20	1	0	2	
Подготовка и защита							

курсовой работы (проекта) / подготовка контрольной работы						
Промежуточная аттестация (зачет)	4	4				0
ИТОГО	**108**	**92**	**6**	**0**	**6**	**4**
В том числе: практическая подготовка	0		0	0	0	

4. Содержание учебной дисциплины

Тема 1. Информационная безопасность. Основные положения, понятия и определения

Понятие информационной безопасности в широком и узком смысле. Основные составляющие информационной безопасности. Информационные войны и информационное оружие. Связь информационной безопасности с другими сферами деятельности общества. Ценность информации. Информация как товар. Угрозы доступности, целостности и конфиденциальности информации.

Тема 2. Методология обеспечения информационной безопасности деятельности общества

Основные составляющие национальных интересов РФ в информационной сфере. Комплексное обеспечение информационной безопасности государства. Области и объекты обеспечения информационной безопасности и защиты информационной деятельности. Доктрина информационной безопасности РФ. Современные подходы к технологиям и методам обеспечения информационной безопасности. Основные проблемы информационной безопасности в РФ.

Тема 3. Организационно-правовое обеспечение информационной безопасности

Уровни обеспечения информационной безопасности. Структура государственной системы обеспечения информационной безопасности. Законодательный уровень информационной безопасности. Отечественные и международные нормативно-правовые акты обеспечения информационной безопасности.

Организационный уровень обеспечения информационной безопасности: правила построения системы защиты информации, методы и средства обеспечения информационной безопасности в системах переработки информации.

Тема 4. Модели и системы обеспечения информационной безопасности деятельности организаций

Политика безопасности. Уровни информационной безопасности: административный, процедурный, программно-технический уровень. Принципы архитектурной безопасности и критерии защищенности информационных систем. Управление рисками информационной безопасности. Аудит информационной безопасности предприятий.

Модели противодействия угрозам безопасности: модели предоставления прав, вероятностные модели, модели Биба, модели защиты информационной системы при отказе в обслуживании, модели анализа безопасности программного обеспечения.

Тема 5. Техническое и методическое обеспечение информационной безопасности

Организация противодействия технической разведке. Методологические основы технического обеспечения защиты процессов переработки информации и контроля её эффективности. Криптографическая защита и программно-аппаратные средства защиты информации. Автоматизация технического контроля защиты потоков информации. Эффективность защиты и методология её расчета.

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

Основная учебная литература

1 Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2022. — 336 с. — (Высшее образование). — DOI: https://doi.org/10.29039/1761-6. - ISBN 978-5-369-01761-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1861657 (дата обращения: 10.09.2022). – Режим доступа: по подписке.

2 Глинская, Е. В. Информационная безопасность конструкций ЭВМ и систем : учебное пособие / Е. В. Глинская, Н. В. Чичварин. - Москва : ИНФРА-М, 2021. - 118 с. - (Высшее образование: Специалитет). - ISBN 978-5-16-016536-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1178153 (дата обращения: 10.09.2022). – Режим доступа: по подписке.

3 Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. — 3-е изд. — Москва : РИОР : ИНФРА-М, 2021. — 400 с. — (Высшее образование). — DOI: https://doi.org/10.12737/1759-3. - ISBN 978-5-369-01759-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1210523 (дата обращения: 10.09.2022). – Режим доступа: по подписке.

Дополнительная учебная литература

4 Бабаш, А. В. История защиты информации в зарубежных странах : учебное пособие / А.В. Бабаш, Д.А. Ларин. — Москва : РИОР : ИНФРА-М, 2021. — 284 с. — (Высшее образование). — DOI: https://doi.org/10.12737/15090. - ISBN 978-5-369-01844-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1215133 (дата обращения: 10.09.2022). – Режим доступа: по подписке.

5 Информационный мир XXI века. Криптография — основа информационной безопасности : методическое руководство / под ред. Э. А. Болелова ; Московский государственный технический университет гражданской авиации. - 4-е изд. — Москва : Издательско-торговая корпорация «Дашков и К°», 2020. — 126 с. - ISBN 978-5-394-03777-1. - Текст : электронный. - URL: https://znanium.com/catalog/product/1081675 (дата обращения: 10.09.2022). – Режим доступа: по подписке.

6 Технические средства и методы защиты информации / Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. - Москва :Гор. линия-Телеком, 2012. - 616 с.: ISBN 978-5-9912-0084-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/560580 (дата обращения: 10.09.2022). – Режим доступа: по подписке.

6. Учебно-методическое, информационное и материально-техническое обеспечение дисциплины

При изучении дисциплины используется следующее учебно-методическое, информационное и материально-техническое обеспечение.

Программное обеспечение:

– тестирующие программные оболочки и контрольно-обучающие программы: ACT-test; Nova-test;

– программы, обеспечивающие доступ в сеть Интернет («Enternet explorer», «Google chrome»);

– программы, демонстрации видео материалов (проигрыватель «Windows Media Player», «Power Point»).

Базы данных, информационно-справочные и поисковые системы:

– Агрегатор научных журналов Directory of Open Access Journals: https://www.doaj.org

– Агрегатор дипломных работ и диссертаций Open Access Theses and Dissertations: https://oatd.org

– Поисковая система научных публикаций Google Scholar: https://scholar.google.ru

– Университетская информационная система РОССИЯ: https://uisrussia.msu.ru/dp.php

– Научная электронная библиотека КиберЛенинка: https://cyberleninka.ru

– Научная электронная библиотека: http://elibrary.ru

– Справочно-правовая система: «Гарант»: https://www.garant.ru

– Справочно-правовая система «Консультант Плюс»: http://www.consultant.ru

– Электронно-библиотечная система Znanium.com : www.znanium.com

– База данных Ruslana. – Режим доступа: http://ruslana.bvdep.com/

– http://nigma.ru – интеллектуальная поисковая система (по темам объединяет результаты, полученные из разных поисковых систем).

Материально-техническое обеспечение

Для осуществления образовательного процесса по дисциплине используются:

- учебные аудитории, оснащенные мультимедийной техникой, позволяющей организовать отработку практических навыков обучающимися, выявить уровень сформированности компетенций методом тестирования и в других интерактивных формах;

- дидактические материалы – презентационные материалы (слайды); бланки анкет и опросов; учебные видеозаписи; комплекты схем, плакатов, стенды;

- технические средства обучения – аудио-, видео-, фотоаппаратура, иные демонстрационные средства; персональный компьютер, множительная техника (МФУ).

Для проведения текущего (рубежного) контроля и промежуточной аттестации (зачета с оценкой) методом компьютерного тестирования используются прошедшие банки тестовых заданий и лицензионная тестирующая программная оболочка типа «АСТ-test», «Nova-test» и(или) другие.

ПЕРЕЧЕНЬ ЛИЦЕНЗИОННОГО И СВОБОДНО РАСПРОСТРАНЯЕМОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, В ТОМ ЧИСЛЕ ОТЕЧЕСТВЕННОГО ПРОИЗВОДСТВА

№ п/п	Комплект лицензионного программного обеспечения		Комплект свободно распространяемого программного обеспечения	
	лицензионное программное обеспечение	лицензионное программное обеспечение отечественного производства	свободно распространяемое программное обеспечение	свободно распространяемое программное обеспечение отечественного производства
1	Microsoft Excel	Антивирус Kaspersky Endpoint Security для бизнеса – Стандартный	Adobe Acrobat Reader DC	Яндекс.Браузер
2	Microsoft Office 365	Электронный периодический справочник "Система Гарант"	Архиватор 7z	Яндекс.Диск
3	Microsoft Word	Электронный периодический справочник "Система Консультант Плюс"		

7. Методические рекомендации для самостоятельной работы обучающихся по дисциплине

Для получения допуска к экзамену обучающийся должен отработать все лабораторные занятия, выполнить все задания самостоятельной (внеаудиторной) работы.

Контроль и оценку самостоятельной (внеаудиторной) работы преподаватель осуществляет на занятиях и в процессе консультаций.

Экзамен проводится в период экзаменационной сессии. В начале обучения по дисциплине обучающиеся знакомятся с программой дисциплины и перечнем вопросов к экзамену.

Аудиторные занятия проводятся в виде:

1) лекций, предусматривающих передачу учебной информации преподавателем обучающимся;

2) лабораторных занятий, обеспечивающих закрепление полученного знания, отработку планируемых навыков и получения опыта деятельности, способствующих формированию компетенций.

Лекция является важным источником информации, так как новый учебный материал не всегда находит отражение в учебниках, отдельные темы учебника могут быть трудны для самостоятельного изучения и требуют освоения в контакте с преподавателем.

Лабораторное занятие предполагает выполнение обучающимися под руководством преподавателя комплекса учебных заданий. На лабораторных занятиях проходит закрепление, углубление, расширение и детализация знаний обучающихся при решении конкретных задач; развитие познавательных способностей, самостоятельности мышления, творческой активности; овладение новыми методами и методиками изучения дисциплины; выработка способности логического осмысления полученных знаний для выполнения заданий; обеспечение рационального сочетания коллективной и индивидуальной форм работы. Лабораторное занятие выполняет познавательную, развивающую и воспитательную функции. При подготовке к лабораторным занятиям следует:

- просмотреть материал предыдущего занятия,
-изучить все термины и понятия по теме лабораторного занятия,
- изучить соответствующий теоретический материал, используя материалы учебника и дополнительной литературы, лекции,
- выполнить задания самостоятельной работы (упражнения, задачи, письменные работы, устные задания и т.п.).

Обучение по дисциплине, наряду с аудиторной работой, предполагает самостоятельную работу обучающихся. В процессе самостоятельной работы обучающиеся повторяют пройденный на занятиях материал, осваивают современные технологии поиска и обработки информации; овладевают стратегиями и методами самообразования; развивают индивидуальные склонности и способности к творчеству.

Самостоятельная работа включает подготовку к лабораторным занятиям; выступлений, докладов и т.п.

В процессе подготовки к занятиям, выполнения самостоятельной работы, подготовки к промежуточной аттестации обучающийся может обратиться к преподавателю за консультацией через личный кабинет электронно-информационной среды или на кафедру.

Тема 1. Информационная безопасность: основные положения, понятия и определения

Цель – получить общее представление об информационной безопасности человека, общества и государства (на примере Российской Федерации) и категориях информационной безопасности

Методические указания к изучению данной темы

Информационная сфера общества состоит из следующих элементов:

- сами субъекты информационного взаимодействия (люди, организации, системы переработки информации);
- информация, используемая этими субъектами;
- информационные технологии и технические средства, используемые для обработки и хранения информации;
- информационная инфраструктура, дающая возможность обмена информацией;
- общественные отношения и система их регулирования.

Для любого элемента информационной сферы существуют свои угрозы информационной безопасности. При этом под *информационной безопасностью* понимают такое состояние социума, при котором обеспечена надежная и всесторонняя защита личности, общества и государства от воздействия на них угроз. Различают информационную безопасность в широком и узком смысле.

В *широком смысле* информационная безопасность подразумевает информационно-психологическую безопасность, т.е. безопасность человека, общества и государства. В *узком смысле* понимается информационно-техническая безопасность, т.е. безопасность компьютерной информации и каналов ее приема и передачи.

Объектами информационной безопасности выступают:

- права и свободы личности;
- материальные и духовные ценности общества;
- государство (его конституционный строй, суверенитет, территориальная целостность, экономика и т.д.)

Если рассматривать информационную безопасность в широком смысле, основной угрозой объектам информационной безопасности является информационная война. *Информационная война* – согласованная деятельность по использованию информации как оружия для разрушающего воздействия на противника в различных сферах (экономической, политической, социальной) и на поле боя. Информационные войны могут происходить не только между

государствами, но и внутри страны, например, при столкновении политических и экономических противников, в ситуациях обострения борьбы за власть, при проведении избирательных кампаний, судебных процессов и т. п.

Основными целями проведения информационной войны является:

- подавление и уничтожение систем управления противника;
- информационное обеспечение боевых действий, политики, экономики;
- подавление электронных систем противника;
- психологическое воздействие на личный состав и население;
- хакерское проникновение в информационные системы противника.

Информационная война ведется с помощью *информационного оружия*, под которым понимается совокупность специально организованной информации, а также информационных технологий, применяемая для деструктивных воздействий на поведение и сознание населения, военнослужащих, а также информационно-технические инфраструктуры государства и общества.

Основной целью применения информационного оружия является завоевание превосходства над противником и нанесение ему поражения как в отдельной боевой операции, так и во внешней и внутренней политике, экономике, обороноспособности страны в целом.

Одной из форм информационной воин является *информационный терроризм,* т.е. особая форма насилия, представляющая собой сознательное и целенаправленное информационное воздействие или угрозу применения такого воздействия для принуждения правительства к реализации целей террористической организации. Обычно информационный терроризм сопровождается эмоциональным воздействием на общество для возбуждения в нем страха, панических настроений, потери доверия к власти и создания политической нестабильности.

В современном обществе информационная безопасность является системообразующим фактором практически всех сфер его жизни. Она оказывает определенное влияние на состояние экономической, оборонной, социальной, политической и других составляющих национальной безопасности. В то же время информационная безопасность сама выступает составной частью национальной безопасности, значение которой с каждым годом неуклонно растет. Особенно тесно она связана с социальной и экологической безопасностью.

Социальная безопасность: с помощью существующих перспективных информационных средств и технологий можно практически полностью контролировать и регулировать информационное взаимодействие людей. Речь идет о потенциальных возможностях подслушивания телефонных разговоров, осуществления контроля за перепиской, создания компьютерных баз данных о каждом человеке, включающих конфиденциальную информацию, и т. д.

К числу форм «скрытого» воздействия на сознание людей можно отнести новые технологии средств массовой информации, психотропное оружие,

сетевые технологии, позволяющие получать доступ к различной негативной информации, в том числе порнографического, националистического и другого характера, современные компьютерные игры, существенно влияющие на формирование сознания детей, и т. д.

Экологическая: до сегодняшнего дня сохраняется определенная закрытость процесса формирования экологической политики страны, которая ведется без достаточного информирования научной общественности. Кроме того, широкие слои населения недостаточно осведомлены об угрозах экологической безопасности, их источниках, о последствиях экологических бедствий и катастроф и т.д. Также, чтобы уменьшить нагрузки на среду, необходимо совершенствовать производственные процессы, переходить к «экологически чистым», энерго- и ресурсосберегающим безотходным технологиям. А это возможно только при условии коренной перестройки экономики за счет ее информатизации, разработке и широком внедрении новых информационных технологий во все отрасли, в том числе в материальное и энергетическое производство, добывающую промышленность.

Формула глобального развития Д. Медоуза позволяет обнаружить прямую связь между информацией и информационными технологиями и нагрузкой на окружающую среду:

$$L = P \cdot A \cdot T, \qquad (1)$$

где L – нагрузка на окружающую среду, P – численность населения, A – уровень благосостояния (потребления на душу населения),
T – технология (ущерб среде, наносимый при производстве единицы продукции с использованием определенной технологии).

Решение большинства экологических проблем и задач связано со сбором и обработкой информации о состоянии природной среды (экологический мониторинг), с моделированием масштабных глобальных процессов, происходящих в природе, с учетом возрастающих техногенных воздействий и антропогенных нагрузок. Очевидно, для эффективного их решения требуется использовать современные информационные средства и технологии.

Информационная безопасность в узком смысле связана с определением, достижением и поддержанием следующих категорий безопасности информации и средств её обработки:

- *конфиденциальность* (доступ к информации только авторизованным пользователям);
- *целостность* (достоверность и полнота информации и методов ее обработки);
- *доступность* (доступ к информации и связанным с ней активам авторизованных пользователей по мере необходимости);
- *неотказуемость* или *апелируемость* (невозможность отказа от авторства);
- *подотчетность* (идентификация субъекта доступа и регистрации его действий);

• *достоверность* (свойство соответствия предусмотренному поведению или результату);

• *аутентичность* или *подлинность* (свойство, гарантирующее, что субъект или ресурс идентичны заявленным).

Основными составляющими информационной безопасности в узком смысле являются:

1. законодательная, нормативно-правовая и научная база;
2. подразделения, обеспечивающие безопасность информационных технологий;
3. организационно-технические и режимные меры и методы;
4. программно-технические способы и средства обеспечения информационной безопасности.

Защищенная автоматизированная система должна обладать следующими свойствами:

• осуществлять автоматизацию процесса обработки;

• успешно противостоять угрозам безопасности, действующим в определенной среде;

• соответствовать требованиям и критериям стандартов информационной безопасности.

Любая информация вне зависимости от формы ее представления может быть предметом товарных отношений. Достоверная информация дает владельцу определенные преимущества перед конкурентами. Недостоверная информация может нанести ее владельцу как материальный, так и моральный ущерб. При этом для конкурентов субъекта информационных взаимоотношений наиболее ценна конфиденциальная информация, т.е. информация, доступ к которой ограничен ее владельцем. Законом «Об информации, информатизации и защите информации» гарантируется право собственника информации на ее использование и защиту от доступа к ней других лиц (организаций).

Распространение информации и ее использование приводят к изменению ее ценности и цены. Ценность большинства видов информации, циркулирующей в обществе, со временем уменьшается, т.к. информация стареет. Ценность информации и время, прошедшее со времени ее создания, связаны между собой формулой:

$$S_i(\tau) = S_0 \cdot e^{\frac{-2,3\tau}{\tau_{жизни}}}, \qquad (2)$$

где S_0 – ценность информации в момент ее создания,

τ – время от момента возникновения информации до момента ее использования,

$\tau_{жизни}$ – продолжительность жизненного цикла информации (от момента возникновения до момента устаревания).

Характер изменения ценности во времени зависит от вида информации. Так, *оперативно-тактическая* информация (например, о стоимости акций на

бирже) теряет ценность в среднем по 10% в день. Ценность *стратегической* информации (например, сведения о получении долгосрочного кредита) убывает до 10% в месяц.

Себестоимость информации зависит от многих факторов, в числе которых:

- затраты на ее получение;
- выбор способов получения информации;
- минимизация затрат при ее добывании.

Количество информации, заключенное в сообщении может быть измерено различными способами. Существуют следующие меры:

- *синтаксическая* – определяется способом представления и кодирования информации;
- *семантическая* – определяется объемом знаний, которое оно несет получателю;
- *прагматическая* – определяется полезностью в достижении получателем его целей.

Задания для самостоятельной работы

Используя приведенный выше материал, подготовьте ответы сохраните их в MS Word на следующие вопросы.

1. По каким признакам можно отличить полезную информацию от информации, являющейся средством агрессии?
2. Прокомментируйте цели и задачи информационных войн.
3. К чему может привести наращивание масштабов и эффективности информационного оружия?
4. Информационная война и «цветные революции» - какие признаки позволяют говорить о наличии связи между ними?
5. Что представляет собой состояние «информационной анархии» в условиях чрезвычайных ситуаций? Как его избежать?
6. Как можно использовать средства информационного противостояния для защиты национальных интересов нашей страны?
7. Как могут повлиять на психику человека информационные военные операции?
8. Влияет ли развитие возможностей информационных средств и систем на духовно-нравственное развитие молодежи? И если да, то как?
9. Почему трудно гарантировать абсолютную сохранность и безопасность данных в компьютерных сетях?
10. Как вы относитесь к сбору и хранению в информационных системах сведений о физических лицах, в том числе о вас лично?
11. Что необходимо расширить в сфере информирования населения СМИ: свободу или систему ограничений?
12. В какой мере обеспечивается сегодня баланс интересов человека, общества и государства в информационной сфере?

13. В чем различие между информационной безопасностью в широком и узком смысле?

14. Дайте определение понятию «информационная война». Каковы ее цели и задачи?

15. Приведите примеры наступательных и оборонительных операций.

16. Дайте определение понятию «информационное оружие». Какие виды информационного оружия существуют?

17. Как связана информационная безопасность с безопасностью экологической и социальной?

18. Прокомментируйте назначение формулы глобального развития Д. Медоуза.

19. Назовите основные категории информационной безопасности и кратко охарактеризуйте их.

20. Назовите виды конфиденциальной информации.

21. Каково соотношение между ценностью информации и временем?

22. Дайте характеристику оперативно-тактической и стратегической информации.

23. От каких факторов зависит себестоимость информации?

24. Охарактеризуйте информацию как экономическую категорию.

25. Назовите и кратко охарактеризуйте меры информации.

26. Охарактеризуйте вероятностный и объемный подходы к измерению семантической меры информации.

27. Что такое защищённая автоматизированная система и каковы ее свойства?

Тема 2. Методология обеспечения информационной безопасности деятельности общества

Цели:

1. получить представление об обеспечении информационной безопасности (ИБ) Российской Федерации;
2. изучить основные положения Доктрины информационной безопасности.

Методические указания к изучению данной темы

Под *информационной безопасностью РФ* понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства. При этом *интересы личности* проявляются в реализации конституционных прав человека и гражданина на доступ к информации и использование информации в интересах осуществления не запрещенной законом деятельности, а также в защите информации, обеспечивающей личную безопасность.

Интересы общества заключаются в:

- обеспечении интересов личности в информационной сфере;
- упрочении демократии;
- создании правового социального государства;
- достижении и поддержании общественного согласия;
- духовном обновлении России.

Интересы государства как общественной структуры заключаются в «создании условий для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и социальной стабильности, в безусловном обеспечении законности и правопорядка, развитии равноправного и взаимовыгодного международного сотрудничества».

Эти определения информационной безопасности взяты из *Доктрины информационной безопасности*, которая представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации.

Доктрина информационной безопасности **является основой для проведения следующих мероприятий** на уровне РФ:

- формирование государственной политики в области обеспечения ИБ РФ;
- подготовка предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения ИБ РФ;

- разработка целевых программ обеспечения ИБ РФ.

Доктрина информационной безопасности **состоит из следующих разделов**.

I. Информационная безопасность РФ. В этом разделе рассматриваются национальные интересы РФ в информационной сфере и меры по их обеспечению, основные угрозы ИБ РФ и их источники, а также современное состояние ИБ РФ и основные задачи по улучшению данной ситуации. В качестве основных национальных интересов подробно рассматриваются следующие: соблюдение конституционного строя; информационное обеспечение государственной политики; развитие отечественных современных информационных технологий; защита информационных ресурсов и информационно-телекоммуникационных систем.

II. Методы обеспечения информационной безопасности РФ. Раздел дает представление о методах обеспечения ИБ РФ и направлениях их приложения, об особенностях обеспечения информационной безопасности РФ в таких сферах общественной жизни, как: экономика, внутренняя и внешняя политика, наука и техника, духовная жизнь, общегосударственные информационные и телекоммуникационные системы, оборона, правоохранительная и судебные сферы. Также в этом разделе приводятся направления международного сотрудничества РФ в области обеспечения ИБ.

III. Основные положения государственной политики обеспечения ИБ РФ и первоочередные мероприятия по ее реализации. В этом разделе рассматриваются основные положения государственной политики обеспечения ИБ РФ и первоочередные мероприятия по реализации государственной политики.

IV. Организационная основа системы обеспечения ИБ РФ. В разделе излагаются основные функции системы обеспечения ИБ РФ и организационные элементы, на основе которых данная система функционирует.

Доктрина информационной безопасности предполагает использование следующих **видов методов** для обеспечения ИБ РФ:

- *правовые*, подразумевающие под собой разработку нормативных правовых актов, регламентирующих отношения в информационной сфере, и нормативных методических документов по вопросам обеспечения ИБ РФ;
- *организационно-технические*, представляющие собой разработку предупреждающих и контролирующих мероприятий органами государственной власти и иных элементов системы обеспечения ИБ РФ с использованием технических и программных средств с целью поддержания защищенности РФ в информационной сфере;
- *экономические*, позволяющие обеспечить материальными и финансовыми средствами соответствующие организационно-технические меры.

Принципы построения государственной политики обеспечения ИБ РФ:

- *законность* представляет собой соблюдение Конституции РФ,

законодательства, принципов и норм международного права при обеспечении ИБ РФ;

• *открытость в реализации функций органов государственной власти* заключается в информировании общества об их деятельности с учетом ограничений, установленных законодательством Российской Федерации;

• *правовое равенство всех участников процесса информационного взаимодействия*, которое основывается на конституционном праве граждан на свободный поиск, получение, передачу, производство и распространение информации любым законным способом;

• *приоритетное развитие отечественных современных информационных и телекоммуникационных технологий.*

Безусловно, для полноценного обеспечения ИБ государства использование одной Доктрины недостаточно. Необходимо учитывать не только современный уровень развития информационных технологий, но и уровень развития системы информационной безопасности в стране и мире в целом.

Различают следующие эволюционные подходы к обеспечению ИБ РФ.

1. Эмпирический подход был наиболее распространен в 60-е гг. прошлого века, когда ЭВМ использовались только в крупных организациях и не были повсеместно распространены. Для него характерно непрерывное слежение за появлением новых угроз и разработка средств защиты от новых угроз. Необходимые механизмы защиты внедрялись на основании предыдущего опыта организации. Среди средств защиты информации преобладали преимущественно построенные на функционально-ориентированных механизмах защиты, которые были ориентированы на предупреждение несанкционированного получения информации посторонними лицами и процессами, не имеющими на это полномочий, а также на контроль целостности информации. Теоретико-вероятностные зависимости для оценки угроз не получили своё развитие в силу малой статистической базы.

2. *Концептуально-ориентированный подход* получил распространение в 70-е гг. прошлого века в связи с появлением первых персональных компьютеров. Его основной особенностью являлась унификация средств защиты и формирование на основе опыта других организаций общей концепции защиты конкретной организации. Кроме того, велась разработка и научное обоснование методов оценки уязвимости информации, что послужило толчком к появлению стандартных решений по защите информации.

3. *Теоретико-концептуальный подход* развился в 80-е гг. прошлого века в связи с широким распространением компьютерной техники и преобладает по настоящее время. Для него характерна разработка основ теории защиты информации, на основании которой обосновывается постановки задача многосторонней комплексной защиты и вводится понятие стратегии защиты. Это в свою очередь позволяет разработать методологии создания систем защиты и управления ими и унифицировать концепции защиты. В настоящее время для области защиты информации характерно широкое развитие

стандартизированных решений и применение на предприятиях систем комплексной защиты. Большинство организаций в ходе реализации своей повседневной деятельности ориентируются на защищенные информационные технологии.

Однако даже самые защищенные механизмы защиты не решают многих проблем ИБ, существующих в современном обществе. Среди них в Доктрине ИБ, а также других источниках указываются следующие:

1. обострение противоречий между потребностями общества в расширении свободного обмена информацией и необходимостью сохранения отдельных ограничений на ее распространение. Особенно актуальной эта проблема становится в связи с развитием файлообменников и социальных сетей, когда содержание и доступность информации практически нельзя проконтролировать;

2. недостаточность нормативного правового регулирования отношений в области реализации возможностей конституционных ограничений свободы массовой информации в интересах защиты основ конституционного строя. В свою очередь это затрудняет поддержание необходимого баланса интересов личности, общества и государства в информационной сфере;

3. права граждан на неприкосновенность частной жизни, личную и семейную тайну, тайну переписки не имеют достаточного программно-аппаратного и законодательного обеспечения, т.к. законодательная база существенно отстает от темпов развития информационных технологий;

4. неудовлетворительно организована защита собираемых органами государственной власти персональных данных, что может приводить к раскрытию этих данных и использования их в корыстных целях злоумышленниками;

5. вытеснение российских средств массовой информации с внутреннего информационного рынка в связи с отсутствием четкой государственной политики в этой области;

6. утечка специалистов по созданию средств информатизации из государственных структур в коммерческие, что препятствует полноценному контролю государства в области создания средств защиты;

7. зависимость РФ от зарубежных поставщиков информационных технологий в связи со слабым развитием своего рынка;

8. отсутствие системы эффективного контроля за обеспечением ИБ со стороны государственных структур и общества в целом, низкая компетенция граждан в вопросах защиты информации.

Задания для самостоятельной работы

Используя приведенный выше теоретический материал и Доктрину информационной безопасности, подготовьте ответы на приведенные ниже вопросы в MS Word.

1. Четыре основные составляющие национальных интересов РФ в информационной сфере и способы их достижения.
2. Основные виды и источники угроз ИБ РФ.

3. Особенности обеспечения ИБ РФ в сферах экономики, внешней и внутренней политики (перечислить угрозы, меры и мероприятия).

4. Особенности обеспечения ИБ РФ в сферах обороны, правоохранительной и судебной систем (перечислить угрозы, меры и мероприятия).

5. Особенности обеспечения ИБ РФ в областях науки и техники, в духовной сфере (перечислить угрозы, меры и мероприятия).

6. Особенности обеспечения ИБ РФ в информационных и телекоммуникационных системах (перечислить угрозы, меры и мероприятия).

7. Основные функции системы обеспечения информационной безопасности Российской Федерации.

8. Основные элементы организационной основы системы обеспечения информационной безопасности Российской Федерации и их обязанности.

9. Какие угрозы – внешние или внутренние – оказываются более существенными для информационной безопасности нашего общества и вас лично? Почему?

10. Ощущаете ли вы в своей повседневной жизни отставание России в разработке и внедрении информационных систем разного уровня? Приведите примеры.

11. Решаются ли все проблемы информационной безопасности человека и общества созданием соответствующей нормативно-правовой базы и внедрением современных информационных технологий?

12. Происшедшая в мире информационная революция, на ваш взгляд, усилила или ослабила национальную безопасность России? Обоснуйте свой вариант ответа.

13. Назовите интересы личности, общества и государства в информационной сфере.

14. Каково назначение Доктрины информационной безопасности?

15. Охарактеризуйте кратко содержание Доктрины информационной безопасности.

16. Каковы основные группы методов обеспечения информационной безопасности РФ?

17. Назовите принципы построения государственной политики обеспечения информационной безопасности Российской Федерации.

18. Каковы первоочередные мероприятия по реализации государственной политике обеспечения информационной безопасности?

19. Перечислите основные проблемы информационной безопасности.

20. Дайте краткую характеристику основным подходам к обеспечению информационной безопасности.

21. Представьте схему организации защиты информации, используемой в эмпирическом подходе к обеспечению информационной безопасности.

22. Охарактеризуйте этапы унифицированной концепции защиты информации.

Тема 3. Организационно-правовое обеспечение информационной безопасности

Цели:

1.1. получить представление об основных нормативно-правовых актах обеспечения информационной безопасности и их требованиях к процессу защиты информации;

1.2. изучить меры ответственности за правонарушения в информационной сфере;

1.3. рассмотреть основные организационные мероприятия по защите информации на предприятии.

Методические указания к выполнению данной темы

Помимо использования программных и аппаратных средств, проблема информационной безопасности решается также на законодательном и организационном уровнях. На законодательном уровне проблема обеспечения информационной безопасности включает в себя не только законы, но и структуру органов обеспечения информационной безопасности и выполнение их функций. Организационный уровень подразумевает выполнение определенных мероприятий на предприятии с использованием штатных программно-аппаратных средств в рамках действия существующих законов и стандартов информационной безопасности.

Существующая система государственной системы обеспечения ИБ согласно действующим нормам делится на международный, федеральный, региональный и местный уровни. При этом нормы каждого уровня могут изменять соответствующие органы управления, за их выполнение отвечают органы контроля. Все основные элементы этой системы приведены в таблице 1.

Таблица 1

Структура государственной системы ИБ

Нормы	Управление	Контроль
Международное право	ООН Совет безопасности ООН	Международный суд
Федеральное законодательство	Президент РФ Совет безопасности Государственная Дума Межведомственная комиссия по защите государственной тайны ФСТЭК, ФСБ и др.	Конституционный суд Верховный суд Генеральная прокуратура
Ведомственные нормативные акты	Органы местного самоуправления Органы по защите информации	Суды Прокуратура
Инструктивно-	Руководители подразделений	Административные

методические документы	Органы по защите информации	органы

Система государственной системы обеспечения ИБ позволяет решить следующие задачи:

1. защита персональных данных;
2. борьба с компьютерной преступностью, в первую очередь в финансовой сфере;
3. защита коммерческой тайны и обеспечение благоприятных условий для предпринимательской деятельности;
4. защита государственных секретов;
5. создание системы взаимных финансовых расчетов в электронной форме с элементами электронной подписи;
6. обеспечение безопасности АСУ потенциально опасных производств;
7. страхование информации и информационных систем;
8. сертификация и лицензирование в области безопасности, контроль безопасности информационных систем;
9. организация взаимодействия в сфере защиты данных с другими странами.

Существующие нормы на федеральном и региональном уровнях закреплены в следующих документах:

- Конституция РФ;
- Федеральные законы РФ («О государственной тайне», «О коммерческой тайне», «Об информации, информационных технологиях и защите информации», «Об электронной подписи», «О техническом регулировании», «О лицензировании отдельных видов деятельности», «О связи», «О персональных данных» и пр.);
- Уголовный, Гражданский кодексы и Кодекс об административных правонарушениях;
- Постановления Правительства РФ;
- Ведомственные нормативные акты;
- Государственные стандарты;
- Руководящие документы.

Государственные стандарты в основном носят добровольный характер, кроме организаций, работающих в банковской сфере и выполняющих работы, связанные с государственной тайной. Процесс подтверждения выполнения требований стандарта на конкретном предприятии называется *сертификацией.* Процесс сертификация деятельности предприятия подразумевает под собой выполнение трех этапов:

1. предварительная оценка системы управления ИБ и ее диагностика штатными средствами предприятия. Решение о проведении внешнего аудита;
2. сертификационный аудит, проводимый внешними аудиторами;
3. в случае положительной оценки деятельности предприятия, данной сертификационным аудитом, выдача сертификата и поддержка его действия (проведение ежегодных инспекционных аудитов). В случае, если инспекционный аудит не покажет эффективность существующей системы

защиты информации, сертификат будет отозван.

Отметим, что наличие подобного сертификата обеспечивает дополнительную конкурентоспособность предприятия на рынке.

Рассмотрим основные стандарты международного уровня в области информационной безопасности.

1. ***Стандарт ISO 27002 (Практические правила управления ИБ)*** устанавливает рекомендации по управлению ИБ лицам, ответственным за планирование, реализацию или поддержку решений безопасности в организации. Он предназначен для обеспечения общих основ для разработки стандартов безопасности и выбора практических мероприятий по управлению безопасностью в организации вне зависимости от используемых технических решений. Основные разделы стандарта:

Текущая версия стандарта состоит из следующих основных разделов:

- Политика безопасности (Security policy);
- Организация информационной безопасности (Organization of information security);
- Управление ресурсами (Asset management);
- Безопасность персонала (Human resources security);
- Физическая безопасность и безопасность окружения (Physical and environmental security);
- Управление коммуникациями и операциями (Communications and operations management);
- Управление доступом (Access control);
- Приобретение, разработка и поддержка систем (Information systems acquisition, development and maintenance);
- Управление инцидентами информационной безопасности (Information security incident management);
- Управление бесперебойной работой организации (Business continuity management);
- Соответствие нормативным требованиям (Compliance).

2. ***Стандарт ISO 15408 (Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологи)*** определяет инструменты оценки безопасности информационных систем и порядок их использования. Выделяются следующие виды требований безопасности:

• *функциональные* – предъявляются к функциям безопасности и реализующим их механизмам, представляют собой активный компонент защиты;

• *требования доверия* – предъявляются к технологии и процессу разработки и эксплуатации информационной системы, представляют собой пассивный компонент защиты.

Названные выше требования рассматриваются на каждом этапе жизненного цикла объекта:

• определение назначения, условий применения, целей и требований безопасности;

• проектирование и разработка;

• испытания, оценка и сертификация;

• внедрение и эксплуатация.

Защитить информационную систему – значит разработать пакет нормативных документов, включающих в себя:

• *профиль защиты* – типовой набор требований, которым должны удовлетворять продукты и/или системы определенного класса;

• *задание по безопасности* – совокупность требований к конкретной разработке, выполнение которых обеспечивает достижение поставленных целей безопасности.

Стандарт состоит из трех частей.

2.1. **Введение и общая модель** определяет так называемые «Общие критерии» (ОК), которые предназначены для использования в качестве основы при оценке характеристик безопасности продуктов и систем информационных технологий. В этой части излагаются общие теоретические вопросы, приводятся основные определения этого стандарта, а также целевые группы, для которых предназначен данный стандарт.

2.2. Часть **«Функциональные требования»** распространяется на функциональные компоненты безопасности, являющиеся основой для функциональных требований безопасности информационных технологий объекта оценки. Требования описывают желательный безопасный режим функционирования объекта оценки и предназначены для достижения целей безопасности, а также описывают также свойства безопасности, которые пользователи могут обнаружить при непосредственном взаимодействии с объектом оценки.

2.3. Часть «**Требования доверия к безопасности»** определяет требования доверия к безопасности и включает в себя оценочные уровни доверия, определяющие шкалу для измерения доверия, собственно компоненты доверия, из которых составлены уровни доверия, и критерии для оценки профиля защиты и задания по безопасности.

3. ***Критерии оценки пригодности компьютерных систем министерства обороны*** (Department of Defence Trusted Computer System Evaluation Criteria;TCSEC), более известная как «Оранжевая книга» (по цвету обложки). Основным постулатом Оранжевой книги является: «Любую систему можно «взломать», если располагать достаточно большими материальными и временными ресурсами». Соответственно есть смысл оценивать лишь степень доверия, которое разумно оказать той или иной системе. При этом под *надежной системой* понимается система, использующая достаточные аппаратные и программные средства, чтобы обеспечить одновременную обработку информации разной степени секретности группой пользователей без нарушения прав доступа. Надежность системы оценивается по существующей на предприятии политике безопасности и *гарантированности*, которая представляет собой меру

доверия, которая может быть оказана архитектуре и реализации системы и показывает, насколько корректны механизмы, отвечающие за проведение в жизнь политики безопасности. В данном стандарте рассматриваются следующие элементы политики безопасности:

- произвольное управление доступом;
- безопасность повторного использования объектов;
- метки безопасности;
- принудительное управление доступом;
- подотчетность;
- идентификация и аутентификация;
- предоставление надежного пути;
- аудит.

Под *меткой безопасности* понимается механизм обеспечения безопасности, включающий уровень секретности и список категорий информации (т.н. предметную область).

4. ***Рекомендации X.800*** являются основополагающим документом в области защиты распределенных систем. Главным отличием от других стандартов является распределение функций обеспечения ИБ по уровням сетевой модели OSI. Перечислим функции безопасности, выделяемые в рекомендациях для распределенных систем:

- *аутентификация*. Данная функция обеспечивает аутентификацию партнеров по общению и аутентификацию источника данных. Она служит для подтверждения подлинности партнера и источника данных;
- *управление доступом* обеспечивает защиту от несанкционированного использования ресурсов, доступных по сети;
- *конфиденциальность данных*. Данная функция обеспечивает защиту от несанкционированного получения информации. При этом различают следующие виды конфиденциальности: конфиденциальность данных при общении с установлением соединения, конфиденциальность данных при общении без установления соединения, конфиденциальность отдельных полей данных и конфиденциальность трафика;
- *целостность данных;*
- *неотказуемость*. Данная функция невозможности отказаться от совершенных действий обеспечивает два вида услуг: неотказуемость с подтверждением подлинности источника данных и неотказуемость с подтверждением доставки.

Помимо рассмотренных международных стандартов, на федеральном уровне применяются российские стандарты, руководящие документы и методические материалы, позволяющие организации регламентировать процесс защиты информации. Более подробно некоторые из этих нормативных документов будут рассмотрены в ходе выполнения практической работы.

Рассмотрим организационный уровень обеспечения ИБ.

При построении системы защиты информации используются следующие **правила**:

• *профилактика возможных угроз*, выявленных в результате оценки информационной системы;

• *законность*, т.е. соответствие существующей нормативной базе;

• комплексное использование сил и средств;

• *координация и взаимодействие внутри и вне предприятия*, в том числе распределение ответственности за сохранность информации между подразделениями;

• сочетание гласности с секретностью;

• *компетентность* специалистов, разрабатывающих систему безопасности, использование современных средств защиты информации;

• *экономическая целесообразность*, т.е. эффективность вложения средств в защиту информации;

• *плановая основа деятельности* по защите информации;

• *системность*, т.е. не хаотичное использование средств защиты, но использование их в определенных целях, позволяющих в комплексе закрыть каналы утечки информации.

Указанные правила основываются на следующих **принципах защиты** информации:

• *адекватность* – совокупная стоимость защиты должна быть ниже стоимости защищаемых ресурсов;

• *системность* – система защита должна строиться на основе анализа угроз и оптимальном наборе средств защиты;

• *прозрачность для легальных пользователей* – для обычных пользователей должно быть понятно назначение применяемых средств защиты;

• *равностойкость звеньев* – прочность всей системы защиты определяется прочностью самого слабого звена;

• *непрерывность* – система должна обеспечивать постоянную защиту информации, без сбоев;

• *многоуровневость защиты* – применение различных наборов средств защиты на каждом уровне доступа к информации в зависимости от уровня ее конфиденциальности.

Перечислим основные организационные мероприятия по защите информации на предприятии:

• отнести информацию к категории ограниченного доступа;

• постоянно прогнозировать и выявлять угрозы безопасности информационным ресурсам;

• создать условия функционирования с наименьшей вероятностью реализации угроз безопасности информационным ресурсам и нанесения ущерба;

• создать механизм и условия оперативного реагирования на угрозы ИБ и их пресечения;

• создать условия для максимально возможного возмещения и локализации ущерба.

Задания для лабораторной работы

Функции органов по защите информации.

Основные нормативные документы по защите информации

Используя материалы Интернета, заполните таблицы 2 и 3.

Таблица 2

Краткая характеристика органов по защите информации

Название	Сфера ответственности	Функции
Федеральная служба по техническому и экспортному контролю		
Федеральная служба безопасности		
Служба внешней разведки		
Министерство обороны		

Таблица 3

Содержание основных нормативных документов по защите информации

Документ	Цель принятия	Контролируемые вопросы по защите информации
Конституция РФ		
Уголовный кодекс		
Гражданский кодекс		
Кодекс об административных правонарушениях		
ФЗ «О государственной тайне»		
ФЗ «О коммерческой тайне»		
ФЗ «Об информации, информатизации и защите информации»		
ФЗ «Об электронной подписи»		
ФЗ «О техническом регулировании»		
ФЗ «О лицензировании отдельных видов деятельности»		
ФЗ «О связи»		

Основные нормативно-правовые акты в области защиты информации

Используя приведенные ниже нормативно-правовые акты, подготовьте ответы на вопросы в текстовом документе MS Word.

Нормативно-правовые акты

1. ГОСТ Р ИСО/МЭК 15408-1-2012 "Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель"
2. ГОСТ Р ИСО/МЭК 15408-2-2013 "Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности"
3. ГОСТ Р ИСО/МЭК 15408-3-2013 "Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности"
4. ГОСТ Р ИСО/МЭК 27002-2012 "Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности"
5. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации
6. Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации
7. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

Вопросы

1. Для каждого нормативно-правового акта заполните таблицу 4.

Таблица 4

Краткая характеристика нормативно-правовых актов по защите информации

Номер акта в списке	Назначение (область применения)	Ключевые понятия
1		
…		
7		

Для стандартов ГОСТ Р ИСО/МЭК 15408-1-2012 (части 1, 2 и 3) найдите ответы на следующие вопросы.

2. Дайте определения следующим понятиям: «атрибут безопасности», «доверие», «задание по безопасности», «потенциал нападения», «профиль защиты», «стойкость функции безопасности», «цель безопасности», «компонент», «элемент», «класс», «пакет».
3. Охарактеризуйте части этого стандарта с точки зрения нужд разработчика и аудитора (оценщика). Результат представьте в виде таблицы.

4. Что такое функциональные требования? Перечислите основные классы функциональных требований и их наиболее важные элементы.

5. Назовите причины появления уязвимостей.

6. Что такое требования доверия? Назовите классы и типы элементов доверия.

Для стандарта ГОСТ Р ИСО/МЭК 27002-2012 выполните задания.

7. Заполните таблицу 5.

Таблица 5

Меры по соблюдению политики безопасности (ПБ)
персоналом и контрагентами предприятия

Направление работ	Мероприятия для соблюдения ПБ
Проведение совместных работ	
Проверка персонала при найме	
Документационное подтверждение ПБ	
Обучение персонала	
Реагирование на инциденты ИБ	

8. Заполните таблицу 6.

Таблица 6

Мероприятия по защите информации
с использованием программно-аппаратных средств

Направление защиты	Мероприятия по защите
Создание охраняемых зон	
Обеспечение безопасности оборудования	
Защита от вирусов	
Работа с переносными устройствами	
Работа сотрудников в дистанционном режиме	
Общие мероприятия по управлению ИБ	

9. Перечислите и кратко охарактеризуйте элементы управления непрерывностью бизнеса.

10. Заполните таблицу 7.

Таблица 7

Мероприятия по выполнению требований законодательства
в области защиты информации

Требования законодательства	Характеристика требования	Мероприятия
Соблюдение права интеллектуальной собственности		
Конфиденциальность персональных данных		

11. Дайте определения следующим понятиям: «журнал аудита», «биометрия», «классификация», «политика ИБ», «цифровая подпись», «межсетевой экран», «принцип необходимого знания», «средства идентификации», «уязвимость».

12. Назовите назначение политики ИБ и приведите обязанности сотрудников по ее выполнению различных категорий.

13. Заполните таблицу 8.

Таблица 8

Обязанности сотрудников предприятия, непосредственно ответственных за соблюдение ПБ

Должность	Обязанности
Руководитель службы обеспечения ИБ	
Ответственный за ИБ	
Оператор обеспечения безопасности	

14. Дайте краткую характеристику каждого уровня документации программы обеспечения ИБ.

15. Заполните таблицу 9.

Таблица 9

Характеристика защитных мер

Направление защиты	Нейтрализуемые угрозы	Используемые средства
Логический контроль доступа		
Защита сетей		
Защита банковских карточек		

16. Что относится к инцидентам ИБ? Какова должна быть реакция руководителей предприятия на инциденты?

Для руководящего документа «Средства вычислительной техники. Защита от несанкционированного доступа к информации …» ответьте на вопросы.

17. Какова область применения показателей, указанных в руководящем документе.

18. Назовите выделяемые классы защищенности информации.

19. Перечислите показатели защищенности информации и дайте их краткую характеристику.

Для руководящего документа «Средства вычислительной техники. Межсетевые экраны …» ответьте на вопросы.

20. Какова область применения выделяемых показателей?

21. Дайте определение понятиям «межсетевой экран», «экранирование».

22. Чем критерии фильтрации отличаются от правил фильтрации?

23. Дайте краткую характеристику выделяемых классов и назовите их назначение.

24. Перечислите показатели защищенности межсетевых экранов и дайте их краткую характеристику.

Для документа «Методика определения актуальных угроз безопасности персональных данных…» ответьте на вопросы.

25. Назовите основные каналы утечки информации.

26. Каковы основные источники угроз персональным данным?

27. Перечислите показатели исходной защищенности ИСПДн.

28. Объясните суть подхода к составлению перечня актуальных угроз. Выделите основные этапы методики и представьте их в виде схемы.

Вопросы для самостоятельной работы.

Используя ресурсы сети Интернет, специализированные словари, а также Уголовный, Гражданский кодексы и Кодекс об административных правонарушениях, найдите ответы на вопросы.

1. Дайте определения понятиям: юридическая ответственность, принцип презумпции невиновности, правонарушение.
2. Назовите виды санкций в соответствии со способом, каким они служат охране правопорядка, и дайте их краткую характеристику.
3. Приведите характеристики правовосстановительной и штрафной (карательной) ответственности.
4. Перечислите виды административных и уголовных наказаний.
5. В чем заключается правовосстановительная ответственность в области защиты коммерческой тайны?
6. Приведите содержание статей Кодекса об административных правонарушениях, затрагивающих следующие вопросы:

а) защита авторских и смежных прав;

б) защита персональных данных;

в) лицензирования деятельности по защите информации (отдельно рассмотреть сведения, относящиеся к государственной тайне и к ней не относящиеся);

г) сертификация информационных систем, баз и банков данных и средств защиты информации (отдельно рассмотреть средства защиты государственной тайны и других видов тайн);

д) защита от разглашения различных видов тайн.

7. Приведите содержание статей Уголовного кодекса, затрагивающих следующие вопросы:

а) неправомерный доступ к охраняемой законом компьютерной информации;

б) создание вредоносных программ («вирусов»);

в) нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

Меры по защите информации, предпринимаемые на организационном уровне

Используя ресурсы сети Интернет, материалы лекций и личный опыт, выполните задания.

1. Заполните таблицу 10.

Таблица 10

Методы обеспечения безопасности процессов переработки информации

Метод	Краткая характеристика	Примеры привлекаемых средств

		и проводимых мероприятий
Препятствие		
Управление доступом		
Маскировка		
Регламентация		
Побуждение		
Принуждение		

2. Заполните таблицу 11.

Таблица 11

Технологии предотвращения угроз ИБ

Угроза	Применяемые технологии	Примеры привлекаемых средств
Шпионаж и диверсии		
Несанкционированный доступ к информации		
Случайные угрозы (ошибки персонала и стихийные бедствия)		

3. Приведите примеры не менее 3 мероприятий, реализующих технологии парирования угроз информационной безопасности. Для каждого мероприятия укажите привлекаемые программно-аппаратные средства.

4. Приведите примеры не менее 3 мероприятий, реализующих технологии нейтрализации угроз информационной безопасности. Для каждого мероприятия укажите привлекаемые программно-аппаратные средства.

5. Дайте краткую характеристику основным направлениям обеспечения ИБ на предприятии.

6. Опишите основные элементы структуры государственной системы обеспечения ИБ и их функциональное назначение.

7. Перечислите основные функции государственной системы обеспечения ИБ.

8. Назовите основные функции Федеральной службы по техническому и экспортному контролю, ФСБ, Службы внешней разведки и Министерства обороны в области защиты информации.

9. Приведите структуру нормативной базы по защите информации и кратко охарактеризуйте основные положения по защите информации, присутствующие в каждом из названных актов.

10. Опишите процесс сертификации предприятия на соответствие требованиям стандартов по информационной безопасности.

11. Опишите назначение и краткое содержание основных разделов стандарта ISO 17799.

12. Назовите ключевые средства контроля, рассматриваемые в стандарте ISO 17799.

13. Опишите назначение стандарта ISO 15408. Какие виды требований безопасности выделяет этот стандарт? Что такое профиль защиты и задание по безопасности?

14. Назовите классы функциональных требований и требований доверия, выделяемых в стандарте ISO 15408.

15. Опишите основную концепцию, на которой построена Оранжевая книга. По каким критериям в ней определяется надежность систем? Какие виды меток безопасности выделяются?

16. Дайте краткую характеристику рекомендациям X.800.

17. Приведите примеры 2-3 руководящих документов в области защиты информации и опишите кратко их назначение.

18. Назовите основные правила построения системы информационной безопасности предприятия.

19. Охарактеризуйте кратко основные принципы защиты информации на предприятии.

20. Перечислите основные методы обеспечения безопасности процессов переработки информации.

21. Назовите основные технологии предотвращения угроз информационной безопасности.

22. Приведите примеры технологий парирования и нейтрализации угроз ИБ и привлекаемых программно-аппаратных средств.

23. Перечислите основные организационные мероприятия по защите информации на предприятии.

Тема 4. Модели и системы обеспечения информационной безопасности деятельности организаций

Цели:

1.1. рассмотреть основные уровни информационной безопасности и научиться выявлять их основные компоненты для конкретного предприятия;
1.2. изучить принципы архитектурной безопасности и критерии защищенности информационных систем;
1.3. получить навыки управления рисками информационной безопасности на предприятии;
1.4. изучить основы проведения аудита информационной безопасности предприятий;
1.5. получить представление о моделях противодействия угрозам безопасности и научиться применять их на практике.

Методические указания к выполнению самостоятельной работы

На современном предприятии применяются следующие уровни информационной безопасности.

Законодательный уровень включает в себя различные нормативно-правовые акты, существующие в тех государствах, с которыми взаимодействует предприятие.

Административный уровень представляет собой приказы и другие действия руководства организации, связанные с защищаемыми информационными системами. Основными целями этого уровня является формирование программы работ и обеспечение ее выполнения с помощью соответствующих ресурсов и контроля. Следует отметить, что в основе административного уровня лежит *политика безопасности*, под которой понимается совокупность документированных решений, принимаемых руководством организации и направленных на защиту информации и ассоциированных с ней ресурсов. В большинстве организаций политика безопасности имеет многоуровневую структуру. Краткая характеристика ее уровней представлена в таблице 12.

Процедурный уровень представляет собой меры безопасности, ориентированные на людей и включает следующие категории:

1. *управление персоналом* (отбор персонала при приеме на работу, обучение вновь принятого персонала и повышение квалификации уже работающего, системное администрирование учетных записей пользователей);

2. *физическая защита* (физическое управление доступом; противопожарные меры; защита систем электро-, водо- и теплоснабжения, средств коммуникаций; защита от перехвата данных по системам связи и защита мобильных систем);

3. *поддержание работоспособности* (техническая поддержка

пользователей, аудит установленного программного обеспечения и контроль за соблюдением прав доступа к нему, конфигурационное управление, резервное копирование, управление носителями с целью соблюдения режима безопасности);

Таблица 12

Характеристика уровней политики безопасности

Название уровня	Направленность	Рассматриваемая информация
верхний	организация в целом	• описание подразделений, отвечающих за работы по управлению безопасностью; • имеющиеся материальные и информационные ресурсы и необходимый уровень их защиты; • меры безопасности, применяемые к персоналу; • вопросы физической безопасности информации; • подход к управлению компьютерами и компьютерными сетями; • правила разграничения доступа к производственной информации; • порядок разработки и сопровождения информационных систем; • меры, направленные на обеспечение непрерывной работы организации • подтверждение соответствия политики безопасности действующему законодательству
средний	отдельные аспекты безопасности для эксплуатируемых систем	• область применения системы; • позиция организации по данному аспекту защиты системы; • права и обязанности сотрудников в процессе поддержки информационной безопасности системы; • соответствие законодательству; • точки контакта (обращение за информацией)
нижний	информационные	• группы сотрудников, имеющих

	сервисы	право доступа к объектам, поддерживаемым сервисом; • условия, при которых можно читать и модифицировать данные; • способ организации защищенного удаленного доступа к сервису

4. *реагирование на нарушения режима безопасности* (локализация инцидента, уменьшение наносимого вреда, выявление нарушителя, предупреждение повторных нарушений);

5. *планирование восстановительных работ* (выявление критически важных функций организации и установление приоритетов; идентификация ресурсов, необходимых для выполнения критически важных функций; определение перечня возможных аварий; разработка стратегии восстановительных работ).

Программно-технический уровень представляет собой сервисы безопасности, реализуемые с помощью комплекса программных и аппаратных средств обеспечения безопасности.

К таким *сервисам* относятся:

- *идентификация и аутентификация* субъектов и процессов системы;
- *управление доступом* к ресурсам системы;
- *протоколирование и аудит* действий пользователей;
- *шифрование* файлов и папок системы;
- *контроль целостности* программного обеспечения и критически важных объектов системы;
- *экранирование* участков компьютерной сети, выделение наиболее защищенных участков сети;
- *анализ защищенности* критически важных объектов системы;
- *обеспечение отказоустойчивости и безопасного восстановления* системы;
- *туннелирование* потоков данных с целью создания защищенных каналов передачи данных.

Все сервисы делятся на следующие категории (при этом один и тот же сервис может относиться одновременно к нескольким категориям):

- превентивные, препятствующие нарушениям информационной безопасности;
- меры обнаружения нарушений;
- локализующие, сужающие зону воздействия нарушений;
- меры по выявлению нарушителя;
- меры восстановления режима безопасности.

При построении системы информационной безопасности на предприятии необходимо учитывать не только указанные выше уровни ИБ, но также принципы архитектурной безопасности и критерии защищенности информационных систем.

К **принципам архитектурной безопасности** относятся:

- *непрерывность защиты в пространстве и времени*, невозможность

миновать защитные средства в конкретном сегменте сети или в какой-то строго определенный момент времени (например, при проведении профилактических работ);

• *следование признанным стандартам*, использование апробированных решений, которые позволяют на основании опыта многих предприятий выработать свою, адаптированную под нужды предприятия, методику защиты;

• *иерархическая организация информационной системы*, предоставляющая больше возможностей администратору систему для организации контроля доступа к ее ресурсам;

• *усиление самого слабого звена*, т.е. если самое слабое звено системы безопасности будет снабжено достаточной защитой, это позволит избежать взлома системы в целом;

• *невозможность перехода в небезопасное состояние* вследствие наступления каких-либо неблагоприятных событий или обстоятельств;

• *минимизация привилегий* пользователей, позволяющая ограничить их зону воздействия на систему и таким образом сократить статьи расходов на обеспечение ее безопасности;

• *разделение обязанностей* пользователей и администраторов системы безопасности для четкого выявления виновных лиц в инцидентах нарушения ИБ;

• *эшелонированность обороны*, т.е. использование нескольких механизмов защиты для наилучшей защиты;

• *разнообразие защитных средств* и применение их в комплексе для решения поставленных задач;

• *простота и управляемость информационной системы* для администраторов системы и директоров предприятия.

Согласно Оранжевой книге безопасности выделяются следующие **критерии защищенности информационных систем**.

• *Политика безопасности*: компьютерная сеть должна поддерживать политику безопасности. Возможность доступа субъектов к объектам должна определяться на основании их идентификации и набора правил управления доступом.

• *Метки*: каждый объект доступа имеет метку безопасности, используемую в качестве исходной информации для исполнения процедур контроля доступа.

• *Идентификация и аутентификация*: все субъекты должны иметь уникальные идентификаторы. Доступ субъекта к ресурсам системы должен осуществляться на основании результатов идентификации и аутентификации пользователей в системе.

• *Регистрация и учет*: для определения ответственности пользователей за действия в системе, все происходящие в ней события, должны отслеживаться и регистрироваться в защищенном объекте (файле-журнале). Система регистрации осуществляет анализ общего потока событий и выделяет из него только те события, которые оказывают влияние на безопасность

системы.

• *Контроль корректности функционирования средств защиты*: все средства защиты, обеспечивающие политику безопасности, должны находиться под контролем средств, проверяющих корректность их функционирования и быть независимыми от них.

• *Непрерывность защиты*: все средства защиты должны быть защищены от несанкционированного воздействия или отключения. Защита должна быть постоянной и непрерывной в любом режиме функционирования системы и ее средств защиты.

Выше были описаны основополагающие моменты, на которые следует опираться при построении защищенных информационных систем предприятия. Но процесс защиты информации является непрерывно развивающимся во времени, поэтому следует периодически оценивать риски информационной безопасности, и в результате этой оценки перестраивать систему информационной безопасности.

Под *управлением рисками* подразумевается оценка их размера, выработка эффективных и экономичных мер их снижения и периодическая проверка, что риски заключены в приемлемые рамки (и остаются таковыми).

По отношению к выявленным рискам возможно проведение следующих действий:

1. *ликвидация* – устранение причины риска;

2. *уменьшение* – использование дополнительных средств защиты для уменьшения влияния риска на информационную систему;

3. *принятие* – при невозможности полной ликвидации этого риска вырабатывается план действий в случае реализации угрозы;

4. *переадресация* – заключение страхового соглашения, согласно которому в случае наступления оговоренного страхового случая предприятию полагается определенная денежная компенсация.

Рассмотрим этапы процесса управления рисками, которые подразделяются на подготовительные и основные.

1. Подготовительные этапы:

1.1. выбор анализируемых объектов и уровня детализации их рассмотрения;

1.2. выбор методологии оценки рисков;

1.3. идентификация активов, в числе которых обычно рассматриваются компоненты информационной системы, поддерживающая инфраструктура, персонал, нематериальные ценности (например, репутация организации).

В результате проведения подготовительных этапов оценщик рисков получает детальную информационную структуру организации и способы ее использования.

2. Основные этапы:

2.1. анализ угроз, выявление уязвимых мест в защите, вероятность их реализации, потенциальный ущерб, который включает в себя непосредственные и отдаленные расходы по нейтрализации последствий реализации угрозы;

2.2. оценка рисков, которая в самом простом случае определяется как

произведение вероятности реализации риска на предполагаемый ущерб от его реализации;

2.3. выбор защитных мер и их денежная оценка с учетом расходов на закупку оборудования и расходы на внедрение и обучение персонала;

2.4. реализация и проверка выбранных мер на практике, их корректировка при необходимости;

2.5. оценка остаточного риска.

Выделяют следующие методы расчета рисков ИБ.

1. Уровень риска определяется путем *оценки степени соответствия определенному набору требований* к информационной безопасности. В качестве источников таких требований могут выступать как нормативно-правовые документы предприятия, касающиеся вопросов информационной безопасности (политика безопасности, регламенты, приказы, распоряжения), так и требования действующего российского законодательства со стороны руководящих документов, государственных и международных стандартов. При этом для более точной оценки степень соответствия может регулироваться весовым коэффициентом, показывающим, насколько важно выполнение рассматриваемого требования. Требования могут быть сгруппированы по блокам, тогда для каждого блока вычисляется средняя оценка уровня риска. Значения весовых коэффициентов и степени соответствия требованиям выбираются в диапазоне [0; 1], где 1 означает наиболее важное требование (соответственно полное соответствие требованию), 0 - наименее важное требование (соответственно полное несоответствие требованию).

2. Уровень риска базируется на определении *вероятности реализации атак, а также уровней их ущерба*. Значение риска вычисляется отдельно для каждой атаки и в общем случае представляется как произведение вероятности проведения атаки на величину возможного ущерба от этой атаки. Значение ущерба определяется собственником информационного ресурса, а вероятность атаки вычисляется группой экспертов, проводящих процедуру аудита. Вероятность в данном случае рассматривается как мера того, что в результате проведения атаки нарушители достигли своих целей и нанесли ущерб компании.

Во второй методике могут использовать количественные или качественные шкалы для определения величины риска информационной безопасности.

В первом случае для риска и всех его параметров берутся численные выражения: вероятность проведения атаки может выражаться числом в интервале [0,1], а ущерб от атаки - задаваться в виде денежного эквивалента материальных потерь, которые может понести организация в случае успешной атаки.

При использовании качественных шкал числовые значения заменяются на эквивалентные им понятийные уровни. Каждому понятийному уровню в этом случае будет соответствовать определенный интервал количественной шкалы оценки. Количество уровней может варьироваться в зависимости от

применяемых методик оценки рисков. В табл. 13 и 14 приведены примеры качественных шкал оценки рисков информационной безопасности, в которых для оценки уровней ущерба и вероятности атаки используется пять понятийных уровней.

Таблица 13

Качественная шкала оценки уровня ущерба

№	Уровень ущерба	Описание
1	Малый	Незначительные потери материальных активов, которые быстро восстанавливаются, или незначительные последствия для репутации компании
2	Умеренный	Заметные потери материальных активов или умеренные последствия для репутации компании
3	Средней тяжести	Существенные потери материальных активов или значительный урон репутации компании
4	Большой	Большие потери материальных активов и большой урон репутации компании
5	Критический	Критические потери материальных активов или полная потеря репутации компании на рынке, что делает невозможным ее дальнейшую деятельность

Таблица 14

Качественная шкала оценки вероятности проведения атаки

№	Вероятность атаки	Описание
1	Очень низкая	Атака практически никогда не будет проведена. Соответствует числовому интервалу вероятности [0, 0,25)
2	Низкая	Вероятность проведения атаки достаточно низкая. Соответствует числовому интервалу вероятности [0,25, 0,5)
3	Средняя	Вероятность проведения атаки приблизительно равна 0,5
4	Высокая	Атака скорее всего будет проведена. Соответствует числовому интервалу вероятности (0,5, 0,75]
5	Очень высокая	Атака почти наверняка будет проведена. Соответствует числовому интервалу вероятности (0,75, 1]

Для вычисления уровня риска по качественным шкалам применяются специальные таблицы, в которых в первом столбце задаются понятийные уровни ущерба, а в первой строке - уровни вероятности атаки (табл.15).

Таблица 15

Определение уровня риска информационной безопасности по качественной шкале

Ущерб	**Вероятность атаки**				
	очень низкая	низкая	средняя	высокая	очень высокая
Малый	Низкий риск	Низкий риск	Низкий риск	Средний риск	Средний риск
Умеренный	Низкий риск	Низкий риск	Средний риск	Средний риск	Высокий риск
Средней тяжести	Низкий риск	Средний риск	Средний риск	Средний риск	Высокий риск
Большой	Средний риск	Средний риск	Средний риск	Средний риск	Высокий риск
Критический	Средний риск	Высокий риск	Высокий риск	Высокий риск	Высокий риск

Отметим, что при расчете значений вероятности атаки, а также уровня возможного ущерба используют преимущественно статистические методы или экспертные оценки. При этом статистические методы предполагают анализ уже накопленных данных о реально случавшихся инцидентах, связанных с нарушением информационной безопасности. Однако статистические методы не всегда удается применить из-за недостатка статистических данных о ранее проведенных атаках на ресурсы рассматриваемой информационной системы или аналогичной ей.

Рассмотренные методики оценки риска могут применяться в ходе проведения аудита, который может быть *внутренним* (проводимым сотрудниками организации) и *внешним* (проводимым независимой организацией).

Под *аудитом* подразумевают анализ накопленной информации, проводимый оперативно, в реальном времени или периодически. Аудит подразумевает сравнение существующей системы защиты информации с эталонными требованиями, предъявляемыми международными стандартами.

В ходе проведения аудита часто используется *протоколирование* – сбор и накопление информации о событиях, происходящих в информационной системе. При этом рассматриваются следующие виды событий:

- *внешние* (вызванные действиями других сервисов);
- *внутренние* (вызванные действиями самого сервиса);

• *клиентские* (вызванные действиями пользователей и администраторов).

Задачами протоколирования и аудита являются:

• обеспечение подотчетности пользователей и администраторов;

• обеспечение возможности реконструкции последовательности событий, приведших к реализации угрозы;

• обнаружение попыток нарушений информационной безопасности;

• предоставление информации для выявления и анализа проблем.

В основном протоколируются следующие виды событий:

• вход в систему (успешный или нет);

• выход из системы;

• обращение к удаленной системе;

• операции с файлами (открыть, закрыть, переименовать, удалить);

• смена привилегий или иных атрибутов безопасности (режима доступа, уровня благонадежности пользователя и т.п.).

При протоколировании этих событий регистрируется также сопутствующая информация:

• дата и время события;

• уникальный идентификатор пользователя – инициатора действия;

• тип события;

• результат действия (успех или неудача);

• источник запроса (например, имя терминала);

• имена затронутых объектов (например, открываемых или удаляемых файлов);

• описание изменений, внесенных в базы данных защиты (например, новая метка безопасности объекта).

Отдельно стоит сказать об *активном аудите*, который обычно включается в систему защиты и представляет собой оперативный аудит с автоматическим реагированием на выявленные нештатные ситуации.

Задачей активного аудита является оперативное выявление подозрительной активности и предоставление средств для автоматического реагирования на нее. При этом под *подозрительной активностью* понимается поведение пользователя или компонента информационной системы, являющееся *злоумышленным* (в соответствии с заранее определенной политикой безопасности) или *нетипичным* (согласно принятым критериям). Так, например, за подозрительную активность может быть принята атака, направленная на незаконное получение правомочий: зафиксированы три последовательные неудачные попытки входа в систему с одного терминала, в результате происходит автоматическое блокирование терминала до выяснения ситуации. Также в качестве подозрительной активности могут быть рассмотрены действия, выполняемые в рамках имеющихся полномочий, но нарушающие политику безопасности (например, перемещение системных файлов на неучтенные носители информации).

Безусловно, в ходе проведения автоматического активного аудита

возможно возникновение ошибок. К ошибкам *первого рода* относят пропуск атак, в ошибках *второго рода* – ложные тревоги.

В основе любого аудита и оценки рисков информационной безопасности системы лежат соответствующие научные концепции и модели обеспечения информационной безопасности. Рассмотрим их подробнее.

1. Модели безопасности по разграничению доступа в систему.

1.1. *Модели предоставления прав:*

- *на основании дискретного доступа* – предоставляют пользователю право доступа к объекту на основании наличия у него так называемого «билета». К преимуществам этой модели относится простота, т.к. система защиты реализуется на основе матрицы доступа, однако модель не учитывает динамику изменения системы (затруднено внесение новых пользователей и новых объектов в матрицу);
- *на основании мандатного доступа* – накладывают ограничения на передачу прав доступа от одного пользователя к другому. Классической моделью мандатного доступа является *модель Белла-Лападула*, в которой все субъекты и объекты ассоциируются с уровнями безопасности, варьирующимися от низких уровней (неклассифицированных) до высоких (совершенно секретных). В модели присутствуют два правила: «нет чтения вверх» (т.е. субъект с низким уровнем доступа не может «прочитать» объект более высокого уровня) и «нет записи вниз» (т.е. субъект высокого уровня не может изменить объект более низкого уровня).

1.2. *Вероятностные модели* исследуют вероятность преодоления системы защиты за определенное время. Их задачей является минимизация вероятности преодоления системы защиты. Преимуществом этих моделей является числовая оценка стойкости системы защиты. К недостаткам можно отнести изначальное допущение того, что система защиты может быть вскрыта. Наиболее распространены следующие виды вероятностных моделей:

- *игровая модель* описывает процесс эволюции системы защиты в течение времени. При этом выделяются две активных роли – разработчика и злоумышленника. Задачей разработчика является создание первоначального варианта системы защиты. После этого злоумышленник начинает преодолевать систему защиты. Если к моменту времени, когда злоумышленник преодолел систему защиты, у разработчика нет нового варианта, то система защиты преодолена, а если нет - процесс продолжается сначала;
- *модель системы безопасности с полным перекрытием* основывается на аксиоме: система должна иметь хотя бы одно средство для обеспечения безопасности на каждом возможном пути проникновения в систему.

1.3. *Модели, основанные на принципах теории информации К. Шеннона,* определяют ограничения на отношения ввода/вывода системы. Выделяют следующие виды этих моделей:

- *модель невмешательства*, при этом основным постулатом модели является положение, при котором ввод высокоуровневого пользователя не

может смешиваться с выводом низкоуровневого (т.н. «невмешательство»). Рассматриваемая система состоит из объектов: высокий ввод, низкий ввод, высокий вывод, низкий вывод;

- *модель невыводимости* определяется терминами «пользователь» и «информация», связанными с одним из двух возможных уровней секретности (высоким и низким). Система считается невыводимо безопасной, когда пользователи с низкими уровнями безопасности не могут получить информацию с высоким уровнем безопасности в результате любых действий пользователей с высоким уровнем безопасности.

2. **Модели контроля целостности информации в системе** в основном представлены моделями Биба:

2.1.*мандатная модель целостности* строится на следующих правилах: «нет чтения снизу», т.е. вводится запрет субъектам на чтение информации из объекта с более низким уровнем целостности; «нет записи наверх», т.е. субъектам запрещено записывать информацию в объект с более высоким уровнем целостности;

2.2.*модель понижения уровня субъекта* строится на правиле: субъекту разрешается осуществлять чтение снизу, но в результате такого чтения уровень целостности субъекта понижается до уровня целостности объекта. Мотивом для введения такого правила является то, что субъекты с высокой целостностью рассматриваются как чистые. Когда к чистому субъекту попадает информация из менее чистого источника, субъект «портится» и его уровень целостности должен быть соответственно изменен;

2.3.*модель понижения уровня объекта* разрешает запись наверх, но снижает уровень целостности объекта до уровня целостности субъекта, осуществлявшего запись.

3. **Модель защиты при отказе в обслуживании** применяется в ситуации, когда зарегистрированным пользователям не предоставляется запрашиваемая услуга. Основным параметром этой модели является *максимальное время ожидания* (MWT) - длина промежутка времени после запроса услуги, в течение которого считается приемлемым предоставление этой услуги. В случае применения мандатной модели контроля доступа к системе модель дополняется следующими положениями:

- субъектам системы соответствуют приоритеты;
- субъект может требовать услугу у вычислительной системы, запрашивая доступ к объектам системы;
- субъект получает отказ в обслуживании, если его запрос зарегистрирован, но не удовлетворен в течение соответствующего MWT;
- один субъект может отказать в обслуживании другому субъекту.

4. **Модель анализа безопасности программного обеспечения** основываются на объектно-ориентированном подходе, т.е. класс программ связан с классами алгоритмов и данных отношением наследования. Наследование – это такое отношение между классами, когда один класс повторяет структуру и поведение другого. Следовательно, к программам

применимы те же операции, что к данным (чтение и запись) и алгоритмам (модификация), а также дополнительная специфическая операция – выполнение. Однако программы, присутствующие в вычислительной системе, не являются однотипными. С точки зрения анализа безопасности можно выделить по крайней мере два класса, связанных с классом программ отношением включения: прикладные и системные программы. Отдельно в системе могут присутствовать *разрушающие программные сущности (РПС)* - сущности, обладающие определенной структурой и свойствами, вступающие во взаимодействие с другими элементами системы (программы и данные). Для их определения используются понятия легитимных и нелегитимных действий.

Легитимные действия - действия программы или пользователя, не приводящие к ущербу безопасности и целостности системы.

Нелегитимные действия - действия программы или пользователя, наносящие ущерб безопасности или целостности системы.

Для РПС характерно нелегитимное использование ресурсов, нелегитимный доступ к данным и нелегитимный запуск программ. Обычно в качестве РПС в этой модели рассматриваются:

- вирусы;
- «троянские кони;
- программы-взломщики систем защиты и средств разграничения доступа.

Задания к контрольной (лабораторной) работе

Уровни информационной безопасности

Для заданного варианта составьте характеристику предприятия с точки зрения информационной безопасности согласно приведенному ниже плану. Крайне желательно, чтобы характеристика была дана реальному предприятию в этой сфере деятельности. Характеристику оформить в виде текстового документа в электронном виде.

Сфера деятельности предприятия

0. Торгово-производственное предприятие
1. Интернет-магазин
2. Предприятие, занимающееся предоставлением IT-услуг
3. Банковская организация с несколькими филиалами
4. Строительная организация
5. Торговое предприятие, имеющее сеть магазинов в разных городах региона
6. Агентство недвижимости
7. Сеть предприятий общественного питания
8. Сеть гостиничных комплексов
9. Сеть салонов красоты

Вариант соответствует последней цифре шифра зачетной книги.

План характеристики

1. Название предприятия, количество филиалов (торговых точек, офисов и т.д.) и их расположение.
2. Дата основания предприятия, наличие конкурентов в данном сегменте рынка.
3. Перечень сведений конфиденциального характера, обрабатываемых на предприятии.
4. Перечислить меры по защите информации законодательного уровня ИБ.
5. Административный уровень ИБ: перечень внутренних организационно-распорядительных документов, способствующих защите информации. Наличие политики безопасности и ее структура на предприятии.
6. Процедурный уровень ИБ (заполнить табл. 16).

Таблица 16

Характеристика процедурного уровня ИБ предприятия

Категория	Проводимые мероприятия	Ответственное лицо	Периодичность проведения и результат
Управление персоналом			
Физическая защита			
Поддержание работоспособности			
Планирование восстановительных работ			

7. Выделите сервисы безопасности, действующие на предприятии (заполнить табл. 17, указав не менее 2-3 сервисов каждой группы).

Таблица 17

Характеристика программно-технического уровня ИБ предприятия

Категория	Назначение сервиса	Наименование программно-технического комплекса, реализующего сервис
Превентивный		
Обнаружение нарушений		
Локализующий		
Выявление нарушителя		
Восстановление режима безопасности		

Задание лабораторной работы

Управление рисками информационной безопасности на предприятии

На основании предприятия, рассмотренного выше, выясните, какие из принципов архитектурной безопасности соблюдаются на предприятии, а какие – нет. Как это влияет на эффективность функционирования системы защиты? Привести примеры возможных нарушений ИБ.

Проведите этапы процесса управления рисками по приведенному ниже плану.

1. Назовите основные активы предприятия с точки зрения ИБ.

2. По каждой группе активов укажите:

2.1. основные угрозы ИБ и вероятность и реализации;

2.2. уязвимые места в организации системы ИБ, благодаря которым возможна реализация угроз;

2.3. потенциальный ущерб предприятию (в денежном эквиваленте) в ходе реализации каждой из угроз.

3. Оцените уровень рисков для предприятия с точки зрения ИБ:

3.1. для вариантов 1, 3, 6 – используйте методику, основанную на оценке соответствия требованиям одного из рассмотренных в третьей части методических указаний стандарта ИБ;

3.2. для вариантов 0, 5, 7, 8 – используйте методику, основанную на определении вероятности реализации угроз с помощью количественной шкалы;

3.3. для вариантов 2, 4, 9 – используйте методику, основанную на определении вероятности реализации угроз с помощью качественной шкалы.

Модели противодействия угрозам безопасности

Используя теоретический материал, изложенный в методических указаниях к выполнению работы, а также ресурсы сети Интернет, выполните задания (номер варианта определяется по последней цифре зачетной книжки).

Варианты

0. Составьте матрицу доступа к элементам информационной системы для модели предоставления прав на основании дискретного доступа (рассмотреть не менее трех групп пользователей и четырех-пяти элементов системы). Каковы основные преимущества и недостатки этой модели?

1. Составьте модель мандатного доступа на основании модели Белла-Лападула (рассмотреть не менее трех групп пользователей и четырех-пяти элементов системы). На основании модели проиллюстрируйте правила «нет чтения вверх» и «нет записи вниз». Почему было необходимо ввести эти правила?

2. На примере предприятия, рассмотренного вашей группой, на основе одной из выявленных угроз составьте игровую модель эволюции системы защиты. Экспертным путем определите вероятность реализации угрозы и ущерб от реализации угрозы на каждом этапе.

3. На примере предприятия, рассмотренного вашей группой, составьте модель

системы безопасности с полным перекрытием. Оцените уровень издержек на внедрение и поддержание системы защиты информации.

4. На примере интернет-магазина рассмотрите модели защиты данных магазина при отказе в обслуживании. Определите MWT, группы пользователей и их приоритеты при запросе информации. Составьте блок-схему функционирования модели.

5. Составьте модель невыводимости (рассмотреть не менее трех групп пользователей и четырех-пяти элементов системы). Проиллюстрируйте на конкретном предприятии, почему составленная вами система считается невыводимо безопасной. При нарушении каких правил эксплуатации это требование может быть нарушено?

6. Составьте мандатную модель целостности Биба (рассмотреть не менее трех групп пользователей и четырех-пяти элементов системы). На основании модели проиллюстрируйте правила «нет записи наверх» и «нет чтения снизу». Почему было необходимо ввести эти правила? Чем они отличаются практически от правил модели Белла-Лападула?

7. Составьте модели понижения уровня субъект и понижения уровня объекта Биба (рассмотреть не менее трех групп пользователей и четырех-пяти элементов системы). На основании модели проиллюстрируйте основные положения моделей. Составьте блок-схемы функционирования моделей.

8. Составьте модель невмешательства для доступа к элементам системы интернет-магазина. Назовите основные объекты системы. Назовите основные требования, при соблюдении которых пользователями возможна реализация модели.

9. Составьте модель анализа безопасности программного обеспечения, установленного в информационной системе предприятия. По каким параметрам будет оцениваться, является ли программное обеспечение разрушающей программной сущностью? Составьте блок-схему модели.

Задания для самостоятельной работы

1. Назовите и кратко охарактеризуйте уровни информационной безопасности на предприятии.
2. Приведите примеры норм, формирующих законодательный уровень ИБ.
3. Назовите основные цели административного уровня ИБ.
4. Дайте определение политике безопасности.
5. Дайте краткую характеристику каждого уровня политики безопасности.
6. Приведите по два примера мер безопасности, входящих в категории процедурного уровня ИБ.
7. Назовите основные сервисы программно-технического уровня.
8. Выделите категории сервисов программно-технического уровня и приведите конкретные примеры для каждого вида сервиса.
9. Назовите принципы архитектурной безопасности информационных систем и дайте их краткую характеристику.
10. Охарактеризуйте политику безопасности и метки объектов с точки

зрения критериев защищенности информационных систем.

11. Охарактеризуйте идентификацию и аутентификацию с точки зрения критериев защищенности информационных систем.
12. Охарактеризуйте регистрацию и учет с точки зрения критериев защищенности информационных систем.
13. Охарактеризуйте контроль функционирования средств защиты и непрерывность защиты с точки зрения критериев защищенности информационных систем.
14. Дайте определение управлению рисками.
15. Дайте характеристику основным действиям, которые возможно выполнять над рисками.
16. Назовите этапы управления рисками.
17. Дайте характеристику методу оценки уровня риска по степени соответствия определенному набору требований.
18. Дайте характеристику методу оценки уровня риска по вероятности реализации атак.
19. Приведите примеры использования количественных и качественных шкал для определения величины риска ИБ.
20. Дайте определение понятию «аудит» и назовите его виды.
21. Приведите примеры внешних, внутренних и клиентских событий, рассматриваемых при протоколировании.
22. Назовите задачи протоколирования и аудита, а также виды протоколируемых событий.
23. Дайте определению понятию «активный аудит» и назовите его задачи.
24. Назовите виды ошибок, допускаемых в ходе проведения автоматического активного аудита.
25. Дайте краткую характеристику моделям предоставления прав. Каковы преимущества и недостатки этих моделей.
26. Дайте краткую характеристику вероятностным моделям. Каковы преимущества и недостатки этих моделей.
27. Дайте краткую характеристику моделям, основанным на принципах теории информации К. Шеннона.
28. Дайте краткую характеристику моделям целостности информации в системе (моделям Биба).
29. Дайте характеристику модели защиты при отказе в обслуживании.
30. Дайте характеристику модели анализа безопасности программного обеспечения.

Тема 5. Техническое и методическое обеспечение информационной безопасности

Цели:

1.1. рассмотреть основные виды средств защиты информации;

1.2. получить представление о комплексном подходе к информационной безопасности объектов предприятия;

1.3. получить навыки организации противодействия технической разведке на предприятии.

Методические указания к выполнению лабораторной работы

При создании комплексной системы защиты информации применяются различные виды средств защиты.

Физические средства защиты представляют собой разнообразные устройства, приспособления, конструкции, аппараты, предназначенные для создания препятствий на пути движения злоумышленников. Они решают следующие задачи защиты информации на предприятии:

- охрана территории предприятия и наблюдение за ней;
- охрана внутренних помещений и контроль за ними;
- охрана оборудования, продукции, финансов и информации;
- осуществление контролируемого доступа в здания и помещения.

Выделяют следующие категории физических средств защиты информации:

- *средства обнаружения* (охранное телевидение и сигнализация);
- *средства предупреждения* (заборы и т.п., усиление дверей и стекол);
- *средства ликвидации* (средства пожаротушения).

По физической природе и функциональному назначению все физические средства защиты информации подразделяются на:

- *охранные системы*, которые позволяют обнаружить различные угрозы ИБ (проникновение на объект, пронос/вынос оружия и средств промышленного шпионажа (т.н. «жучков»), кража материальных ценностей и денежных средств) и оповестить охранников о появлении этих угроз;
- *охранное телевидение* позволяет зафиксировать режим охраны объекта, контролировать обстановку вокруг объекта, а также вести скрытое наблюдение и предоставить видеозапись для последующего анализа правонарушения;
- *охранное освещение*, которое подразделяется на *дежурное* (используется в нерабочие часы предприятия для удобства сотрудников охраны) и *тревожное* (включается при поступлении сигнала тревоги от сигнализации);
- *средства физической защиты* представляют собой различные ограждения периметра объекта. К ним относятся: различные способы защиты окон (решетки, закаленные стекла, датчики, реагирующие на удар и т.д.), средства защиты компьютеров от хищения и проникновения к его внутренним компонентам (электронные замки и встроенные «шредеры», которые при попытке вскрыть кожух системного блока осуществляют резервное копирование информации и форматируют жесткий диск), различного рода

запирающие устройства, системы контроля доступа в помещения организации (могут быть атрибутивные (на основе ввода пароля или использования различного рода карт) и биометрические (на основании физиологической информации о субъекта: сетчатка глаза, отпечатки пальцев, анализ голосовой информации, почерка и т.д.).

Аппаратные средства защиты представляют собой технические конструкции, обеспечивающие защиту от утечки и противодействие несанкционированному доступу к источникам конфиденциальной информации. Данный вид средств защиты решает следующие задачи:

- проведение специальных исследований производственной деятельности на наличие возможных каналов утечки информации;
- выявление каналов утечки информации на разных объектах и в помещениях предприятия;
- локализация каналов утечки информации;
- поиск и обнаружение средств промышленного шпионажа;
- противодействие несанкционированному доступу к источникам конфиденциальной информации.

По функциональному назначению аппаратные средства подразделяются на следующие виды:

- *средства обнаружения* – отвечают за поиск и локализацию уже внедренных средств несанкционированного доступа к информации (т.н. «жучков»);
- *средства поиска и детальных измерений* – выявляют каналы утечки информации путем сопоставления допустимых показателей излучения и реальной ситуации (в том числе как *прямые* каналы утечки информации: аудиовизуальные каналы, вибрации; так и *побочные*: электромагнитные излучения от мониторов компьютеров, системных блоков);
- *средства активного и пассивного противодействия технической разведке* – позволяют путем генерации различных шумов искажать исходные сигналы излучений.

Программные средства защиты информации представляют собой программные комплексы, решающие различные задачи по защите информации. Они могут устанавливаться как на серверные компьютеры, так и на отдельные компьютеры пользователей. Примерный перечень видов программных средств приведен в таблице 18.

Программные средства используются в следующих направлениях, решая соответствующие задачи:

- *защита информации от несанкционированного доступа* - идентификация и аутентификация пользователей в информационной системе; разграничение доступа к ресурсам вычислительной сети; контроль и регистрация действий пользователей с программами и данными в них; использование элементов криптографии; блокировка компьютера на время отсутствия пользователя;
- *защита информации и программ от копирования* – затруднение считывания скопированной информации (например, за счет нестандартной

разметки носителя или криптографической защиты информации); создание препятствий к непосредственному использованию скопированного объекта (например, с помощью блока контроля среды размещения программы, учитывающего все характеристики компьютера, на котором открывается программа или файл, или с помощью usb-ключей);

- *защита программ и данных от вирусов*;
- *программная защита каналов связи* – организация защищенных каналов передачи информации как внутри сети, так и между сетями (VPN-сети); контроль входящего и исходящего трафика (файерволлы, средства аудита трафика); шифрование трафика (программные комплексы, работающие на основе криптографии).

Таблица 18

Характеристика средств программной защиты информации

Вид средств защиты	**Назначение**
Средства собственной защиты	Сопровождают продажу программного обеспечения и препятствуют незаконным действиям
Средства защиты в составе вычислительной системы	Защищают аппаратуру, диски и ресурсы вычислительной сети
Средства защиты с запросом информации	Идентифицируют полномочия пользователей путем затребования для своей работы ввода дополнительной информации
Средства активной защиты	Инициируются при вводе неправильного пароля, попытках доступа к информации без разрешения и пр.
Средства пассивной защиты	Направлены на предостережение, контроль, поиск улик и доказательств с целью раскрытия преступления

Отдельно стоит отметить, что при криптографической защите информации применяются различные методы шифрования в зависимости от объекта шифрования. Так, при шифровании *речи* используются скремблеры или речевые шифраторы (переставляют отдельные вырезки входного сигнала) и маскираторы (заменяют входной сигнал цифровой передачей данных). При шифровании *данных*, передаваемых по сетям используются такие методы как перестановка (подблоки внутри каждого блока информации меняются местами) и замещение (подблоки входных данных заменяются согласно заданному алгоритму).

Комплексный подход к информационной безопасности объектов подразумевает под собой проведение ряда мероприятий с использованием упомянутых выше средств защиты информации.

1. Исследование и анализ возможных технических каналов утечки информации ограниченного доступа из помещений объекта (с использованием побочных электромагнитных излучений).

2. Разработка моделей доступности для злоумышленников защищаемых объектов с помощью технического проникновения.

3. Проведение мероприятий в помещениях, автомашинах организации и ее работников работ по обнаружению средств негласного получения информации (т.н. «жучков») и каналов утечки речевой информации.

4. Контроль радиоэфира во время ответственных совещаний и переговоров с целью выявления «жучков».

5. Работы по устранению выявленных технических каналов утечки информации:

а) приведение в негодность средств негласного получения информации;

б) защита телефонных аппаратов организации от прослушивания;

в) защита компьютеров от утечки обрабатываемой информации за счет побочных электромагнитных излучений;

г) защита компьютерных сетей с помощью криптографических методов;

д) организация приема и передачи электронной почты в зашифрованном виде;

е) защита стен, потолков, окон, систем отопления и вентиляции от съема речевой информации по виброакустическому каналу.

6. Установка в помещении специальной аппаратуры:

а) сигнализирующей о наличии в помещении работающих «жучков»;

б) сигнализирующей о несанкционированном подключении к телефонным линиям;

в) генераторов радиоакустических и виброакустических помех;

г) разработка организационно-технических мер по предотвращению появления технических каналов утечки информации.

7. Проведение профилактических проверок помещений на наличие принесенных «жучков».

8. Обучение сотрудников фирмы и службы безопасности работе с конкретными средствами.

9. Оборудование офисов, квартир, дач, автомобилей сотрудников современными системами видеонаблюдения, аппаратурой подавления радиовзрывателей и «жучков».

Следует отметить, что целесообразность проведения тех или иных мероприятий зависит от масштабов организации и ценности циркулирующей конфиденциальной информации для конкурентов.

Задания лабораторной работы

Анализ современного рынка средств защиты информации

Используя ресурсы сети Интернет, выполните задания.

1. Заполните таблицу 19. Графы принцип действия и стоимость заполняются для каждого вида средств защиты.

Таблица 19

Характеристика физических средств защиты информации

Название категории	Виды	Принцип действия	Стоимость
Охранная сигнализация			
Детекторы оружия			
Детекторы жучков			
Защита окон			
Атрибутивные системы контроля доступа			
Биометрические системы контроля доступа			

2. Заполните таблицу 20. Для каждой категории аппаратных средств выберите одно устройство, опишите его функциональные возможности и цену.

Таблица 20

Характеристика аппаратных средств защиты

Категория	Пример устройства	Функциональные возможности	Стоимость
Средства обнаружения			
Средства поиска и детальных измерений			
Средства активного и пассивного противодействия технической разведке			

3. Для каждого направления использования программных средств выберите задачу защиты информации и приведите пример программного средства. Укажите, входит ли оно в штатный комплект операционной системы, распространяется бесплатно или в коммерческих целях (в этом случае укажите стоимость лицензии).

4. Согласно таблице 18, для каждого вида средств защиты приведите пример используемого программного средства. В случае коммерческого распространения продукта, укажите стоимость его лицензии.

Используя данные рейтингов антивирусных программ, а также данные официального сайта, охарактеризуйте антивирусные средства Kaspersky Internet Security, Dr.Web Security Space, Avast! Internet Security, Avira Premium Security Suite (плюс еще один программный продукт на Ваш выбор) по приведенным ниже критериям. Результат представьте в виде таблицы. По окончании таблицы выберите наиболее удачный антивирус и обоснуйте Ваш выбор.

Критерии:

а) стоимость;
б) поддерживаемые операционные системы;
в) надежность и удобство работы;
г) качество обнаружения вирусов;
д) сканирование архивов;
е) возможность лечения зараженных объектов;
ж) отсутствие ложных срабатываний;
з) периодичность обновления антивирусных баз;
и) дополнительные возможности;
к) место в рейтинге антивирусов (указать ссылку на сайт с рейтингом).

Организация противодействию технической разведке на предприятии

1. На примере предприятия, рассмотренного в четвертой части методических указаний, выберите соответствующие защитные меры для нейтрализации угроз, вызывающих наибольшие риски, и оцените стоимость их внедрения на предприятии.

2. Используя методологию комплексного подхода к обеспечению информационной безопасности, составьте план мероприятий по защите информации на рассматриваемом предприятии. Результат оформите в виде таблицы 21.

Таблица 21

Примерная форма плана мероприятий по защите информации

Направление защиты	Мероприятия	Привлекаемые программно-аппаратные средства	Ответственные за проведение лица
Исследование и анализ возможных каналов утечки информации ограниченного доступа из помещений объекта			
Устранение выявленных каналов утечки информации			
Обучение сотрудников фирмы и службы безопасности работе со средствами защиты информации			

Задания для самостоятельной работы

1. Охарактеризуйте физические средства защиты информации и обозначьте задачи, которые они решают.

2. Назовите категории физических средств защиты информации. Приведите примеры соответствующих средств каждой категории.

3. Назовите виды физических средств защиты информации, выделяемые по физической природе и функциональному назначению. Приведите примеры средств защиты соответствующих видов.

4. Назовите виды охранных систем и кратко охарактеризуйте принцип их действия.

5. Приведите схему функционирования охранного телевидения.

6. Назовите способы защиты окон от проникновения злоумышленников.

7. Приведите виды средств контроля доступа в помещения организации и дайте краткую характеристику механизмов их функционирования.

8. Охарактеризуйте аппаратные средства защиты информации и назовите задачи, которые решают эти средства.

9. Назовите виды аппаратных средств защиты информации по функциональному назначению и приведите примеры средств защиты на каждый вид.

10. Назовите направления использования программных средств защиты информации. Приведите примеры соответствующих программных продуктов.

11. Приведите краткую характеристику средств программной защиты информации и примеры соответствующих программных продуктов.

12. Назовите способы шифрования речи.

13. Назовите способы шифрования данных, передаваемых по сетям.

14. Приведите примеры мероприятий, проводимых в рамках комплексного подхода к информационной безопасности объектов предприятия.

15. Назовите средства защиты информации (по одному на каждый вид), который вы используете для защиты информации на вашем домашнем рабочем месте.

Самостоятельная (аудиторная и внеаудиторная) работа обучающихся является одним из основных видов познавательной деятельности, направленной на более глубокое и разностороннее изучение материалов учебной дисциплины и включает: обязательное ведение конспектов лекций; подготовку выступлений (сообщений, докладов) к практическим занятиям, семинарам; подготовку письменных контрольных работ (реферата, эссе, презентации).

Результаты выполнения самостоятельной работы представляются обучающимися во время аудиторных занятий, проверяются и оцениваются преподавателем в ходе аудиторных занятий, текущего (рубежного) контроля и промежуточной аттестации.

Для повышения эффективности самостоятельной работы обучающимся рекомендуется пользоваться расширенным поиском в национальном цифровом ресурсе РУКОНТ – межотраслевой электронной библиотеке. Доступ к ресурсу осуществляется на сайте: http://www.rucont.ru

Важной формой самостоятельной исследовательской работы, углубленного изучения той или иной проблемы учебного курса является подготовка и написание рефератов и эссе. Данная форма самостоятельной

работы является важным элементом подготовки обучающихся к оформлению и написанию дипломной работы.

Виды самостоятельной работы:

- поиск и изучение нормативных правовых актов, в том числе с использованием электронных баз данных;
- поиск и изучение научной литературы, в том числе с использованием сети Интернет;
- решение задач из практикума;
- подготовка рефератов, докладов, эссе, презентаций;

Модель (особенности) самостоятельной работы обучающихся по отдельным разделам и темам курса:

- составление проектов профессиональных документов;
- обобщение материалов профессиональной практики по определенным вопросам;
- подготовка к проведению ролевой игры;
- подготовка для обсуждения дискуссионных вопросов;
- составление схем, сравнительных таблиц;
- решение практических ситуаций;
- подготовка к практическим занятиям.

8. Методические рекомендации для преподавателя. Образовательные технологии

Перед началом изучения дисциплины (на первом занятии) преподаватель обязан сообщить обучающимся порядок освоения тем (разделов) дисциплины, сроки и формы отчетностей, процедуры оценки системы учета уровня сформированности компетенций. Преподавание ведется методом комплексного и системно-проблемного изучения проблемных явлений и процессов, а также анализа их последствий применительно к современной профессиональной практике. Изложение материала должно строиться как с использованием теоретической подачи материала в виде лекций, так и в виде проведения семинаров (практических занятий). В ходе лекционных занятий рекомендуется использовать презентационные материалы (слайды).

На лекциях излагаются основные актуальные проблемы, раскрываются наиболее сложные вопросы дисциплины, активизируется мыслительная деятельность путем постановки проблемных вопросов и вовлечения, обучаемых в их решение, развиваются их творческие способности.

В ходе семинарских и практических занятий для реализации компетентностного подхода рекомендуется использование активных и интерактивных форм обучения (решения задач, деловых и ролевых игр, разбора конкретных ситуаций) в сочетании с внеаудиторной самостоятельной работой (подготовка устных выступлений (докладов, сообщений), что позволит углубить понимание наиболее сложных теоретических и прикладных проблем, рассмотренных в ходе лекций, и сформировать навыки и умения использования необходимых нормативных правовых актов для регулирования профессиональных ситуаций.

Преимущественной формой текущего контроля успеваемости обучающихся является тестирование, которое должно быть обязательным и которым должно быть завершено изучение каждого раздела учебной программы дисциплины.

При подготовке обучающихся к промежуточной аттестации необходимо провести консультацию по курсу и акцентировать внимание обучающихся на использовании рекомендованной основной и дополнительной литературы, содержания конспектов лекций, а также необходимости составления тезисов ответов на вопросы, выносимые на зачет.

9. Обеспечение доступности освоения программы обучающимися с ограниченными возможностями здоровья.

Условия организации и содержание обучения и контроля знаний обучающихся с ограниченными возможностями здоровья (далее – ОВЗ) определяются программой дисциплины, адаптированной при необходимости для обучения указанных обучающихся.

Организация обучения, текущей и промежуточной аттестации обучающихся с ОВЗ осуществляется с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся. Исходя из психофизического развития и состояния здоровья обучающихся с ОВЗ, организуются занятия совместно с другими обучающимися в общих группах, используя социально-активные и рефлексивные методы обучения создания комфортного психологического климата в учебной группе или, при соответствующем заявлении такого обучающегося, по индивидуальной программе, которая является модифицированным вариантом основной рабочей программы дисциплины. При этом содержание программы дисциплины не изменяется. Изменяются, как правило, формы обучения и контроля знаний, образовательные технологии и учебно-методические материалы.

Обучение лиц с ОВЗ также может осуществляться индивидуально и/или с применением элементов электронного обучения. Электронное обучение обеспечивает возможность коммуникаций с преподавателем, а также с другими обучаемыми посредством вебинаров (например, с использованием программы Skype), что способствует сплочению группы, направляет учебную группу на совместную работу, обсуждение, принятие группового решения. В образовательном процессе для повышения уровня восприятия и переработки учебной информации обучающимися с ОВЗ применяются мультимедийные и специализированные технические средства приема-передачи учебной информации в доступных формах для обучающихся с различными нарушениями, обеспечивается выпуск альтернативных форматов печатных материалов (крупный шрифт), электронных образовательных ресурсов в формах, адаптированных к ограничениям здоровья обучающихся, наличие необходимого материально-технического оснащения. Подбор и разработка учебных материалов производится преподавателем с учетом того, чтобы обучающиеся с нарушениями слуха получали информацию визуально, с нарушениями зрения – аудиально (например, с использованием программ-синтезаторов речи).

Для осуществления процедур текущего контроля успеваемости и промежуточной аттестации обучающихся лиц с ОВЗ фонд оценочных средств по дисциплине, позволяющий оценить достижение ими результатов обучения и уровень сформированности компетенций, предусмотренных учебным планом и рабочей программой дисциплины, адаптируется для лиц с ограниченными возможностями здоровья с учетом индивидуальных психофизиологических особенностей (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п.). При необходимости

обучающимся предоставляется дополнительное время для подготовки ответа при прохождении всех видов аттестации.

Особые условия предоставляются обучающимся с ограниченными возможностями здоровья на основании заявления, содержащего сведения о необходимости создания соответствующих специальных условий.

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

1.1. Перечень компетенций и индикаторов достижения компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Перечень формируемых компетенций (код и содержание)	Код индикатора достижения компетенции	Этапы формирования компетенций в процессе освоения образовательной программы	
		дисциплины/ практики	семестр
1	*2*	*3*	*4*
ПК-2	ПК-2.2	Экономическая безопасность	7
	ПК-2.2	Практика по профилю профессиональной деятельности	8
	ПК-2.2	Бухгалтерские информационные системы	9
	ПК-2.2	Информационная безопасность	9
	ПК-2.2	Подготовка к процедуре защиты и защита выпускной квалификационной работы	10
	ПК-2.2	Подготовка к сдаче и сдача государственного экзамена	10
	ПК-2.2	Преддипломная практика	10
	ПК-2.2	Проекты и проектная деятельность	10
ПК-5	ПК-5.2	Бухгалтерский учет	5
	ПК-5.2	Экономика организации (предприятия)	5
	ПК-5.2	Экономика организации (предприятия)	6
	ПК-5.2	Аудит	7
	ПК-5.2	Экономика организаций сферы услуг	7
	ПК-5.2	Экономика финансовой сферы	7
	ПК-5.2	Контроль и ревизия	8
	ПК-5.2	Экономика организаций сферы услуг	8
	ПК-5.2	Экономика финансовой сферы	8
	ПК-5.2	Бухгалтерские информационные системы	9
	ПК-5.2	Информационная безопасность	9

	ПК-5.2	Экономика и управление в бюджетной сфере	9
	ПК-5.2	Экономика потребительской кооперации	9
	ПК-5.2	Подготовка к процедуре защиты и защита выпускной квалификационной работы	10
	ПК-5.2	Преддипломная практика	10

1.2 Этапы формирования компетенций и оценочные материалы для проверки хода освоения дисциплины и достижения планируемых результатов обучения.

Перечень формируемых компетенций (код и содержание)	Перечень формируемых индикаторов достижений компетенций (код и содержание)	Этапы формирования компетенций (з, у)	Оценочные средства	Темы дисциплины, обеспечивающие этапы формирования компетенции
ПК-2 – Способен проводить анализ возможных экономических рисков и давать им оценку, составлять и обосновывать прогнозы динамики развития основных угроз экономической	ПК-2.2 Проводит комплексный анализ угроз экономической безопасности при планировании и	**Знает:** -основные принципы обеспечения безопасности информационной системы -сущности информационной безопасности и защиты	ВЗ, ЛР	Темы 1-5

безопасности	осуществлении инновационных проектов	информации, их места в системе национальной безопасности; нормативных правовых актов в области защиты государственной тайны и информационной безопасности; режимы секретности.		
		Умеет: -применять нормативные правовые акты в области защиты информации и учитывать их при создании систем экономической безопасности хозяйствующих субъектов -разрабатывать и применять нормативно-методические материалы по регламентации процессов обработки, хранения и защиты конфиденциальных документов с учетом нормативных правовых актов в области защиты государственной тайны и информационной безопасности с	ВЗ, ЛР	Темы 1-5

		учетом соблюдения необходимого режима секретности		
ПК-5 Способен проводить оценку и интерпретацию полученных, в ходе экономического обоснования финансовых результатов	ПК-5.2 Разрабатывает аналитические материалы (отчеты) о финансово-хозяйственной деятельности по результатам оценки финансовых показателей	**Знает:** -основные угрозы информационной безопасности и их классификацию в процессе осуществления финансово-хозяйственной деятельности	ВЗ, ЛР	Темы 1-5
		Умеет: -строить модель актуальных угроз на основе предоставленных сведениях и процессах информационной системы организации в процессе осуществления финансово-хозяйственной деятельности	ВЗ, ЛР	Темы 1-5

ВЭ - Вопросы к зачету;
ЛР - Защита лабораторных работ

Раздел 2. Содержание фонда оценочных средств для текущего контроля и промежуточной аттестации

2.1. Оценочные материалы: текущий контроль

Текущий контроль знаний предусматривает проверку качества получаемых обучающимися умений и знаний.

Основные методы контроля, позволяющие оценить знания и умения в рамках приобретенных компетенций: вопросы собеседования по итогам выполнения лабораторных занятий и контрольной работы.

2.1.1 Вопросы собеседования по итогам выполнения лабораторных занятий

Тема 3. Организационно-правовое обеспечение информационной безопасности

Лабораторная работа 1-6

1. Основные нормативные документы по защите информации
2. Назовите причины появления уязвимостей.
3. Перечислите и кратко охарактеризуйте элементы управления непрерывностью бизнеса.
4. Дайте определения следующим понятиям: «журнал аудита», «биометрия», «классификация», «политика ИБ», «цифровая подпись», «межсетевой экран», «принцип необходимого знания», «средства идентификации», «уязвимость».
5. Назовите назначение политики ИБ и приведите обязанности сотрудников по ее выполнению различных категорий.
6. Что относится к инцидентам ИБ? Какова должна быть реакция руководителей предприятия на инциденты?
7. Назовите выделяемые классы защищенности информации.
8. Перечислите показатели защищенности информации и дайте их краткую характеристику.
9. Какова область применения выделяемых показателей?
10. Дайте определение понятиям «межсетевой экран», «экранирование».
11. Перечислите показатели защищенности межсетевых экранов и дайте их краткую характеристику.
12. Назовите основные каналы утечки информации.
13. Каковы основные источники угроз персональным данным?
14. Перечислите показатели исходной защищенности ИСПДн.
15. Объясните суть подхода к составлению перечня актуальных угроз. Выделите основные этапы методики и представьте их в виде схемы.
16. Приведите примеры 2-3 руководящих документов в области защиты информации и опишите кратко их назначение.
17. Назовите основные правила построения системы информационной безопасности предприятия.
18. Охарактеризуйте кратко основные принципы защиты информации на предприятии.
19. Перечислите основные методы обеспечения безопасности процессов переработки информации.
20. Назовите основные технологии предотвращения угроз информационной безопасности.
21. Приведите примеры технологий парирования и нейтрализации угроз ИБ и привлекаемых программно-аппаратных средств.
22. Перечислите основные организационные мероприятия по защите информации на предприятии.

Тема 4. Модели и системы обеспечения информационной безопасности деятельности организаций

Лабораторные работы 7-12

1. Назовите и кратко охарактеризуйте уровни информационной безопасности на предприятии.
2. Приведите примеры норм, формирующих законодательный уровень ИБ.
3. Назовите основные цели административного уровня ИБ.
4. Дайте определение политике безопасности.
5. Дайте краткую характеристику каждого уровня политики безопасности.

6. Приведите по два примера мер безопасности, входящих в категории процедурного уровня ИБ.
7. Назовите основные сервисы программно-технического уровня.
8. Выделите категории сервисов программно-технического уровня и приведите конкретные примеры для каждого вида сервиса.
9. Назовите принципы архитектурной безопасности информационных систем и дайте их краткую характеристику.
10. Охарактеризуйте политику безопасности и метки объектов с точки зрения критериев защищенности информационных систем.
11. Охарактеризуйте идентификацию и аутентификацию с точки зрения критериев защищенности информационных систем.
12. Охарактеризуйте регистрацию и учет с точки зрения критериев защищенности информационных систем.
13. Охарактеризуйте контроль функционирования средств защиты и непрерывность защиты с точки зрения критериев защищенности информационных систем.
14. Дайте определение управлению рисками.
15. Дайте характеристику основным действиям, которые возможно выполнять над рисками.
16. Назовите этапы управления рисками.
17. Дайте характеристику методу оценки уровня риска по степени соответствия определенному набору требований.
18. Дайте характеристику методу оценки уровня риска по вероятности реализации атак.
19. Приведите примеры использования количественных и качественных шкал для определения величины риска ИБ.
20. Дайте определение понятию «аудит» и назовите его виды.
21. Приведите примеры внешних, внутренних и клиентских событий, рассматриваемых при протоколировании.
22. Назовите задачи протоколирования и аудита, а также виды протоколируемых событий.
23. Дайте определению понятию «активный аудит» и назовите его задачи.
24. Назовите виды ошибок, допускаемых в ходе проведения автоматического активного аудита.
25. Дайте краткую характеристику моделям предоставления прав. Каковы преимущества и недостатки этих моделей.
26. Дайте краткую характеристику вероятностным моделям. Каковы преимущества и недостатки этих моделей.
27. Дайте краткую характеристику моделям, основанным на принципах теории информации К. Шеннона.
28. Дайте краткую характеристику моделям целостности информации в системе (моделям Биба).
29. Дайте характеристику модели защиты при отказе в обслуживании.
30. Дайте характеристику модели анализа безопасности программного обеспечения.

Тема 5. Техническое и методическое обеспечение информационной безопасности

Лабораторные работы 13-17

1. Охарактеризуйте физические средства защиты информации и обозначьте задачи, которые они решают.
2. Назовите категории физических средств защиты информации. Приведите примеры соответствующих средств каждой категории.
3. Назовите виды физических средств защиты информации, выделяемые по физической природе и функциональному назначению. Приведите примеры средств защиты соответствующих видов.

4. Назовите виды охранных систем и кратко охарактеризуйте принцип их действия.
5. Приведите схему функционирования охранного телевидения.
6. Назовите способы защиты окон от проникновения злоумышленников.
7. Приведите виды средств контроля доступа в помещения организации и дайте краткую характеристику механизмов их функционирования.
8. Охарактеризуйте аппаратные средства защиты информации и назовите задачи, которые решают эти средства.
9. Назовите виды аппаратных средств защиты информации по функциональному назначению и приведите примеры средств защиты на каждый вид.
10. Назовите направления использования программных средств защиты информации. Приведите примеры соответствующих программных продуктов.
11. Приведите краткую характеристику средств программной защиты информации и примеры соответствующих программных продуктов.
12. Назовите способы шифрования речи.
13. Назовите способы шифрования данных, передаваемых по сетям.
14. Приведите примеры мероприятий, проводимых в рамках комплексного подхода к информационной безопасности объектов предприятия.
15. Назовите средства защиты информации (по одному на каждый вид), который вы используете для защиты информации на вашем домашнем рабочем месте.

Описание оценочного материала:
Форма предъявления: вопросы / темы.
Процедура: Устное собеседование с обучающимся по окончании выполнения лабораторной работы.

Шкала оценивания /критерии:	
«Зачтено»	Обучающийся знает теоретический материал, терминологию, умеет применять теоретические знания для объяснения обсуждаемых явлений, предлагает практические решения обсуждаемых проблем на основе синтеза изученного материала и личного опыта.
«Не зачтено»	Обучающийся не освоил теоретический материал, не продемонстрировал умение применять знания для решения поставленных задач. Обучающийся отказался от ответа.

2.2. Оценочные материалы: промежуточная аттестация

Промежуточная аттестация обеспечивает оценивание окончательных результатов обучения по дисциплине. Промежуточная аттестация осуществляется в форме зачета. Знания и умения обучающихся, характеризующие этапы формирования компетенций, по данным контроля оцениваются по шкале.

Вид ОМ	**Описание оценочного материала**	
	Тема	**Перечень вопросов**
Вопросы зачета (ВЗ)	Тема 1. Информационная безопасность. Основные положения, понятия и определения	1. Назначение и структура Доктрины информационной безопасности (ИБ) РФ. 2. Четыре основные составляющие национальных интересов РФ в информационной сфере. 3. Интересы государства, общества и личности в информационной сфере. 4. Основные направления международного сотрудничества РФ в области ИБ. 5. Определения понятий конфиденциальной информации, степеней её секретности. 6. Основные методы определения объема

		информации. 7. Товарная ценность информации, пути её получения. 8. Особенности обеспечения ИБ РФ в сферах экономики, внешней и внутренней политики. 9. Особенности обеспечения ИБ РФ в сферах обороны, правоохранительной и судебной систем. 10. Особенности обеспечения ИБ РФ в областях науки и техники, в духовной сфере. 11. Особенности обеспечения ИБ РФ в информационных и телекоммуникационных системах. 12. Основные эволюционные подходы к обеспечению ИБ деятельности общества.
	Тема 2. Методология обеспечения информационной безопасности деятельности общества.	13. Основные виды и источники угроз ИБ РФ. 14. Информационное оружие и примеры его применения. 15. Основные проблемы информационной безопасности всемирного сообщества. 16. Основные признаки ИБ объектов и субъектов. 17. Формула Д. Медоуза и области её применения. 18. Основные принципы защиты процессов переработки информации.
	Тема 3. Организационно-правовое обеспечение информационной безопасности	19. Классификация организационных и правовых методов нейтрализации угроз ИБ. 20. Классификация средств нейтрализации угроз ИБ. 21. Структура государственных органов обеспечения ИБ в РФ. 22. Четыре группы методов и средств защиты процессов переработки информации в защищенных компьютерных системах. 23. Стратегии обеспечения ИБ организаций и предприятий.
	Тема 4. Модели и системы обеспечения информационной безопасности деятельности организаций	24. Основные группы моделей безопасности. 25. Модели безопасности по разграничению доступа в систему. 26. Управление доступом, идентификация и аутентификация. 27. Модели защиты процессов переработки информации. 28. Модели защиты при отказе в обслуживании. 29. Модели анализа безопасности программного обеспечения. 30. Модели контроля целостности информации в системе.
	Тема 5. Техническое и методическое обеспечение информационной безопасности	31. Категорирование объектов и защита информационных сетей. 32. Основные положения защищенной сети. 33. Процедурный уровень информационной безопасности. 34. Основные программно-технические меры

		защиты информации. 35. Основные организационные меры по обеспечению ИБ в нормальных и чрезвычайных условиях. 36. Классификация методов предотвращения угроз шпионажа и диверсий. 37. Основные критерии защищенности вычислительных систем. 38. Основные направления обеспечения ИБ, применяемые в мировой практике. 39. Основные положения ИБ, изложенные в «Европейских критериях». 40. Основные функции государственной системы обеспечения ИБ. 41. Отечественные стандарты в области ИБ. 42. Зарубежные стандарты в области ИБ. 43. Политика безопасности предприятия (организации). 44. Законодательство РФ в информационной сфере и меры ответственности за его нарушение. 45. Управление рисками ИБ. 46. Основные методики оценивания рисков ИБ. 47. Обзор технических средств обеспечения защиты объектов. 48. Обзор криптографических методов и средств обеспечения ИБ. 49. Обзор программно-аппаратных средств защиты информационных систем. 50. Аудит информационной безопасности предприятий.

Форма предъявления: Средство контроля, организованное как специальная беседа преподавателя с обучающимися на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенной теме.

Процедура: Зачет проводится в конце семестра по завершении аудиторной и самостоятельной работы по дисциплине путем собеседования.

Критерии/шкала оценивания:	
«Зачтено»	заслуживает обучающийся, обнаруживший знания учебного материала от достаточных до всесторонних и глубоких, умеющий свободно выполнять задания, предусмотренные программой, усвоивший основную и знакомый с дополнительной литературой. Обучающийся демонстрирует уверенное владение понятийно-терминологическим аппаратом дисциплины, отсутствуют ошибки в употреблении терминов.
«Не зачтено»	заслуживает обучающийся, обнаруживший не удовлетворительные знания учебного материала, не умеющий выполнять задания, предусмотренные программой, усвоивший основную литературу. Обучающийся демонстрирует слабое владение понятийно-терминологическим аппаратом дисциплины, присутствуют

	ошибки в употреблении терминов.

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

Текущий контроль

Текущий контроль успеваемости по дисциплине осуществляется для проверки хода и качества усвоения учебного материала, стимулирования учебной деятельности обучающихся, совершенствования методики проведения занятий и проводится в ходе всех видов занятий в форме устного опроса на лекционных, семинарских и практических занятиях, выполнения устных и письменных практических заданий, в форме рубежного контроля и в форме выполнения контрольных работ.

Критерии оценки устных ответов
в ходе проведения семинарских и практических занятий

Шкала оценивания и отметка	**Показатели оценивания**
Отлично	Содержание материала раскрыто в полном объеме, предусмотренном учебной программой. Речь последовательна, хорошо продумана, изложена грамотным языком, с точным использованием терминологии. Обучающийся продемонстрировал умение иллюстрировать материал конкретными примерами, в том числе на основе раннее изученного материала, показано умение делать обобщение, выводы, сравнение. Изложение ответа осуществляется самостоятельно, без наводящих вопросов. Обучающийся принимает активное участие в изложении или в обсуждении изучаемого материала.
Хорошо	Обучающийся не полно раскрыл содержание материала, но показано общее понимание вопроса, достаточное для дальнейшего изучения программного материала. Изложение материала недостаточно последовательное, имеются затруднения и допущены ошибки в определении понятий и в использовании терминологии, однако обучающийся активно участвует в обсуждении изучаемого материала.
Удовлетворительно	Обучающийся затрудняется в изложении

	материала, делает обобщения, выводы, сравнения с помощью преподавателя, отвечает с помощью наводящих вопросов и подсказок, затрудняется в приведении примеров. С трудом вспоминает пройденный материал, не активен, в обсуждении материала участвует эпизодически.
Неудовлетворительно	Обучающийся не раскрыл основное содержание учебного материала или содержание материала излагалось с многочисленными подсказками, показавшими незнание или непонимание большей части учебного материала, допущены путаница и ошибки в определении понятий, продемонстрировано полное неумение приводить примеры при объяснении материала, в обсуждении материала пассивен.

Рубежный контроль является одним из видов текущего контроля. Рубежный контроль осуществляется с целью систематической проверки достижения обучающимися обязательных результатов обучения по дисциплине – минимума, который необходим для дальнейшего обучения, выполнения программных требований к уровню подготовки обучающихся. Рубежный контроль проводится по завершении изучения отдельных наиболее сложных и объемных тем, разделов учебной дисциплины. Рубежный контроль проводится на практических или семинарских занятиях. Лица, не сдавшие (не прошедшие) рубежный контроль, до промежуточной аттестации не допускаются. Результаты рубежного контроля заносятся в журнал учета учебных занятий. Рубежный контроль проводится в форме письменного или автоматизированного (компьютерного) тестирования. Обучающемуся предъявляется не менее 20 тестовых вопросов. Время для выполнения задания предоставляется из расчета: 1 минута на один тестовый вопрос.

Критерии оценки результатов тестирования

Шкала оценивания	**Критерии оценивания**
Отлично	Даны ответы не менее, чем на 90% тестовых заданий
Хорошо	Даны ответы не менее, чем на 75% тестовых заданий
Удовлетворительно	Даны ответы не менее, чем на 60% тестовых заданий
Неудовлетворительно	Даны ответы менее, чем на 60% тестовых заданий

Контрольная работа является видом текущего контроля, в отдельных случаях (если есть соответствующее указание в учебном плане) контрольная работа является формой промежуточной аттестации. Контрольные работы выполняются обучающимися в виде письменных ответов на вопросы, решения задач, выполнения контрольных (в том числе тестовых) заданий или практической проверки выполнения практических действий по составлению (корректировке) юридических документов. Выполнение контрольных работ может быть организовано в электронной форме. Содержание заданий на контрольную работу и порядок ее выполнения устанавливаются кафедрой.

Критерии оценки результатов выполнения контрольной работы, проведенной в форме решения практических задач

Оценка	**Критерии оценивания**
Отлично	Решение задачи (выполнение задания) осуществлено верно, обучающимся продемонстрировано умение пользоваться теоретическими знаниями, приведены все необходимые ссылки на нормативно-правовые акты. Выводы достоверны и аргументированы с привлечением источников нормативно-правовой информации. Формулировки выводов четкие, понятные и обоснованные. При неоднозначности возможного решения (описания ситуации) приведены возможные варианты с указанием последствий.
Хорошо	Задача (выполнение задания) решена верно, обучающимся продемонстрировано умение пользоваться теоретическими знаниями для решения практической задачи. Однако приведены не все необходимые ссылки на нормативно-правовые акты, формулировки выводов недостаточно четкие и понятные. Аргументация выводов свидетельствует об их недостаточной достоверности и обоснованности.
Удовлетворительно	Задача в целом решена, однако отсутствуют ссылки на нормативно-правовые акты. Решение задачи осуществлено шаблонно, без должного проявления профессиональной компетентности. Отсутствует логика, точность

	и грамотность изложения решения задачи (выполнения задания). Вывод недостаточно обоснован, не содержит необходимой аргументации, поверхностный или не следует из решения задачи.
Неудовлетворительно	Задача решена неверно или решение задачи отсутствует.

При оценивании результатов письменных контрольных работ обязательно учитываются грамотность изложения, чистота и правильность оформления работ. Работа, правильно передающая содержание материала, но изложенная с грамматическими ошибками или ошибками в графическом оформлении, не может быть оценена выше, чем - удовлетворительно. За работу, выполненную с грубыми грамматическими ошибками, нелитературным языком, неграмотно или небрежно графически оформленную, выставляется оценка - неудовлетворительно.

Критерии оценки результатов выполнения контрольной работы, проведенной в форме тестирования:

Шкала оценивания	Критерии оценивания
Отлично	Даны ответы не менее, чем на 90% тестовых заданий
Хорошо	Даны ответы не менее, чем на 75% тестовых заданий
Удовлетворительно	Даны ответы не менее, чем на 60% тестовых заданий
Неудовлетворительно	Даны ответы менее, чем на 60% тестовых заданий

При проведении контрольной работы в смешенной форме (теоретическая часть – в форме тестирования, а практическая часть – в форме выполнения практического задания) каждая часть работы оценивается отдельно по пятибалльной шкале в соответствии с вышеуказанными критериями. Оценка за контрольную работу в целом выставляется по сумме балов за теоретическую и практическую часть в соответствии со следующей шкалой оценивания:

Оценка	Сумма баллов за теоретическую и практическую часть контрольной работы
Отлично	**9-10**
Хорошо	**7-8**
Удовлетворительно	**5-6**
Неудовлетворительно	**0-4**

Заведующий кафедрой
информационных систем и технологий И.В. Бондарь

Разработчик
Доцент кафедры
информационных систем и технологий И.А. Голдобин

Обсуждено и одобрено на заседании кафедры
протокол №7 от «25» июля 2023 г.

Лист дополнений и изменений, внесенных в рабочую программу дисциплины

Номер изменений	Номера страниц				Всего страниц	Дата	Основание* для изменений
	изме-ненных	заме-ненных	анну-лирован-ных	новых			

*Основанием для внесения изменения является решение кафедры (протокол № ___ от «___» _____ 20___ г.).