Автономная некоммерческая организация высшего образования
“ИНСТИТУТ БИЗНЕСА И ДИЗАЙНА”
ФАКУЛЬТЕТ УПРАВЛЕНИЯ БИЗНЕСОМ

УТВЕРЖДАЮ
Ректор _____ С.С. Юров
«29» июня 2023 г.

Б1.О.04 МОДУЛЬ ОБЩЕПРОФЕССИОНАЛЬНОЙ ПОДГОТОВКИ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.О.04.11 ЗАЩИТА ИНФОРМАЦИИ

Для направления подготовки:
09.03.02 Информационные системы и технологии
(уровень бакалавриата)

Типы задач профессиональной деятельности:
организационно-управленческий; проектный

Направленность (профиль):
Разработка и управление цифровыми продуктами

Форма обучения:
очная, заочная

Москва – 2023

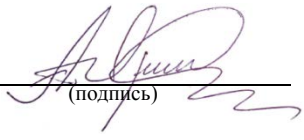
Разработчик: Мелехов Игорь Сергеевич, преподаватель кафедры гуманитарных и естественно-научных дисциплин АНО ВО «Институт бизнеса и дизайна».

«20» июня 2023 г.  /И.С.Мелехов/

СОГЛАСОВАНО:

Декан факультета  /Н.Е. Козырева /

(подпись)

Заведующий кафедрой
разработчика РПД  /А.Б.Оришев /

(подпись)

Протокол заседания кафедры № 10 от «22» июня 2023 г.

1. ЦЕЛЬ И ЗАДАЧИ ДИСЦИПЛИНЫ

Цель: формирование у студентов системы знаний в области информационной безопасностии применения на практике методов и средств защиты информации.

Задачи:

формирование умения обеспечить защиту информации и объектов информатизации;формирование умения составлять заявительную документацию в надзорные государственные органы инфокоммуникационной отрасли;

формирование навыков выполнения работ в области технического регулирования, сертификации технических средств, систем, процессов, оборудования и материалов;формирование навыков обеспечения защиты объектов интеллектуальной собственности и результатов исследований и разработок как коммерческой тайны предприятия;

настройка и обслуживание аппаратно-программных средств.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

2.1. Место дисциплины в учебном плане:

Блок: Блок 1. Дисциплины (модули).

Часть: Обязательная часть.

Модуль: Модуль общепрофессиональной подготовки.

Осваивается: 4 семестр по очной форме обучения, 5 семестр по заочной форме обучения.

3. КОМПЕТЕНЦИИ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

УК - 2 - способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений;

ОПК - 3 - способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

4. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ ОБУЧАЮЩИМСЯ

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Результаты освоения компетенции
УК-2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	**УК-2.2** Выбирает оптимальный способ решения задач, учитывая действующие правовые нормы и имеющиеся условия, ресурсы и ограничения	**Знает:** методологию выбора оптимальных способов решения задач, учитывая действующие правовые нормы и имеющиеся условия, ресурсы и ограничения **Умеет:** определять круг задач, планировать и выбирать пути их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений **Владеет:** способами решения конкретных задач в профессиональной деятельности, исходя из действующих норм, имеющихся ресурсов

ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**ОПК-3.2.** Самостоятельно подготавливает обзоры, аннотации, составляет рефераты, научные доклады, публикации при решении задач профессиональной деятельности с учетом требований информационной безопасности	**Знает:** существующие методы и способы обеспечения функционирования баз данных и обеспечения их информационной безопасности **Умеет:** выполнять работы по обеспечению функционирования баз данных и обеспечению их информационной безопасности. **Владеет:** методами и способами выполнения работы по обеспечению функционирования баз данных и обеспечению их информационной безопасности

5. ОБЪЕМ ДИСЦИПЛИНЫ И РАСПРЕДЕЛЕНИЕ ВИДОВ УЧЕБНОЙ РАБОТЫ ПО СЕМЕСТРАМ

Общая трудоемкость дисциплины «Защита информации» для студентов всех форм обучения, реализуемых в АНО ВО «Институт бизнеса и дизайна» по направлению подготовки 09.03.02 Информационные системы и технологии составляет: 3 з.е. / 108 час.

Вид учебной работы	Всего число часов и (или) зачетных единиц (по формам обучения)	
	Очная	Заочная
Аудиторные занятия	72	14
в том числе:		
Лекции	36	6
Практические занятия	36	8
Лабораторные работы	-	-
Самостоятельная работа	36	90
в том числе:		
часы на выполнение КР / КП	-	-
Промежуточная аттестация:		
Вид	Зачет с оценкой – 4 семестр	Зачет с оценкой – 5 семестр
Трудоемкость (час.)		4
Общая трудоемкость з.е. / часов	3 з.е. / 108 час.	3 з.е. / 108 час.

6. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Темы дисциплины		**Количество часов (по формам обучения)**							
		Очная				**Заочная**			
№	**Наименование**	**Лекции**	**Практические занятия**	**Лабораторные работы**	**Самост. работа** *(в т.ч. КР / КП)*	**Лекции**	**Практические занятия**	**Лабораторные работы**	**Самост. работа** *(в т.ч. КР / КП)*
1	Понятие и сущность информационной	2	-	-	6	1	-	-	9

Темы дисциплины		Количество часов (по формам обучения)							
		Очная				Заочная			
№	Наименование	Лекции	Практические занятия	Лабораторные работы	Самост. работа *(в т.ч. КР / КП)*	Лекции	Практические занятия	Лабораторные работы	Самост. работа *(в т.ч. КР / КП)*
	безопасности и защиты информации								
2	Становление и развитие информационной безопасности и защиты информации	2	-	-	6	-	-	-	9
3	Правовой уровень обеспечения информационной безопасности	4	-	-	3	1	-	-	9
4	Информационная безопасность в системе национальной безопасности РФ	4	-	-	3	-	-		9
5	Основы государственной политики РФ в области информационной безопасности	4	6	-	3	1	1	-	9
6	Основные угрозы информационной безопасности	4	6	-	3	-	1	-	9
7	Методы и средства обеспечения информационной безопасности и защиты информации	4	6	-	3	-	2	-	9
8	Административный уровень обеспечения информационной безопасности и защиты информации	4	6	-	3	1	1	-	9
9	Процедурный уровень обеспечения информационной безопасности и защиты информации	4	6	-	3	1	1	-	9
10	Аппаратно-программный уровень обеспечения информационной безопасности и защиты информации	4	6	-	3	1	2	-	9
	Итого (часов)	36	36	-	36	6	8	-	90
	Форма контроля:	*зачёт с оценкой*			-	*зачёт с оценкой*			4
	Всего по дисциплине:	108 / 3 з.е.				108 / 3 з.е.			

СОДЕРЖАНИЕ ТЕМ ДИСЦИПЛИНЫ

Тема 1. Понятие и сущность информационной безопасности и защиты информации

Необходимость и значимость нормативно-правового определения основных понятий. Понятие информационной безопасности (ИБ) и защиты информации. Основные компоненты безопасности государства и доминирующая роль ИБ.

Тема 2. Становление и развитие информационной безопасности и защиты информации

Цели и задачи информационной безопасности в Российской Федерации. Связь информационной безопасности с информатизацией общества. Базовые уровни обеспечения информационной безопасности и защиты информации.

Тема 3. Правовой уровень обеспечения информационной безопасности

Основные федеральные органы, генерирующие в Российской Федерации нормативно-правовые акты в сфере информационной безопасности и защиты информации. Роль в России Межведомственной комиссии по защите государственной тайны в формировании перечня сведений, составляющих государственную тайну. Место коммерческой тайны в системе предпринимательской деятельности. Основания и методика отнесения сведений к коммерческой тайне.

Тема 4. Информационная безопасность в системе национальной безопасности РФ

Основные федеральные органы, генерирующие в Российской Федерации нормативно-правовые акты в сфере информационной безопасности и защиты информации. Роль в России Межведомственной комиссии по защите государственной тайны в формировании перечня сведений, составляющих государственную тайну. Место коммерческой тайны в системе предпринимательской деятельности. Основания и методика отнесения сведений к коммерческой тайне.

Тема 5. Основы государственной политики РФ в области информационной безопасности

Основные федеральные органы, генерирующие в Российской Федерации нормативно-правовые акты в сфере информационной безопасности и защиты информации. Роль в России Межведомственной комиссии по защите государственной тайны в формировании перечня сведений, составляющих государственную тайну. Место коммерческой тайны в системе предпринимательской деятельности. Основания и методика отнесения сведений к коммерческой тайне.

Тема 6. Основные угрозы информационной безопасности

Классификация источников угроз безопасности информации по принципу и характеру его воздействия на объект защиты. Методы и способы воздействия источников угроз на объект защиты в зависимости от используемых средств нападения. Классификация угроз безопасности информации по степени нарушения состояния информационной безопасности (доступности, целостности, конфиденциальности). Каналы несанкционированного доступа к информационным ресурсам в информационной системе. Цели и задачи по защите информационных ресурсов от несанкционированного доступа в соответствии с нормативно-правовыми документами России.

Тема 7. Методы и средства обеспечения информационной безопасности и защиты информации

Правовые, организационно-технические и экономические методы обеспечения информационной безопасности. Модели, стратегии и системы обеспечения ИБ. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем.

Тема 8 Административный уровень обеспечения информационной безопасности и защиты информации

Правовые, организационно-технические иэкономические методы обеспечения информационной безопасности. Модели, стратегии и системы обеспечения ИБ. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем.

Тема 9. Процедурный уровень обеспечения информационной безопасности и защиты информации

Основные классы мер процедурного уровня Управление персоналом Физическая защита Поддержание работоспособности Реагирование на нарушения режима безопасности Планирование восстановительных работ

Тема 10. Аппаратно-программный уровень обеспечения информационной безопасности и защиты информации

Программно-аппаратные сервисы обеспечения безопасности информационных ресурсов в информационных системах. Идентификация и аутентификация пользователей как передовой рубеж защиты информации. Базовые методы парольной аутентификации. Модели разграничения доступа к

информации. Протоколирование и аудит (активный и пассивный) ИС, их основные цели и особенности. Базовые методы криптографического преобразования данных. Процедура формирования электронной подписи. Экранирование информации в информационно-телекоммуникационных сетях. Компьютерные вирусы и вредоносные программы: классификация, методы и средства борьбы с вредоносными программами. Управление высокой доступности.

7. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ РАБОТ

Курсовая работа не предусмотрена

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ: Приложение 1.

9. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ:

9.1. Рекомендуемая литература:

1. Ищейнов, В. Я. Информационная безопасность и защита информации: теория и практика: учебное пособие: [16+] / В. Я. Ищейнов. – Москва; Берлин: Директ-Медиа, 2020. – 271 с.
Режим доступа: https://biblioclub.ru/index.php?page=book_red&id=571485

2. Введение в информационную безопасность и защиту информации: учебное пособие: [16+] / В. А. Трушин, Ю. А. Котов, Л. С. Левин, К. А. Донской. – Новосибирск: Новосибирский государственный технический университет, 2017. – 132 с.
Режим доступа: https://biblioclub.ru/index.php?page=book_red&id=575113

3. Основы информационной безопасности: учебник / В. Ю. Рогозин, И. Б. Галушкин, В. Новиков, С. Б. Вепрев; Академия Следственного комитета Российской Федерации. – Москва: Юнити-Дана: Закон и право, 2018. – 287 с.
Режим доступа: https://biblioclub.ru/index.php?page=book_red&id=562348

6.2. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень лицензионного и свободно распространяемого программного обеспечения.

При осуществлении образовательного процесса по данной учебной дисциплине предполагается использование:

Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства:

1. Windows 10 Pro Professional (Договор: Tr000391618, Лицензия: V8732726);
2. Microsoft Office Professional Plus 2019 (Договор: Tr000391618, Лицензия: V8732726);
3. Браузер Google Chrome;
4. Браузер Yandex;
5. Adobe Reader - программа для просмотра, печати и комментирования документов в формате PDF

6.3. Перечень современных профессиональных баз данных, информационных справочных систем и ресурсов информационно-телекоммуникационной сети «Интернет»

1. http://window.edu.ru/ - единое окно доступа к образовательным ресурса
2. https://biblioclub.ru/ - университетская библиотечная система online Библиоклуб.ру
3. https://uisrussia.msu.ru/ - база данных и аналитических публикаций университетской информационной системы Россия
4. https://www.elibrary.ru/ - электронно-библиотечная система eLIBRARY.RU, крупнейшая в России электронная библиотека научных публикаций
5. http://www.consultant.ru/ - справочная правовая система КонсультантПлюс
6. https://gufo.me/ - справочная база энциклопедий и словарей
7. https://slovaronline.com - поисковая система по всем доступным словарям и энциклопедиям

8. https://www.tandfonline.com/ - коллекция журналов Taylor&Francis Group включает в себя около двух тысяч журналов и более 4,5 млн. статей по различным областям знаний

9. https://openedu.ru - «Национальная платформа открытого образования» (ресурсы открытого доступа)

10. https://www.rsl.ru - Российская Государственная Библиотека (ресурсы открытого доступа)

11. https://link.springer.com - Международная реферативная база данных научных изданий Springerlink (ресурсы открытого доступа)

12. https://zbmath.org - Международная реферативная база данных научных изданий zbMATH (ресурсы открытого доступа)

13. http://www.fstec.ru – федеральная служба по техническому и экспортному контролю

14. http://www.securitylab.ru - информационный портал о защите информации

10. Материально-техническое обеспечение дисциплины

1. Оборудованные учебные аудитории, в том числе с использованием видеопроектора и подключением к сети «Интернет» и доступом в электронную информационно-образовательную среду Института.

2. Аудитории для самостоятельной работы с подключением к сети «Интернет» и доступом в электронную информационно-образовательную среду Института.

3. Компьютерный класс с подключением к сети «Интернет» и доступом в электронную информационно-образовательную среду Института.

4. Аудио и видеоаппаратура.

№ 403

Учебная аудитория для проведения учебных занятий. Аудитория оснащена оборудованием и техническими средствами обучения:

а) учебной мебелью: столы, стулья, доска маркерная учебная

б) стационарный широкоформатный мультимедиа-проектор Epson EB-X41, экран, колонки.

в) 11 компьютеров, подключенных к сети «Интернет», с обеспечением доступа в электронную информационно-образовательную среду АНО ВО «Институт бизнеса и дизайна»

№ 402

Помещение для самостоятельной работы. Аудитория оснащена оборудованием и техническими средствами обучения:

а) учебной мебелью: столы, стулья, доска маркерная учебная

б) стационарный широкоформатный мультимедиа-проектор Epson EB-X41, экран, колонки.

в) 11 компьютеров, подключенных к сети «Интернет», с обеспечением доступа в электронную информационно-образовательную среду АНО ВО «Институт бизнеса и дизайна»

11. Методические указания для обучающихся по освоению дисциплины

В процессе освоения дисциплины студенту необходимо посетить все виды занятий, предусмотренные рабочей программой дисциплины и выполнить контрольные задания, предлагаемые преподавателем для успешного освоения дисциплины. Также следует изучить рабочую программу дисциплины, в которой определены цели и задачи дисциплины, компетенции обучающегося, формируемые в результате освоения дисциплины и планируемые результаты обучения. Рассмотреть содержание тем дисциплины; взаимосвязь тем лекций и практических занятий; бюджет времени по видам занятий; оценочные средства для текущей и промежуточной аттестации; критерии итоговой оценки результатов освоения дисциплины. Ознакомиться с методическими материалами, программно-информационным и материально техническим обеспечением дисциплины.

Работа на лекции

Лекционные занятия включают изложение, обсуждение и разъяснение основных

направлений и вопросов изучаемой дисциплины, знание которых необходимо в ходе реализации всех остальных видов занятий и в самостоятельной работе студентов. На лекциях студенты получают самые необходимые знания по изучаемой проблеме. Непременным условием для глубокого и прочного усвоения учебного материала является умение студентов сосредоточенно слушать лекции, активно, творчески воспринимать излагаемые сведения. Внимательное слушание лекций предполагает интенсивную умственную деятельность студента. Краткие записи лекций, конспектирование их помогает усвоить материал. Конспект является полезным тогда, когда записано самое существенное, основное. Запись лекций рекомендуется вести по возможности собственными формулировками.

Желательно запись осуществлять на одной странице, а следующую оставлять для проработки учебного материала самостоятельно в домашних условиях. Конспект лучше подразделять на пункты, параграфы, соблюдая красную строку. Принципиальные места, определения, формулы следует сопровождать замечаниями. Работая над конспектом лекций, всегда следует использовать не только основную литературу, но и ту литературу, которую дополнительно рекомендовал лектор.

Практические занятия

Подготовку к практическому занятию следует начинать с ознакомления с лекционным материалом, с изучения плана практических занятий. Определившись с проблемой, следует обратиться к рекомендуемой литературе. Владение понятийным аппаратом изучаемого курса является необходимым, поэтому готовясь к практическим занятиям, студенту следует активно пользоваться справочной литературой: энциклопедиями, словарями и др. В ходе проведения практических занятий, материал, излагаемый на лекциях, закрепляется, расширяется и дополняется при подготовке сообщений, рефератов, выполнении тестовых работ. Степень освоения каждой темы определяется преподавателем в ходе обсуждения ответов студентов.

Самостоятельная работа

Студент в процессе обучения должен не только освоить учебную программу, но и приобрести навыки самостоятельной работы. Самостоятельная работа студентов играет важную роль в воспитании сознательного отношения самих студентов к овладению теоретическими и практическими знаниями, привитии им привычки к направленному интеллектуальному труду. Самостоятельная работа проводится с целью углубления знаний по дисциплине. Материал, законспектированный на лекциях, необходимо регулярно дополнять сведениями из литературных источников, представленных в рабочей программе. Изучение литературы следует начинать с освоения соответствующих разделов дисциплины в учебниках, затем ознакомиться с монографиями или статьями по той тематике, которую изучает студент, и после этого – с брошюрами и статьями, содержащими материал, дающий углубленное представление о тех или иных аспектах рассматриваемой проблемы. Для расширения знаний по дисциплине студенту необходимо использовать Интернет-ресурсы и специализированные базы данных: проводить поиск в различных системах и использовать материалы сайтов, рекомендованных преподавателем на лекционных занятиях.

Подготовка к сессии

Основными ориентирами при подготовке к промежуточной аттестации по дисциплине являются конспект лекций и перечень рекомендуемой литературы. При подготовке к сессии студенту следует так организовать учебную работу, чтобы перед первым днем начала сессии были сданы и защищены все практические работы. Основное в подготовке к сессии – это повторение всего материала курса, по которому необходимо пройти аттестацию. При подготовке к сессии следует весь объем работы распределять равномерно по дням, отведенным для подготовки, контролировать каждый день выполнения работы.

Особенности организации образовательной деятельности для лиц с ограниченными возможностями здоровья

В АНО ВО «Институт бизнеса и дизайна» созданы специальные условия для получения высшего образования по образовательным программам обучающимися с ограниченными возможностями здоровья (ОВЗ).

Для перемещения инвалидов и лиц с ограниченными возможностями здоровья в АНО ВО «Институт бизнеса и дизайна» созданы специальные условия для беспрепятственного доступа в учебные помещения и другие помещения, а также их пребывания в указанных помещениях с

учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

При получении образования обучающимся с ограниченными возможностями здоровья при необходимости предоставляются бесплатно специальные учебники и учебные пособия, иная учебная литература. Также имеется возможность предоставления услуг ассистента, оказывающего обучающимся с ограниченными возможностями здоровья необходимую техническую помощь, в том числе услуг сурдопереводчиков и тифлосурдопереводчиков.

Получение доступного и качественного высшего образования лицами с ограниченными возможностями здоровья обеспечено путем создания в институте комплекса необходимых условий обучения для данной категории обучающихся. Информация о специальных условиях, созданных для обучающихся с ограниченными возможностями здоровья, размещена на сайте института (https://obe.ru/sveden/ovz/#anchor_health).

Для обучения инвалидов и лиц с ОВЗ, имеющих нарушения опорно-двигательного аппарата обеспечиваются и совершенствуются материально-технические условия беспрепятственного доступа в учебные помещения, столовую, туалетные, другие помещения, условия их пребывания в указанных помещениях (наличие пандусов, поручней, расширенных дверных проемов и др.).

Для адаптации к восприятию обучающимися инвалидами и лицами с ОВЗ с нарушенным слухом справочного, учебного материала, предусмотренного образовательной программой по выбранным направлениям подготовки, обеспечиваются следующие условия:

для лучшей ориентации в аудитории, применяются сигналы, оповещающие о начале и конце занятия (слово «звонок» пишется на доске);

внимание слабослышащего обучающегося привлекается педагогом жестом (на плечо кладется рука, осуществляется нерезкое похлопывание);

разговаривая с обучающимся, педагог смотрит на него, говорит ясно, короткими предложениями, обеспечивая возможность чтения по губам.

Компенсация затруднений речевого и интеллектуального развития слабослышащих инвалидов и лиц с ОВЗ проводится за счет:

использования схем, диаграмм, рисунков, компьютерных презентаций с гиперссылками, комментирующими отдельные компоненты изображения;

регулярного применения упражнений на графическое выделение существенных признаков предметов и явлений;

обеспечения возможности для обучающегося получить адресную консультацию по электронной почте по мере необходимости.

Для адаптации к восприятию инвалидами и лицами с ОВЗ с нарушениями зрения справочного, учебного, просветительского материала, предусмотренного образовательной программой АНО ВО «Институт бизнеса и дизайна» по выбранной специальности, обеспечиваются следующие условия:

ведется адаптация официального сайта в сети Интернет с учетом особых потребностей инвалидов по зрению, обеспечивается наличие крупношрифтовой справочной информации о расписании учебных занятий;

в начале учебного года обучающиеся несколько раз проводятся по зданию АНО ВО «Институт бизнеса и дизайна» для запоминания месторасположения кабинетов, помещений, которыми они будут пользоваться;

педагог, его собеседники, присутствующие представляются обучающимся, каждый раз называется тот, к кому педагог обращается;

действия, жесты, перемещения педагога коротко и ясно комментируются;

печатная информация предоставляется крупным шрифтом (от 18 пунктов), тотально озвучивается; обеспечивается необходимый уровень освещенности помещений;

предоставляется возможность использовать компьютеры во время занятий и право записи объяснения на диктофон (по желанию обучающегося).

Форма проведения текущей и промежуточной аттестации для обучающихся с ОВЗ

определяется преподавателем в соответствии с учебным планом. При необходимости обучающемуся с ОВЗ с учетом его индивидуальных психофизических особенностей дается возможность пройти промежуточную аттестацию устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п., либо предоставляется дополнительное время для подготовки ответа.

Приложение 1

Автономная некоммерческая организация высшего образования
«ИНСТИТУТ БИЗНЕСА И ДИЗАЙНА»

Факультет управления бизнесом

Фонд оценочных средств

Текущего контроля и промежуточной аттестации
по дисциплине (модулю)

Б1.О.04.11 ЗАЩИТА ИНФОРМАЦИИ

Для направления подготовки:
09.03.02 Информационные системы и технологии
(уровень бакалавриата)

Типы задач профессиональной деятельности:
организационно-управленческий; проектный

Направленность (профиль):
Разработка и управление цифровыми продуктами

Форма обучения:
очная, заочная

Москва – 2023

РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ ОБУЧАЮЩИМСЯ

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Результаты освоения компетенции
УК-2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	**УК-2.2** Выбирает оптимальный способ решения задач, учитывая действующие правовые нормы и имеющиеся условия, ресурсы и ограничения	**Знает:** методологию выбора оптимальных способов решения задач, учитывая действующие правовые нормы и имеющиеся условия, ресурсы и ограничения **Умеет:** определять круг задач, планировать и выбирать пути их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений **Владеет:** способами решения конкретных задач в профессиональной деятельности, исходя из действующих норм, имеющихся ресурсов
ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**ОПК-3.2.** Самостоятельно подготавливает обзоры, аннотации, составляет рефераты, научные доклады, публикации при решении задач профессиональной деятельности с учетом требований информационной безопасности	**Знает:** существующие методы и способы обеспечения функционирования баз данных и обеспечения их информационной безопасности **Умеет:** выполнять работы по обеспечению функционирования баз данных и обеспечению их информационной безопасности. **Владеет:** методами и способами выполнения работы по обеспечению функционирования баз данных и обеспечению их информационной безопасности

ТИПОВЫЕ ОЦЕНОЧНЫЕ СРЕДСТВА, НЕОБХОДИМЫЕ ДЛЯ ОЦЕНКИ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ):

ТЕКУЩИЙ КОНТРОЛЬ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ (МОДУЛЮ)

Тест для формирования ОПК-3.2

Вопрос №1 .

Безопасность информационных ресурсов.

Варианты ответов:

1. Безопасность всего, что используется целевым образом.
2. Безопасность документов и массивов документов в информационных системах (библиотеках, архивах, фондах, банках данных, депозитариях, музейных хранилищах и т. п.).
3. Оба варианта не верны.

Вопрос №2 .

Вычислительные сети

Варианты ответов:

1. Система, обеспечивающая обмен данными между вычислительными устройствами — компьютерами, серверами, маршрутизаторами и другим оборудованием или программным обеспечением.
2. Логически самостоятельная выделенная сеть использующей ресурсы другой физической сети.
3. Оба варианта верны.

Вопрос №3 .

Угроза информационной безопасности.

Варианты ответов:

1. Совокупность условий и факторов, создающих опасность нарушения информационной безопасности.
2. Возможное событие, действие (воздействие), процесс или явление, которые могут привести к нанесению ущерба чьим-либо интересам.
3. Оба варианта верны.

Вопрос №4 .

Защита информации.

Варианты ответов:

1. Практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации.
2. Отсутствие недопустимого риска, связанного с возможностью нанесения ущерба.
3. Оба варианта не верны.

Вопрос №5 .

Требования к содержанию нормативно-методических документов по защите информации.

Варианты ответов:

1. Соответствовать структуре, целям и задачам ИС.
2. Описывать общую программу обеспечения безопасности сети, включая вопросы эксплуатации и усовершенствования.
3. Перечислять возможные угрозы информации и каналы ее утечки, результаты оценки опасностей и рекомендуемые защитные меры.
4. Всё вышеперечисленное.

Критерии оценки выполнения задания

Оценка	Критерии оценивания
Неудовлетворительно	от 0% до 30% правильных ответов из общего числа тестовых заданий
Удовлетворительно	от 31% до 50% правильных ответов из общего числа тестовых заданий
Хорошо	от 51% до 80% правильных ответов из общего числа тестовых заданий
Отлично	от 81% до 100% правильных ответов из общего числа тестовых заданий

Выполнение реферата для формирования ОПК-3.2

1. Цели и задачи защиты информации.
2. Проблемы защиты информации.
3. Этапы развития концепции обеспечения безопасности информации. Общие теоретические принципы теории безопасности.
4. Общие методические принципы теории безопасности. Проблемы информационного противоборства.
5. Государственная политика в информационной сфере. Региональные проблемы информационной безопасности.
6 Современная доктрина информационной безопасности Российской Федерации.
7. Современная концепция информационной безопасности.
8. Основное содержание теории защиты информации.
9. Общеметодологические принципы формирования теории защиты информации. Модели систем и процессов защиты информации.
10. Особенности и состав научно-методологического базиса решения задач защиты информации. Нечеткие множества.

11. Нестрогая математика.Методы оценки.
12. Неформальный поиск оптимальных решений. Требования системного подхода к защите информации.
13. Условия обеспечения требований безопасности. Виды обеспечения системы информационной безопасности.
14. Концептуальная модель информационной безопасности.
15. Критерии, условия и принципы отнесения информации к защищаемой.
16. Количественная и качественная оценки ценности информации. Категории важности информации.
17. Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности: государственная тайна, коммерческая тайна, коммерческая информация, персональная информация,информация для внутреннего пользования и др.
18. Виды и типы угроз безопасности.Классификация угроз.
19. Классификация угроз конфиденциальности, целостности и доступности информации. Изменение активности угроз в зависимости от стадии жизненного цикла.
20. Формирование и коррекция кортесовпотенциальных угроз.
21. Источники, виды и методы дестабилизирующего воздействия на защищаемую информацию.
22. Причины, обстоятельства и условия, вызывающие дестабилизирующее воздействие на защищаемуюинформацию.
23. Виды уязвимости информации и формы ее проявления. Каналы несанкционированного получения информации.Радиоканалы утечки информации.
24. Акустические каналы утечки информации. Электрические каналы утечки информации. Визуально-оптические каналы утечки информации.
25. Материально-вещественные каналы утечки информации.Линии связи.
26. Каналы утечки информации при эксплуатации ЭВМ.
27. Методы и средства несанкционированного получения информации по техническим каналам. Методы и средства разрушения информации.
28. Направления, виды и особенности деятельности спецслужб по несанкционированному доступу к конфиденциальной информации.
29. Система мер, направленных на обеспечение информационной безопасности.Подходы к созданию комплексной системы защиты информации.
30. Виды защиты информации. Характеристики защитных действий. Кадровое и ресурсное обеспечение защиты информации.
31. Современные методы и средства оценивания состояния безопасности информационных систем: препятствие, управление доступом, маскировка, регламентация, принуждение, побуждение.
32. Классификация средств защиты информации. Технические средства защиты информации. Программные средства защиты.
33. Программно-технические средства защиты.Криптографическая защита.
34. Скремблирование.Стеганография.
35. Законодательные средства. Организационные средства защиты.Морально-этические средства.
36. Кадровое и ресурсное обеспечение защиты информации.Построение систем защиты информации.
37. Определение и общеметодологические принципы построения систем защиты информации. Основы архитектурного построения систем защиты.
38. Функциональное, организационное и структурное построение систем защиты информации. Типизация систем защиты.
39. Стандартизация систем защиты. Современные факторы, влияющие на защиту информации

Критерии оценки выполнения задания

Оценка	Критерии оценивания

Неудовлетворительно	Обучающийся не раскрыл материал по теме задания или материал раскрыт поверхностно, излагаемый материал не систематизирован, выводы недостаточно аргументированы, обучающийся не высказывал своего мнения, не проявил способность к анализу, имеются смысловые и речевые ошибки в реферате
Удовлетворительно	Обучающийся демонстрирует логичность и доказательность изложения материала по теме задания, но допускает отдельные неточности при использовании ключевых понятий. Обучающийся не продемонстрировал способность к научному анализу, не высказывал в работе своего мнения, допустил ошибки в логическом обосновании своего ответа
Хорошо	Реферат написан грамотным научным языком, имеет чёткую структуру и логику изложения, точка зрения обучающегося обоснована, в работе присутствуют ссылки на научные источники, мнения известных учёных в данной области
Отлично	Реферат написан грамотным научным языком, имеет чёткую структуру и логику изложения, точка зрения обучающегося обоснована, при разработке реферата использовано не менее 5-8 научных источников. В работе выдвигаются новые идеи и трактовки, демонстрируется способность обучающегося анализировать материал, выражается его мнение по проблеме

Выполнение реферата для формирования УК-2.2

1. Организация допуска и доступа к сведениям, составляющих государственную тайну на предприятии.
2. Порядок допуска и доступа работников сторонних организаций (командировочных) к сведениям конфиденциального характера.
3. Правовые методы регулирования отношений между работодателем и работником по сохранности сведений конфиденциального характера.
4. Особенности защиты информации при опубликовании материалов, определяемые характером деятельности организации, целями публикации, содержанием и характером публикации.
5. Организационно-правовые правила передачи сведений конфиденциального характера в сторонние организации.
6. Разработка политики информационной безопасности на предприятии.

Критерии оценки выполнения задания

Оценка	Критерии оценивания
Неудовлетворительно	Обучающийся не раскрыл материал по теме задания или материал раскрыт поверхностно, излагаемый материал не систематизирован, выводы недостаточно аргументированы, обучающийся не высказывал своего мнения, не проявил способность к анализу, имеются смысловые и речевые ошибки в реферате
Удовлетворительно	Обучающийся демонстрирует логичность и доказательность изложения материала по теме задания, но допускает отдельные неточности при использовании ключевых понятий. Обучающийся не продемонстрировал способность к научному анализу, не высказывал в работе своего мнения, допустил ошибки в логическом обосновании своего ответа
Хорошо	Реферат написан грамотным научным языком, имеет чёткую структуру и логику изложения, точка зрения обучающегося обоснована, в работе присутствуют ссылки на научные источники, мнения известных учёных в данной области

Отлично	Реферат написан грамотным научным языком, имеет чёткую структуру и логику изложения, точка зрения обучающегося обоснована, при разработке реферата использовано не менее 5-8 научных источников. В работе выдвигаются новые идеи и трактовки, демонстрируется способность обучающегося анализировать материал, выражается его мнение по проблеме

Выполнение реферата для формирования ПК-2.2

Концепция и роль организационно-правовых методов в обеспечении информационной безопасности.

Критерии оценки выполнения задания

Оценка	Критерии оценивания
Неудовлетворительно	Обучающийся не раскрыл материал по теме задания или материал раскрыт поверхностно, излагаемый материал не систематизирован, выводы недостаточно аргументированы, обучающийся не высказывал своего мнения, не проявил способность к анализу, имеются смысловые и речевые ошибки в реферате
Удовлетворительно	Обучающийся демонстрирует логичность и доказательность изложения материала по теме задания, но допускает отдельные неточности при использовании ключевых понятий. Обучающийся не продемонстрировал способность к научному анализу, не высказывал в работе своего мнения, допустил ошибки в логическом обосновании своего ответа
Хорошо	Реферат написан грамотным научным языком, имеет чёткую структуру и логику изложения, точка зрения обучающегося обоснована, в работе присутствуют ссылки на научные источники, мнения известных учёных в данной области
Отлично	Реферат написан грамотным научным языком, имеет чёткую структуру и логику изложения, точка зрения обучающегося обоснована, при разработке реферата использовано не менее 5-8 научных источников. В работе выдвигаются новые идеи и трактовки, демонстрируется способность обучающегося анализировать материал, выражается его мнение по проблеме

Выполнение реферата для формирования ПК-2.2

1. Объекты и субъекты интеллектуальной собственности (ИС), порядок передачи исключительных прав на объекты ИС.
2. Правовая охрана интеллектуальной собственности в России и за рубежом.
3. Порядок оформление патента на программное обеспечение и баз данных.
4. Контрафаксная продукция, правовая защита отнедобрасовестной конкуренции.
5. Средства индивидуализации: фирменного наименования, товарного знака, наименования места происхождения товара, критерии охраноспособности и особенности его регистрации в РФ и за рубежом.
6. Компьютерные преступления с использованием высоких технологий, меры дисциплинарной, административной и уголовной ответственности.

Критерии оценки выполнения задания

Оценка	Критерии оценивания
Неудовлетворительно	Обучающийся не раскрыл материал по теме задания или материал раскрыт поверхностно, излагаемый материал не систематизирован, выводы недостаточно аргументированы, обучающийся не высказывал своего мнения, не проявил способность к анализу, имеются смысловые и речевые ошибки в реферате

Удовлетворительно	Обучающийся демонстрирует логичность и доказательность изложения материала по теме задания, но допускает отдельные неточности при использовании ключевых понятий. Обучающийся не продемонстрировал способность к научному анализу, не высказывал в работе своего мнения, допустил ошибки в логическом обосновании своего ответа
Хорошо	Реферат написан грамотным научным языком, имеет чёткую структуру и логику изложения, точка зрения обучающегося обоснована, в работе присутствуют ссылки на научные источники, мнения известных учёных в данной области
Отлично	Реферат написан грамотным научным языком, имеет чёткую структуру и логику изложения, точка зрения обучающегося обоснована, при разработке реферата использовано не менее 5-8 научных источников. В работе выдвигаются новые идеи и трактовки, демонстрируется способность обучающегося анализировать материал, выражается его мнение по проблеме

Выполнение реферата для формирования ПК-2.2

1. Методы борьбы с фишинговыми атаками.
2. Законодательство о персональных данных.
3. Защита авторских прав.
4. Назначение, функции и типы систем видеозащиты.
5. Как подписывать с помощью ЭЦП электронные документы различных форматов.
6. Обзор угроз и технологий защиты Wi-Fi-сетей.
7. Проблемы внедрения дискового шифрования.
8. Борьба со спамом: основные подходы, классификация, примеры, прогнозы на будущее.
9. Особенности процессов аутентификации в корпоративной среде.
10. Квантовая криптография.
11. Утечки информации: как избежать. Безопасность смартфонов.
12. Безопасность применения пластиковых карт - законодательство и практика.
13. Защита CD- и DVD-дисковот копирования.
14. Современные угрозы и защита электронной почты.
15. Программные средства анализа локальных сетей на предмет уязвимостей.
16. Безопасность применения платежных систем - законодательство и практика.
17. Аудит программного кода по требованиям безопасности.
18. Антишпионское ПО (antispyware).
19. Обеспечение безопасности Web-сервисов.
20. Защита от внутренних угроз.
21. Технологии RFID.
22. Уничтожение информации на магнитных носителях.
23. Ботнеты - плацдарм современных кибератак.
24. Цифровые водяные знаки в изображениях.
25. Электронный документооборот. Модели нарушителя.
26. Идентификация по голосу. Скрытые возможности.
27. Безопасность океанских портов.
28. Безопасность связи.
29. Безопасность розничной торговли.
30. Банковская безопасность.
31. Распределенные атаки на распределенные системы.
32. Оценка безопасности автоматизированных систем.
33. Функциональная безопасность программных средств.
34. Технологические процессы и стандарты обеспечения функциональной безопасности в жизненном цикле программных средств.
35. Информационная безопасность: экономические аспекты.

Критерии оценки выполнения задания

Оценка	Критерии оценивания
Неудовлетворительно	Обучающийся не раскрыл материал по теме задания или материал раскрыт поверхностно, излагаемый материал не систематизирован, выводы недостаточно аргументированы, обучающийся не высказывал своего мнения, не проявил способность к анализу, имеются смысловые и речевые ошибки в реферате
Удовлетворительно	Обучающийся демонстрирует логичность и доказательность изложения материала по теме задания, но допускает отдельные неточности при использовании ключевых понятий. Обучающийся не продемонстрировал способность к научному анализу, не высказывал в работе своего мнения, допустил ошибки в логическом обосновании своего ответа
Хорошо	Реферат написан грамотным научным языком, имеет чёткую структуру и логику изложения, точка зрения обучающегося обоснована, в работе присутствуют ссылки на научные источники, мнения известных учёных в данной области
Отлично	Реферат написан грамотным научным языком, имеет чёткую структуру и логику изложения, точка зрения обучающегося обоснована, при разработке реферата использовано не менее 5-8 научных источников. В работе выдвигаются новые идеи и трактовки, демонстрируется способность обучающегося анализировать материал, выражается его мнение по проблеме

Практическое задание для формирования ПК-2.3

АУДИТ РЕЕСТРА В ОПЕРАЦИОННОЙ

СИСТЕМЕ WINDOWS

1. Цель: знакомство с реестром сетевых операционных систем Windows и анализ экономических рисков при потенциальных угрозах

2. Теоретическая часть

2.1. Структура реестра

Реестр хранится на диске в пяти отдельных файлах-кустах, каждый из которых содержит определенный тип конфигурационной информации (т.е. пользовательские данные и установки, связанные с компьютером). Название каждого корневого раздела начинается с HKEY_, и каждый корневой раздел содержит несколько подразделов. Нужные кусты загружаются в память при запуске операционной системы, а также при входе в нее нового пользователя, после чего объединяются в реестр.

Предупреждение. Неумелое редактирование реестра может привести к необходимости переустановки операционной системы!!

Реестр имеет иерархическую древовидную структуру (рис. 2.1). На ее верхнем уровне располагаются так называемые ветви (subtrees), основными из которых являются:

HKEY_LOCAL_MACHINE;
HKEY_USERS.

Остальные ветви представляют собой их подразделы и служат для более быстрого доступа к ним:

HKEY_CLASSES_ROOT;
HKEY_GURRENT_CONFIG;
HKEY_CURRENT_USER.

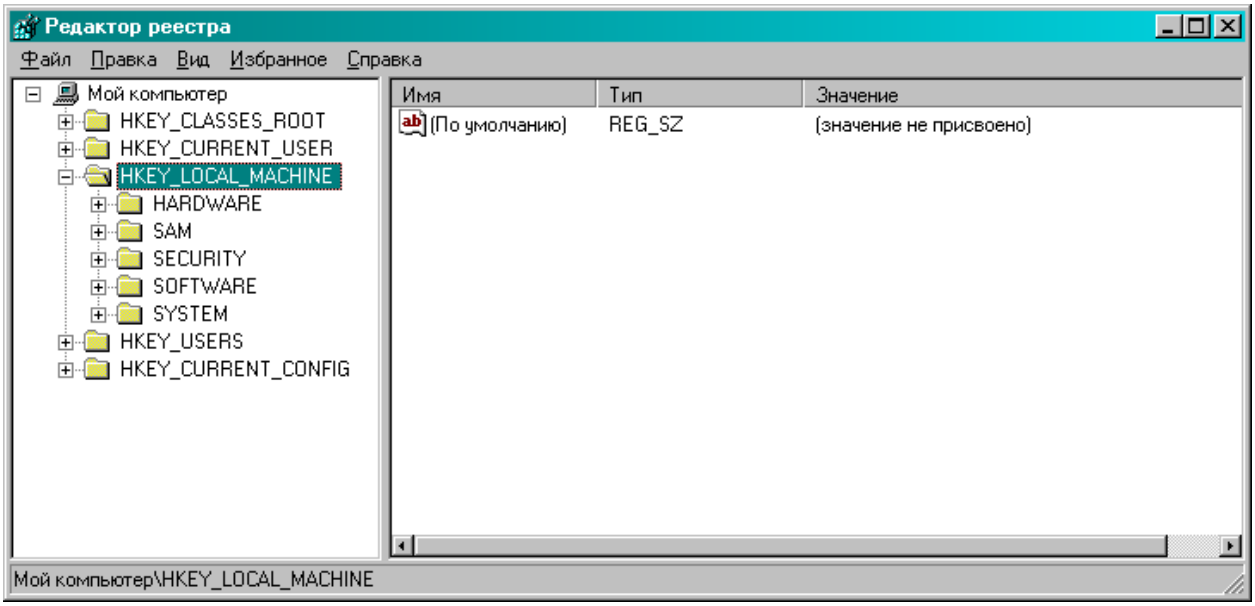


Рис. 2.1. Редактор реестра

Реестр формируется в памяти компьютера при запуске Windows на основе нескольких файлов из папки \Windows\System32\Config. Разделы реестра, которым соответствуют эти файлы, называются кустами (hives). Основные кусты реестра находятся в ветви HKEY_LOCAL MACHINE и называются SAM, SECURITY, S0FTWARE и SYSTEM. Раздел SAM — база данных диспетчера учетных записей, а SECURITY хранит информацию, используемую LSA. В кусте SOFTWARE хранятся настройки программного обеспечения, а в SYSTEM — конфигурационная информация (параметры драйверов и служб), необходимая для загрузки .

Раздел HARDWARE ветви HKEY_LOCAL MACHINE не является кустом, поскольку его информация не сохраняется в файлах, а формируется заново при каждом запуске операционной системы (ОС).

Целостность данных реестра в процессе их модификации обеспечивает механизм, основанный на применении журналов транзакций. Любое изменение, вносимое в реестр, вначале фиксируется в журнале (для этого у каждого из кустов существует свой отдельный файл с расширением LOG) и только затем переносится в файл соответствующего куста. Такой механизм позволяет предотвратить повреждение информации, если в момент ее модификации происходит аппаратный сбой. При следующем запуске ОС основе анализа журналов транзакций определяется, какие изменения на момент сбоя были завершены, а какие — нет. Первые записываются в файл, соответствующий нужному кусту реестра, вторые – просто удаляются из журнала.

Кроме ветви HKEY_LOCAL_MACHINE, в которой находится информация, относящаяся ко всему компьютеру с Windows в целом, в реестре есть ветвь HKEY USERS, где хранятся профили пользователей.

2.2.2. Редактор реестра

Разделы и подразделы реестра защищаются аналогично папкам на дисках NTFS. Настройка параметров системы безопасности для разделов реестра в Windows осуществляется с помощью программы REGEDT32 через ее пункт «Разрешения» меню «Безопасность».

В Windows, как и Windows программа REGEDIT не имеет средств работы с информацией о безопасности, хотя имеет более развитые средства поиска.

В Windows осталась лишь общая программа редактора реестра regedit. Пункт «Разрешения» перенесен в меню «Правка».

2.2.3. Разрешения на доступ к разделам реестра

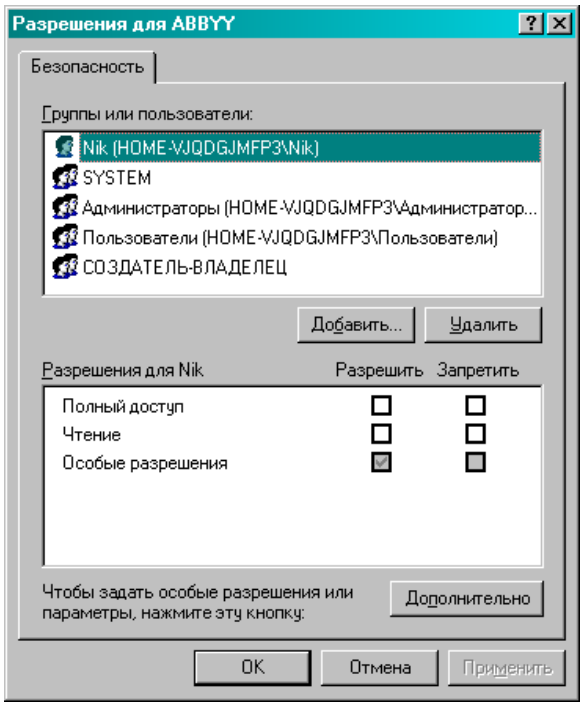


Рис. 2.2. Задание разрешений для папок

Для каждого раздела и подраздела создается отдельный объект со своим отдельным ACL (DACL и SACL). У каждого раздела реестра есть владелец (owner) – либо конкретный пользователь, либо группа Administrators или операционная система (Owner - SYSTEM). Возможны следующие стандартные разрешения на доступ к разделу:

читать;
полный доступ;

В Windows в списке стандартных разрешений в явной форме появились особые разрешения (рис. 2.2).

При нажатии в окне «Разрешения» кнопки дополнительно можно просмотреть полный дискреционный список контроля доступа DACL (рис. 2.3).

Нажав кнопку «Добавить» или выбрав одну из записей списка и нажав «Изменить» можно задать особые разрешения (рис. 2.4).

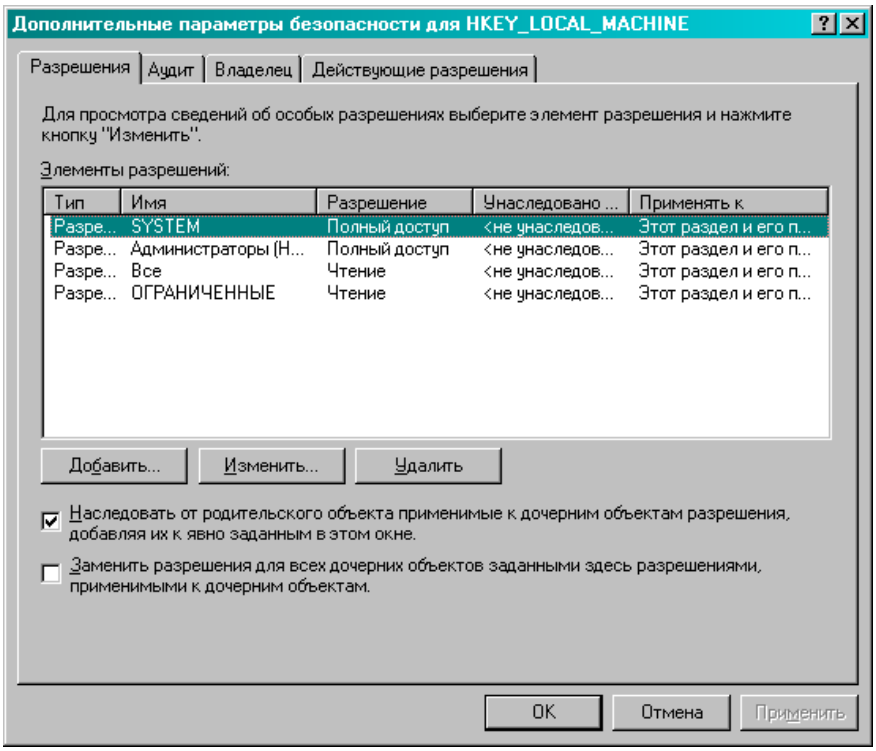


Рис. 2.3. Окно дополнительных параметров безопасности

В этом окне могут быть выборочно установлены права доступа к соответствующему разделу, приведенные в таблице 2.1.

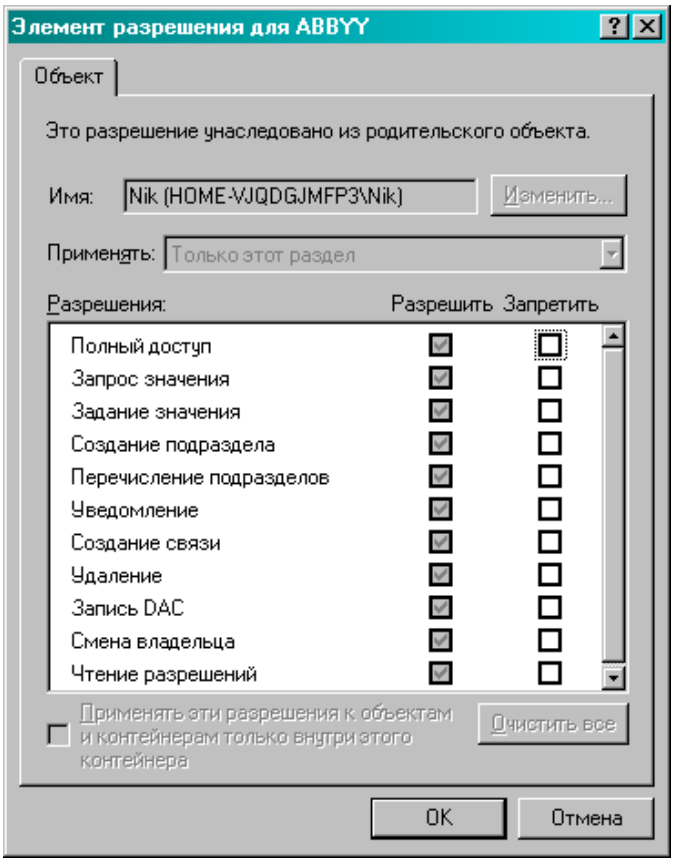


Рис. 2.4. Разрешения/запрет для доступа к объекту

Таблица 2.1

Права доступа и их возможности

Право доступа	Возможности
Запрос значения	Чтение значения параметров раздела, времени последнего изменения параметров раздела
Задание значения	Запись в раздел новых параметров, изменение значения существующих
Создание подраздела	Создание подраздела в данном разделе
Перебор подразделов	Просмотр списка подразделов
Уведомление	Получение оповещения об изменениях в данном разделе
Создание связи	Создание в разделе символической ссылки на другой раздел

Продолжение таблицы 2.1	
Удаление	Удаление раздела целиком или отдельных его параметров
Запись DAC	Изменение списка прав доступа к разделу
Смена владельца	Стать владельцем раздела
Чтение разрешений	Просмотр информации о разрешениях на доступ к разделу

Разрешения на доступ к разделам реестра, установленные в системе Windows по умолчанию, не позволяют обычным пользователям модифицировать его части, наиболее важные для функционирования омой операционной системы, ее системы безопасности и большинства приложении. Некоторые разделы ветви HKEY LOCAL MACHINE, в частности SAM и SECURITY, по умолчанию недоступны для просмотра и модификации даже администратору (хотя последний может

просмотреть и изменить ACL к ним).

2.2.3. Аудит реестра

Аудит представляет собой процесс, который операционные системы Windows используют для обнаружения и регистрации событий, связанных с системой безопасности. К таким событиям относятся, например, попытки создания или удаления системных объектов, а также попытки получения доступа к таким объектам. Обратите внимание, что в объектно-ориентированных системах в качестве объекта может рассматриваться все что угодно — файлы, папки, ключи реестра и т. д. Все эти и другие подобные им события регистрируются в файле, известном под названием журнала безопасности (security log). По умолчанию аудит в системе не активизирован. Таким образом, если вам необходимо контролировать события, относящиеся к безопасности, то требуется его активизировать. После того как это будет сделано, операционная система начинает регистрировать события, связанные с системой безопасности, и зарегистрированные данные можно просмотреть с помощью специального средства просмотра — утилиты Просмотр событий (Event Viewer). При установке аудита можно указать типы событий, подлежащих регистрации в обнале безопасности, и операционная система будет создавать в журнале безопасности запись о событии каждый раз, когда событие указанного типа происходит в системе. Запись в журнале безопасности содержит описание события, имя пользователя, который выполнил соответствующие этому событию действия, а также дату и время события. Аудит можно установить как на успешные, так и на неудачные попытки выполнения операций, и журнал безопасности, соответственно, будет отображать имена пользователей, совершивших успешные попытки, и имена пользователей, пытавшихся выполнить запрещенные действия.

Вначале надо проверить, включен ли в политике безопасности аудит доступа к объектам. Для регистрации событий, связанных с доступом к тому или иному разделу реестра, в частности HKEY_LOCAL MACHINE\SECURITY и \SAM, надо внести соответствующие записи в SACL к нужному разделу. Для этого в листе «Дополнительные параметры безопасности» (рис. 2.5) выбрать лист «Аудит» и нажать кнопку «оббавить» или «Изменить» и в окне элемент аудита произвести настройку записи аудита (ACE) (рис. 2.6).

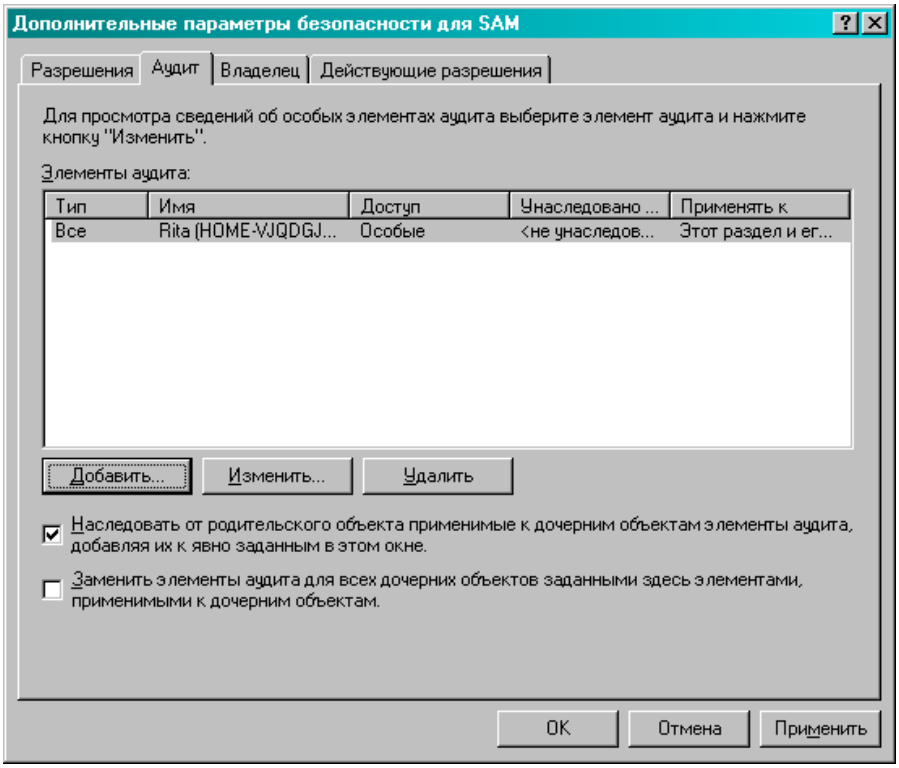


Рис. 2.5. Дополнительные параметры безопасности
для выбранного раздела реестра

Для указанных разделов рекомендуется установить аудит на успешное или неуспешное выполнение

таких действий, как «Запрос значения (Query Value)», «Задание значения (Set Value)», «Запись DAC (Write DAC)» и «Чтение разрешений (Read Control)» для всех пользователей, обладающих административными полномочиями в системе. Можно это сделать и для группы Все (Everyone), но тогда количество записей аудита в журнале безопасности будет больше. Чтобы отслеживать только изменения, можно не следить за событиями типов «Запрос значения (Query Value)» и «Чтение разрешений (Read Control)».

В качестве стартового раздела при выполнении этой операции лучше выбрать SECURITY, поскольку он, кроме всего прочего, включает символическую ссылку на раздел SAM. Таким образом, администратор может проставить нужные параметры аудита для двух указанных разделов одновременно и изменить права доступа к разделам SAM и SECURITY.

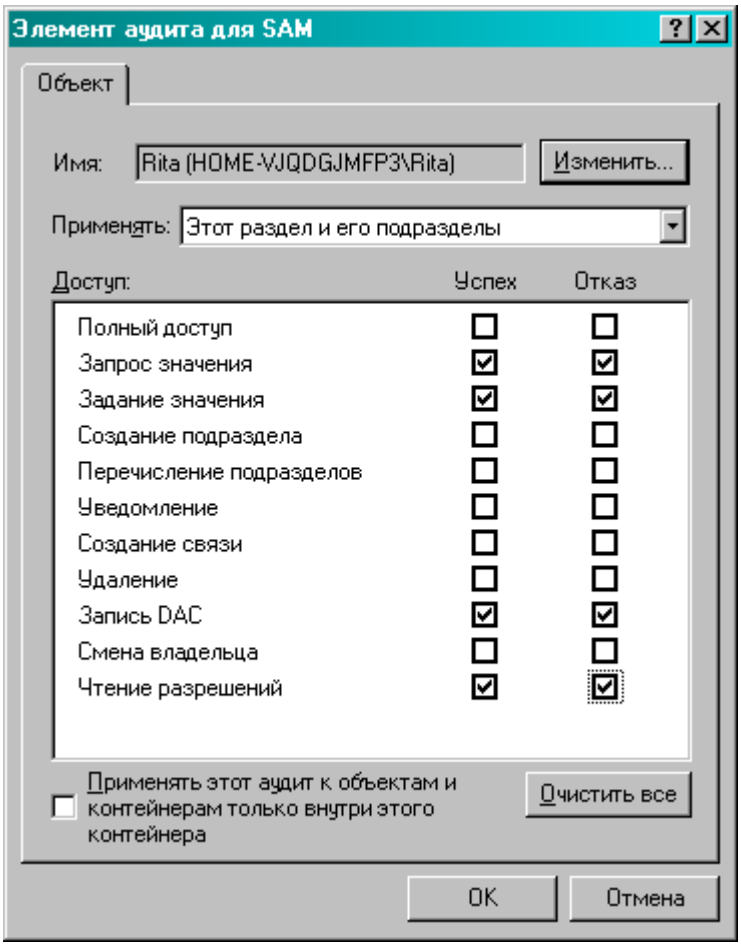


Рис. 2.6. Аудит для отмеченного раздела реестра

.После настройки аудита реестра информация о чтении и модификации параметров соответствующих разделов будет появляться в журнале безопасности Windows.

Записей о событиях категории Object Access может быть довольно велико. Системный администратор должен периодически просматривать и анализировать записи аудита, в том числе те, что относятся к событиям доступа к тому или иному разделу реестра.

2.2.4 Анализ экономических рисков при потенциальных угрозах

овести анализ экономических рисков при потенциальных угрозах для организации с 20 ПК и годовым оборотом 5 млн. руб.

2.3. Порядок выполнения

1. Познакомьтесь с возможностями работы программы Regedit.
2. Познакомьтесь с установками прав на отдельные разделы реестра и приведите установки, сделанные для администратора.

3. Просмотрите права, предоставленные пользователям в указанных разделах реестра.
4. Включите аудит реестра.

2.4. Требования к отчету

Отчет должен оформляться в электронном и печатном виде на листах формата А4 и содержать задание, краткие необходимые теоретические сведения, полученные по каждому пункту задания результаты и выводы.

Контрольные вопросы

1. Каковы основные ветви реестра?
2. Что такое куст?
3. Где и как хранится реестр?
4. Что хранится в основных кустах реестра?
5. Как обеспечивается целостность данных в реестре?
6. Как можно установить (модифицировать) DACL к разделу реестра?
7. Какие права доступа можно установить к разделу реестра?
8. Кто имеет доступ к разделам SAM, Security реестра?
9. Какие вы можете дать рекомендации по усилению защиты реестра?
10. Как установить аудит реестра?
11. Какие события можно отследить с помощью аудита реестра?

Критерии оценки выполнения задания

Оценка	Критерии оценивания
Неудовлетворительно	Работа выполнена не полностью и объем выполненной части работы не позволяет сделать правильных выводов
Удовлетворительно	Работа выполнена не полностью, но не менее 50% объема, что позволяет получить правильные результаты и выводы; в ходе проведения работы были допущены ошибки
Хорошо	Работа выполнена в полном объеме с соблюдением необходимой последовательности действий, но допущена одна ошибка или не более двух недочетов и обучающийся может их исправить самостоятельно или с небольшой помощью преподавателя
Отлично	Работа выполнена в полном объеме без ошибок с соблюдением необходимой последовательности действий

Практическое задание для формирования ПК-2.3

Перечислите основные принципы реализации архитектурного уровня обеспечения информационной безопасности системы с указанием причин необходимости существования этого уровня.

Критерии оценки выполнения задания

Оценка	Критерии оценивания
Неудовлетворительно	Работа выполнена не полностью и объем выполненной части работы не позволяет сделать правильных выводов
Удовлетворительно	Работа выполнена не полностью, но не менее 50% объема, что позволяет получить правильные результаты и выводы; в ходе проведения работы были допущены ошибки

Хорошо	Работа выполнена в полном объеме с соблюдением необходимой последовательности действий, но допущена одна ошибка или не более двух недочетов и обучающийся может их исправить самостоятельно или с небольшой помощью преподавателя
Отлично	Работа выполнена в полном объеме без ошибок с соблюдением необходимой последовательности действий

Практическое задание для формирования ПК-2.3

1. Опишите используемые при реализации политики ИБ стандарты, процессы и правила безопасности и отобразите схематически их взаимосвязь.
2. Перечислите государственные, ведомственные и организационные нормативные акты, регламентирующие защиту информации в издательской деятельности.
3. Перечислите возможные пути и методы несанкционированного доступа к источникам защищаемой информации.
4. Разработайте перечень организационно-правовых методов для построения вербального объекта защиты информации.
5. Отобразите схему разработки политики информационной безопасности для вербального предприятия.

Критерии оценки выполнения задания

Оценка	Критерии оценивания
Неудовлетворительно	Работа выполнена не полностью и объем выполненной части работы не позволяет сделать правильных выводов
Удовлетворительно	Работа выполнена не полностью, но не менее 50% объема, что позволяет получить правильные результаты и выводы; в ходе проведения работы были допущены ошибки
Хорошо	Работа выполнена в полном объеме с соблюдением необходимой последовательности действий, но допущена одна ошибка или не более двух недочетов и обучающийся может их исправить самостоятельно или с небольшой помощью преподавателя
Отлично	Работа выполнена в полном объеме без ошибок с соблюдением необходимой последовательности действий

Практическое задание для формирования ПК-2.3

Постройте иерархическую пирамиду защищаемых ресурсов информационной системы, обозначив 1 - наиболее защищаемый ресурс, 4 - наименее защищаемый ресурс.

Критерии оценки выполнения задания

Оценка	Критерии оценивания
Неудовлетворительно	Работа выполнена не полностью и объем выполненной части работы не позволяет сделать правильных выводов
Удовлетворительно	Работа выполнена не полностью, но не менее 50% объема, что позволяет получить правильные результаты и выводы; в ходе проведения работы были допущены ошибки
Хорошо	Работа выполнена в полном объеме с соблюдением необходимой последовательности действий, но допущена одна ошибка или не более двух недочетов и обучающийся может их исправить самостоятельно или с небольшой помощью преподавателя

Отлично	Работа выполнена в полном объеме без ошибок с соблюдением необходимой последовательности действий

Практическое задание для формирования ПК-2.3

По выбранной теме представить теоретический материал, с приведением конкретных примеров:

1. Общая характеристика ИБ: определение понятий «Информационная безопасность», «Безопасность информации»», «Защита информации».
2. Характеристика свойств безопасности информации: доступности, целостности, конфиденциальности.
3. «Концепция национальной безопасности Российской Федерации «о роли и значении информационной безопасности в общей системе национальной безопасности РФ.
4. Назначение, дата принятия, общая структура «Доктрины информационной безопасности Российской Федерации» (ДИБ РФ).
5. ДИБ РФ: определение понятия «информационная безопасность Российской Федерации» (ИБ РФ).
6. ДИБ РФ: информационные интересы личности, общества и государства в информационной сфере.
7. ДИБ РФ: обобщённые группы информационных интересов РФ.
8. ДИБ РФ: источники и виды угроз информационной безопасности РФ.
9. ДИБ РФ: общее содержание угроз информационной безопасности.
10. ДИБ РФ: основные методы обеспечения ИБ РФ и их краткая характеристика.
11. Особенности методов обеспечения ИБ РФ в сфере экономики.
12. ДИБ РФ: структура и задачи государственной системы обеспечения ИБ РФ.
13. Сущность и содержание правового обеспечения ИБ (ОИБ).
14. Вертикальная структура правового ОИБ: назначение НПА каждого уровня.
15. Горизонтальная структура правового ОИБ: существо и примеры нормативно-правовых актов, содержащих отдельные информационно-правовые нормы в сфере ИБ.
16. Назначение (цели) и общая структура закона РФ «Об информации, информационных технологиях и о защите информации».
17. Назначение (цели) и общая структура закона РФ «О государственной тайне».
18. Назначение (цели) и общая структура закона РФ «О персональных данных».
19. Назначение (цели) и общая структура закона РФ «О коммерческой тайне».
20. Назначение (цели) и общая структура закона РФ «Об электронной цифровой подписи»

1. Краткая характеристика компьютерных систем (КС) как объектов защиты информации (ЗИ).
2. Общая структура, виды КС, особенности каждого вида КС с точки зрения ЗИ.
3. Угрозы безопасности информации (БИ) в КС, основные признаки классификации угроз.
4. Виды и существо случайных (непреднамеренных) угроз БИ в КС.
5. Виды и существо преднамеренных угроз БИ в КС.
6. Общие методы противодействия случайным (непреднамеренным) угрозам БИ в КС.
7. Общие методы противодействия преднамеренным угрозам БИ в КС.
8. Методы дублирования информации как мера защиты от случайных угроз.
9. Повышение надёжности как способ противодействия случайным угрозам БИ в КС.
10. Обеспечение отказоустойчивости как способ противодействия случайным угрозам БИ в КС.

Критерии оценки выполнения задания

Оценка	Критерии оценивания
Неудовлетворительно	Работа выполнена не полностью и объем выполненной части работы не позволяет сделать правильных выводов
Удовлетворительно	Работа выполнена не полностью, но не менее 50% объема, что позволяет получить правильные результаты и выводы; в ходе проведения работы были допущены ошибки

Хорошо	Работа выполнена в полном объеме с соблюдением необходимой последовательности действий, но допущена одна ошибка или не более двух недочетов и обучающийся может их исправить самостоятельно или с небольшой помощью преподавателя
Отлично	Работа выполнена в полном объеме без ошибок с соблюдением необходимой последовательности действий

Вопросы для проведения промежуточной аттестации по итогам освоения дисциплины

Тема 1. Понятие и сущность информационной безопасности и защиты информации

1. Опишите необходимость и значимость нормативно-правовых документов в области информационной безопасности.
2. Дайте определение информационной безопасности и защите информации.
3. Назовите основные компоненты (параметры) информационной безопасности.
4. Перечислите цели и основные задачи в области обеспечения информационной безопасности.

Тема 2. Становление и развитие информационной безопасности и защиты информации

5. Назовите цели и задачи информационной безопасности в Российской Федерации.
6. Опишите связь информационной безопасности с информатизацией общества.
7. Назовите базовые уровни обеспечения информационной безопасности и защиты информации.

Тема 3. Правовой уровень обеспечения информационной безопасности

8. Перечислите основные федеральные органы, генерирующие в Российской Федерации нормативно-правовые акты в сфере ИБ и защиты информации.
9. перечислите основные задачи Межведомственной комиссии по защите государственной тайны в формировании перечня сведений, составляющих государственную тайну.
10. Значение обеспечения безопасности коммерческой тайны в системе предпринимательской деятельности.
11. Опешите порядок отнесения сведений к коммерческой тайне.
12. Порядок формирования на фирме перечня сведений, относящихся к коммерческой тайне.

Тема 4. Информационная безопасность в системе национальной безопасности РФ

13. Дайте определение национальная безопасность.
14. Назовите виды безопасности и дайте им определение: экономическая внутриполитическая, социальная, военная. международная, информационная, экологическая.
15. Перечислите виды защищаемой информации.
16. Назначение и роль информационной безопасности в обеспечение национальной безопасности государства.

Тема 5. Основы государственной политики РФ в области информационной безопасности

17. Перечислите национальные интересы РФ в информационной сфере и методы их обеспечения.
18. Перечислите виды угроз национальной безопасности РФ.
19. Назовите возможные сценарии подрыва национальных интересов РФ.

Тема 6. Основные угрозы информационной безопасности

20. Проведите классификацию источников угроз безопасности информации по принципу и характеру его воздействия на объект защиты.
21. Перечислите методы и способы воздействия источников угроз на объект защиты в зависимости от используемых средств нападения.
22. Проведите классификацию угроз безопасности информации по степени нарушения состояния информационной безопасности (доступности, целостности, конфиденциальности).
23. Назовите возможные каналы несанкционированного доступа к информационным ресурсам в информационной системе.
24. Перечислите цели и задачи по защите информационных ресурсов от несанкционированного доступа в соответствии с нормативно-правовыми документами России.

Тема 7. Методы и средства обеспечения информационной безопасности и защиты информации

25. Перечислите правовые, и организационные методы обеспечения информационной безопасности

26. Перечислите технические методы обеспечения информационной безопасности
27. Перечислите экономические методы обеспечения информационной безопасности.
28. Назовите модели и системы обеспечения информационной безопасности.
29. Перечислите классы защищенности от несанкционированного доступа к средствам вычислительной техники и автоматизированным системам.

Тема 8. Административный уровень обеспечения информационной безопасности и защиты информации

30. Перечислите концептуальные основы обеспечения информационной безопасности.
31. Назовите состав, структуру и содержимое документа политика информационной безопасности
32. Перечислите задачи, решаемые при анализе рисков для информационных систем.
33. Назовите базовые методики, используемые для оценки рисков.
34. Перечислите основные стандарты в области разработки политики информационной безопасности и анализа рисков.
35. Перечислите базовые инструментальные средства для анализа рисков и управления рисками.

Тема 9. Процедурный уровень обеспечения информационной безопасности и защиты информации

36. Основные классы мер процедурного уровня
37. Управление персоналом
38. Физическая защита
39. Поддержание работоспособности
40. Реагирование на нарушения режима безопасности
41. Планирование восстановительных работ

Тема 10. Аппаратно-программный уровень обеспечения информационной безопасности и защиты информации

42. Программно-аппаратные сервисы обеспечения безопасности информационных ресурсов в информационных системах.
43. Идентификация и аутентификация пользователей как передовой рубеж защиты информации.
44. Базовые методы парольной аутентификации. Модели разграничения доступа к информации.
45. Протоколирование и аудит (активный и пассивный) ИС, их основные цели и особенности.
46. Базовые методы криптографического преобразования данных.
47. Потоковое и блочное шифрование.
48. Процедура формирования электронной подписи.
49. Экранирование информации в информационно-телекоммуникационных сетях (ИТС).
50. Основные сервисы защиты в ИТС.
51. Компьютерные вирусы и вредоносные программы: классификация, методы и средства борьбы с ними. Антивирусные программные комплексы.

Уровни и критерии итоговой оценки результатов освоения дисциплины

	Критерии оценивания	Итоговая оценка
Уровень 1. Недостаточный	Незнание значительной части программного материала, неумение даже с помощью преподавателя сформулировать правильные ответы на задаваемые вопросы, невыполнение практических заданий	Неудовлетворительно/ Незачтено
Уровень 2. Базовый	Знание только основного материала, допустимы неточности в ответе на вопросы, нарушение логической последовательности в изложении программного материала, затруднения при решении практических задач	Удовлетворительно/ зачтено

Уровень 3. Повышенный	Твердые знания программного материала, допустимые несущественные неточности при ответе на вопросы, нарушение логической последовательности в изложении программного материала, затруднения при решении практических задач	Хорошо/ зачтено
Уровень 4. Продвинутый	Глубокое освоение программного материала, логически стройное его изложение, умение связать теорию с возможностью ее применения на практике, свободное решение задач и обоснование принятого решения	Отлично/ зачтено