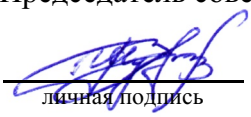
Аккредитованное образовательное частное учреждение высшего образования
«Московский финансово-юридический университет МФЮА»

Рассмотрено и одобрено на заседании учебно-методического совета

Протокол № 11 от 26.07.2021

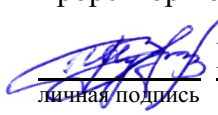
Председатель совета



личная подпись В.В. Шутенко
инициалы, фамилия

УТВЕРЖДАЮ

Проректор по учебной работе



личная подпись В.В. Шутенко
инициалы, фамилия

« 26 » июля 2021 г.

Гудов Геннадий Николаевич
(уч. звание, степень, ФИО авторов программы)

Рабочая программа дисциплины (модуля)

Информационная безопасность
(наименование дисциплины (модуля))

Направление подготовки (специальность): 38.05.01 Экономическая безопасность
(код, наименование без кавычек)

ОПОП: Судебная экономическая экспертиза
(наименование)

Форма освоения ОПОП: очная, очно-заочная, заочная
(очная, очно-заочная, заочная)

Общая трудоемкость: 4 (з.е.)

Всего учебных часов: 144 (ак. час.)

Формы промежуточной аттестации	СЕМЕСТР		
	очная	очно-заочная	заочная
Дифференцированный зачет	5	5	5

Москва 2021 г.

Год начала подготовки студентов - 2021

1. Цель и задачи освоения дисциплины

Цель освоения дисциплины	формирование у студентов системы знаний в области информационной безопасности и применения на практике методов и средств защиты информации.
Задачи дисциплины	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

Блок 1 «Дисциплины (модули)»	
Дисциплины и практики, знания и умения по которым необходимы как "входные" при изучении данной дисциплины	Административное право Информационные системы в экономике Предпринимательское право Программные комплексы решения интеллектуальных задач Уголовное право Экономическая теория
Дисциплины, практики, ГИА, для которых изучение данной дисциплины необходимо как предшествующее	Управление трудовыми ресурсами Финансовая безопасность Экономическая безопасность

3. Требования к результатам освоения дисциплины

Компетенции обучающегося, формируемые в результате освоения дисциплины. Степень сформированности компетенций

Индикатор	Название	Планируемые результаты обучения	ФОС
ПК2 Способен формировать, анализировать и оценивать информацию, необходимую для принятия решений по обеспечению экономической безопасности			
ПК-2.1	Знать: принципы построения и использования информационных баз, методы и приемы анализа информации	Студент должен знать принципы построения и использования информационных баз, методы и приемы анализа информации.	Тест
ПК-2.2	Уметь: находить и формировать информационную базу, необходимую для обеспечения экономической безопасности	Студент должен уметь находить и формировать информационную базу, необходимую для обеспечения экономической безопасности.	Выполнение реферата
ПК-2.3	Уметь: анализировать и оценивать полученную информацию, необходимую для нейтрализации угроз экономической безопасности	Студент должен уметь анализировать и оценивать полученную информацию, необходимую для нейтрализации угроз экономической безопасности	Практическое задание

4. Структура и содержание дисциплины

Тематический план дисциплины

№	Название темы	Содержание	Литера-тура	Индикаторы
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.	9.2.1, 9.1.1, 9.2.2, 9.1.2, 9.2.3, 9.1.3	ПК-2.1 ПК-2.2 ПК-2.3
2.	Становление и развитие понятия «информационная безопасность»	Связь ИБ с информатизацией общества. Базовые уровни обеспечения ИБ и защиты информации.	9.2.1, 9.1.1, 9.2.2, 9.1.2, 9.2.3, 9.1.3	ПК-2.1 ПК-2.2 ПК-2.3
3.	Правовой уровень обеспечения информационной безопасности	Основные федеральные органы, генерирующие в Российской Федерации нормативно-правовые акты в сфере ИБ 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. Степени конфиденциальности сведений, составляющих коммерческую тайну. Методика формирования на фирме перечня сведений, относящихся к коммерческой тайне.	9.2.1, 9.1.1, 9.2.2, 9.1.2, 9.2.3, 9.1.3	ПК-2.1 ПК-2.2 ПК-2.3
4.	Информационная безопасность в системе национальной безопасности РФ	Понятие национальной безопасности. Виды безопасности: экономическая внутриполитическая, социальная, военная. международная, информационная, экологическая и другие. Соотношение безопасности личности, общества и государства. Виды защищаемой информации. Роль информационной безопасности в обеспечение национальной безопасности государства.	9.2.1, 9.1.1, 9.2.2, 9.1.2, 9.2.3, 9.1.3	ПК-2.1 ПК-2.2 ПК-2.3
5.	Основы государственной политики РФ в области информационной безопасности	Национальные интересы РФ в информационной сфере и их обеспечение. Виды угроз национальной безопасности РФ. Возможные сценарии подрыва национальных интересов РФ.	9.2.1, 9.1.1, 9.2.2, 9.1.2, 9.2.3, 9.1.3	ПК-2.1 ПК-2.2 ПК-2.3

6.	Информационная война, методы и средства её ведения	Информационная безопасность и информационное противоборство. Информационное оружие, его классификация и возможности. Методы нарушения конфиденциальности, целостности и доступности информации. Причины, виды, каналы утечки и искажения информации.	9.2.1, 9.1.1, 9.2.2, 9.1.2, 9.2.3, 9.1.3	ПК-2.1 ПК-2.2 ПК-2.3
7.	Методы и средства обеспечения ИБ объектов информационной сферы	Правовые, организационно-технические и экономические методы обеспечения ИБ. Модели, стратегии и системы обеспечения ИБ. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем.	9.2.1, 9.1.1, 9.2.2, 9.1.2, 9.2.3, 9.1.3	ПК-2.1 ПК-2.3 ПК-2.2
8.	Основные угрозы информационной безопасности	Классификация угроз безопасности по цели реализации угрозы, принципу, характеру и способу её воздействия. Особенности угроз воздействия на объект атаки в зависимости от его состояния и используемых средств атаки. Основные методы и каналы несанкционированного доступа к информации в информационной системе (ИС). Базовые принципы защиты от несанкционированного доступа к информации в соответствии с нормативно-правовыми документами России. Задачи по защите ИС от реализации угроз.	9.2.1, 9.1.1, 9.2.2, 9.1.2, 9.2.3, 9.1.3	ПК-2.1 ПК-2.2 ПК-2.3
9.	Административный уровень обеспечения информационной безопасности	Концепция ИБ, её цели и этапы построения. Политика информационной безопасности (ПИБ) как основа административных мер по защите информации на предприятии. Структура документа, характеризующего политику безопасности, и основные этапы разработки ПИБ. Задачи, решаемые при анализе рисков для ИС. Базовые методики, используемые для оценки рисков. Основные стандарты в области разработки ПИБ и анализа рисков. Базовые инструментальные средства для анализа рисков и управления рисками. Основные принципы реализации ПИБ.	9.2.1, 9.1.1, 9.2.2, 9.1.2, 9.2.3, 9.1.3	ПК-2.1 ПК-2.2 ПК-2.3

10.	Программно-технический уровень обеспечения защиты информации	Программные сервисы защиты информации в ИС. 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. Потоковое и блочное шифрование. Процедура формирования электронной подписи. Экранирование информации в информационно-телекоммуникационных сетях (ИТС). Основные сервисы защиты в ИТС. Компьютерные вирусы и вредоносные программы: классификация, методы и средства борьбы с ними. Антивирусные программные комплексы.	9.2.1, 9.1.1, 9.2.2, 9.1.2, 9.2.3, 9.1.3	ПК-2.1 ПК-2.2 ПК-2.3

Распределение бюджета времени по видам занятий с учетом формы обучения

Форма обучения: очная, 5 семестр

№	Контактная работа	Аудиторные учебные занятия			Самостоятельная работа
		занятия лекционного типа	лабораторные работы	практические занятия	
1.	3	1	0	2	6
2.	3	1	0	2	6
3.	4	2	0	2	8
4.	6	2	0	4	8
5.	6	2	0	4	8
6.	6	2	0	4	8
7.	6	2	0	4	10
8.	6	2	0	4	10
9.	6	2	0	4	10
10.	6	2	0	4	12
	Промежуточная аттестация				
	2	0	0	0	4
	Консультации				
	0	0	0	0	0
Итого	54	18	0	34	90

Форма обучения: очно-заочная, 5 семестр

№	Контактная работа	Аудиторные учебные занятия			Самостоятельная работа
		занятия лекционного типа	лабораторные работы	практические занятия	
1.	1	1	0	0	8
2.	1	1	0	0	8
3.	2	1	0	1	10
4.	2	1	0	1	12
5.	2	1	0	1	12

6.	2	1	0	1	12
7.	3	1	0	2	12
8.	3	1	0	2	12
9.	4	2	0	2	14
10.	4	2	0	2	14
	Промежуточная аттестация				
	2	0	0	0	4
	Консультации				
	0	0	0	0	0
Итого	26	12	0	12	118

Форма обучения: заочная, 5 семестр

№	Контактная работа	Аудиторные учебные занятия			Самостоятельная работа
		занятия лекционного типа	лабораторные работы	практические занятия	
1.	0	0	0	0	10
2.	0	0	0	0	12
3.	1	0.5	0	0.5	12
4.	1	0.5	0	0.5	12
5.	1.5	0.5	0	1	12
6.	1.5	0.5	0	1	12
7.	1.5	0.5	0	1	14
8.	1.5	0.5	0	1	14
9.	1.5	0.5	0	1	14
10.	2.5	0.5	0	2	14
	Промежуточная аттестация				
	2	0	0	0	4
	Консультации				
	0	0	0	0	0
Итого	14	4	0	8	130

5. 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.

6. Фонды оценочных средств для текущего контроля успеваемости, промежуточной аттестации и самоконтроля по итогам освоения дисциплины

Технология оценивания компетенций фондами оценочных средств:

- формирование критериев оценивания компетенций;
- ознакомление обучающихся в ЭИОС с критериями оценивания конкретных типов оценочных средств;
- оценивание компетенций студентов с помощью оценочных средств;
- публикация результатов освоения ОПОП в личном кабинете в ЭИОС обучающегося;

Тест для формирования «ПК-2.1»

Вопрос №1 .

Виды компьютерных сетей.

Варианты ответов:

1. Локальные, региональные, глобальные.
2. Проводные, беспроводные.
3. С централизованным управлением, децентрализованные сети.
4. Всё вышеперечисленное.

Вопрос №2 .

Средства информационной технологии.

Варианты ответов:

1. Это технические, программные, информационные и другие средства, при помощи которых реализуется информационная технология.
2. Это - инструменты, машины, механизмы, автоматические устройства.
3. Это средства, которые облегчают и обеспечивают офисную и инженерно-техническую работу, копировальное и проектное оборудование.

Вопрос №3 .

Виртуальная реальность.

Варианты ответов:

1. Это модельное отображение квазиреальности с помощью определенных технологий и технических средств, позволяющих обеспечить частичное или полное погружение человека в это отображение.
2. Искусственно созданная компьютерными средствами среда, в которую можно проникать, меняя ее изнутри, наблюдая трансформации и испытывая при этом реальные ощущения.
3. Оба варианта верны.

Вопрос №4 .

Техническая и программная платформы.

Варианты ответов:

1. Оборудования, на которое можно установить информационную технологию.
2. Тип компьютера, определяемый типом процессора и операционная система.
3. Специальные программные средства.

Вопрос №5 .

Схема программы.

Варианты ответов:

1. Графическое представление определения, анализа или метода решения задачи.
2. Отображает последовательность операций в программе, то есть ее алгоритм.
3. Отображает управление операциями и потоками данных и представляет технологический процесс обработки данных в экономических информационных системах.
4. Это горизонтальный список объектов на экране, представляющих группу действий, доступных пользователю для выбора.

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 «ПК-2.2»

Цели и задачи защиты информации.

Проблемы защиты информации.

Этапы развития концепции обеспечения безопасности информации.

Общие теоретические принципы теории безопасности.

Общие методические принципы теории безопасности.

Проблемы информационного противоборства.

Государственная политика в информационной сфере.

Региональные проблемы информационной безопасности.

Современная доктрина информационной безопасности Российской Федерации.

Современная концепция информационной безопасности.

Основное содержание теории защиты информации.

Общеметодологические принципы формирования теории защиты информации.

Модели систем и процессов защиты информации.

Особенности и состав научно-методологического базиса решения задач защиты информации.

Нечеткие множества.

Нестрогая математика.

Методы оценки.

Неформальный поиск оптимальных решений.

Требования системного подхода к защите информации.

Условия обеспечения требований безопасности. Виды обеспечения системы информационной безопасности.

Концептуальная модель информационной безопасности.

Критерии, условия и принципы отнесения информации к защищаемой.

Количественная и качественная оценки ценности информации. Категории важности информации.

Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности: государственная тайна, коммерческая тайна, коммерческая информация, персональная информация, информация для внутреннего пользования и др.

Виды и типы угроз безопасности.

Классификацияугроз.

Классификация угроз конфиденциальности, целостности и доступности информации.

Изменение активности угроз в зависимости от стадии жизненного цикла.

Формирование и коррекция кортесов

потенциальных угроз.

Источники, виды и методы дестабилизирующего во

здействия на защищаемую информацию.

Причины, обстоятельства и условия, вызывающие дестабилизирующее воздействие на защищаемую информацию.

Виды уязвимости информации и формы ее проявления.

Каналы несанкционированного получения информации.

Радиоканалы утечки информации.

Акустические каналы утечки информации.

Электрические каналы утечки информации.

Визуально-оптические каналы утечки информации.

Материально-вещественные каналы утечки информации.

Линии связи.

Каналы утечки информации при эксплуатации ЭВМ.

Методы и средства несанкционированного получения информации по техническим каналам.

Методы и средства разрушения информации.

Направления, виды и особенности деятельности спецслужб по несанкционированному доступу к конфиденциальной информации.

Система мер, направленных на обеспечение информационной безопасности.

Подходы к созданию комплексной системы защиты информации.

Виды защиты информации. Характеристики защитных действий.

Кадровое и ресурсное обеспечение защиты информации.

Современные методы и средства оценивания состояния безопасности информационных систем: препятствие, управление доступом, маскировка, регламентация, принуждение, побуждение.

Классификация средств защиты информации.

Технические средства защиты информации.

Программные средства защиты.

Программно-технические средства защиты.

Криптографическая защита.

Скремблирование.

Стеганография.

Законодательные средства.

Организационные средства защиты.

Морально-этические средства.

Кадровое и ресурсное обеспечение защиты информации.

Построение систем защиты информации.

Определение и общеметодологические принципы построения систем защиты информации.

Основы архитектурного построения систем защиты.

Функциональное, организационное и структурное построение систем защиты информации.

Типизация систем защиты.

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 «ПК-2.2»

1. Классификация информации. Виды данных и носителей.

2. Ценность информации. Цена информации.

3. Количество и качество информации.

4. Виды защищаемой информации.

5. Демаскирующие признаки объектов защиты.

6. Классификация источников и носителей информации.

7. мероприятия по управлению доступом к информации.

8. Функциональные источники сигналов. Опасный сигнал.

9. Основные средства и системы, содержащие потенциальные источники опасных сигналов.

10. Вспомогательные средства и системы, содержащие потенциальные источники опасных сигналов.

11. Виды паразитных связей и наводок, характерные для любых радиоэлектронных средств и проводов, соединяющих их кабелей.

12. Виды угроз безопасности информации.

13. Основные принципы добывания информации.

14. Процедура идентификации, как основа процесса обнаружения объекта.

15. Методы синтеза информации.

16. Методы несанкционированного доступа к информации.

17. Основными способами привлечения сотрудников государственных и коммерческих структур, имеющих доступ к интересующей информации.

18. Способы наблюдения с использованием технических средств.

19. Каналы утечки информации. Технические каналы утечки

20. Классификация технических каналов утечки по физической природе носителя.

21. Классификация технических каналов утечки по информативности.

22. Классификация технических каналов утечки по времени функционирования.

23. Классификация технических каналов утечки по структуре.

24. Наблюдение в оптическом диапазоне и применяемые для этого средства. Характеристики таких средств.

25. Перехват электромагнитных излучений.

26. Акустическое подслушивание. Эффекты, возникающие при подслушивании.

27. Понятия скрытия информации, виды скрытий. Информационный портрет.

28. Противодействие наблюдению. Способы маскировки.

29. Способы и средства противодействия подслушиванию.

30. Нейтрализация закладных устройств.

31. Состав инженерной защиты и технической охраны объектов.

32. Инженерные конструкции и сооружения для защиты информации. Их классификация.

33. Средства идентификации личности.

34. Классификация датчиков охранной сигнализации.

35. Классификация извещателей.

36. Телевизионные системы наблюдения.

37. Основные средства системы видеоконтроля.

38. Защита личности как носителя информации.

39. Системный подход к защите 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 «ПК-2.2»

15. Общие понятия, история развития и классификация криптографических средств.

16. Общая характеристика различных методов шифрования. Криптостойкость. Шифрование с симметричным и несимметричным ключами.

17. Различные методы шифрования.

18. Отечественные и зарубежные стандарты шифрования.

19. Общая характеристика и классификация компьютерных вирусов.

20. Механизм заражения файловыми и загрузочными вирусами. Особенности макровирусов.

21. Средства, используемые для обнаружения компьютерных вирусов.

22. Профилактика заражения компьютерными вирусами.

23. Антивирусные средства для лечения и удаления компьютерных вирусов. Программы-полифаги. Эвристические анализаторы.

24. Содержательный смысл понятия комплексной системы защиты информации (КСЗИ) в компьютерных системах. Основные принципы и положения, реализующие системный подход к построению КСЗИ.

25. Основные технологические этапы разработки КСЗИ.

26. Организационно-технические мероприятия, проводимые в процессе эксплуатации КСЗИ.

27. Задачи, решаемые подсистемой аудита в составе защищенных КС.

28. Международные стандарты в области информационной безопасности. Основные положения. Основные положения РД Гостехкомиссии РФ (Пятикнижие).

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. Понятие информационной безопасности. Информационная безопасность личности, общества и государства. Конфиденциальная информация.

2. Информационная безопасность как составляющая национальной безопасности. Задачи государства в этой области. Информационное оружие, информационные войны и терроризм. Государственные органы РФ, реализующие функции обеспечения информационной безопасности.

3. Компьютерная система (КС) как объект защиты информации. Угрозы

информационной безопасности в КС. Классификация угроз.

4. Общая характеристика угроз доступности.

5. Общая характеристика угроз целостности.

6. Общая характеристика угроз конфиденциальности.

7. Обобщенные модели системы защиты информации в КС. Одноуровневые и многоуровневые модели. Общая характеристика средств и методов защиты информации в КС.

8. Общая характеристика организационных мероприятий, обеспечивающих

информационную безопасность КС. Основные задачи службы безопасности.

9. Отечественное законодательство в области информации и защиты информации.

10. Минимизация ущерба, наносимого КС авариями и стихийными бедствиями. Дублирование информации. Технология RAID. Резервирование технических средств.

11. Общая характеристика технических каналов утечки информации в КС.

12. Базовые принципы, лежащие в основе моделей политики безопасности в КС. Матричная (дискреционная) модель и мандатная (полномочная) модель управления доступом к ресурсам КС.

13. Средства и методы разграничения доступа к ресурсам КС.

14. Защита программных средств КС от несанкционированного копирования и исследования.

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.Информатизация управления транспортной безопасностью.

32.Биопаспорт.

33.Обзор современных платформ архивации данных.

34.Что такое консалтинг в области ИБ.

35.Бухгалтерская отчетность как источник рассекречивания информации.

36.Управление рисками: обзор употребительных подходов.

37.Категорирование информации и информационных систем. Обеспечение базового уровня информационной безопасности.

38.Распределенные атаки на распределенные системы.

39.Оценка безопасности автоматизированных систем.

40.Windows и Linux: что безопаснее?

41.Функциональная безопасность программных средств.

42.Технологические процессы и стандарты обеспечения функциональной безопасности в жизненном цикле программных средств.

43.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»

Определите, к какому виду информации в зависимости от порядка ее предоставления или распространения относится информация в ситуации: государственный фонд данных государственного экологического мониторинга включает в себя: информацию, содержащуюся в базах данных подсистем единой системы государственного экологического мониторинга; результаты производственного контроля в области охраны окружающей среды и государственного экологического надзора; данные государственного учета объектов, оказывающих негативное воздействие на окружающую среду.

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»

Укажите, какой вид электронной подписи должен использоваться при обмене электронными документами между работодателем и дистанционным работником?

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»

Проведите анализ информационно-правовой нормы и определите вид формы предписания: организация должна определять действия, необходимые для устранения причин потенциальных несоответствий требованиям системы менеджмента информационной безопасности, с целью предотвратить их повторное появление.

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»

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.

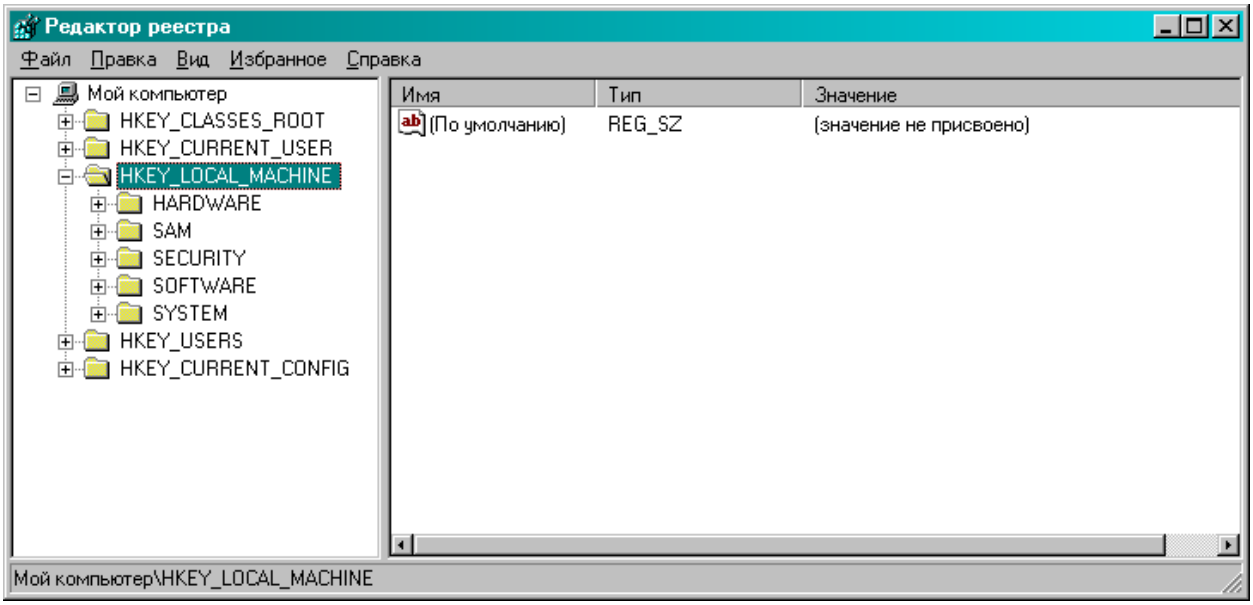


Рис. 2.1. Редактор реестра

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

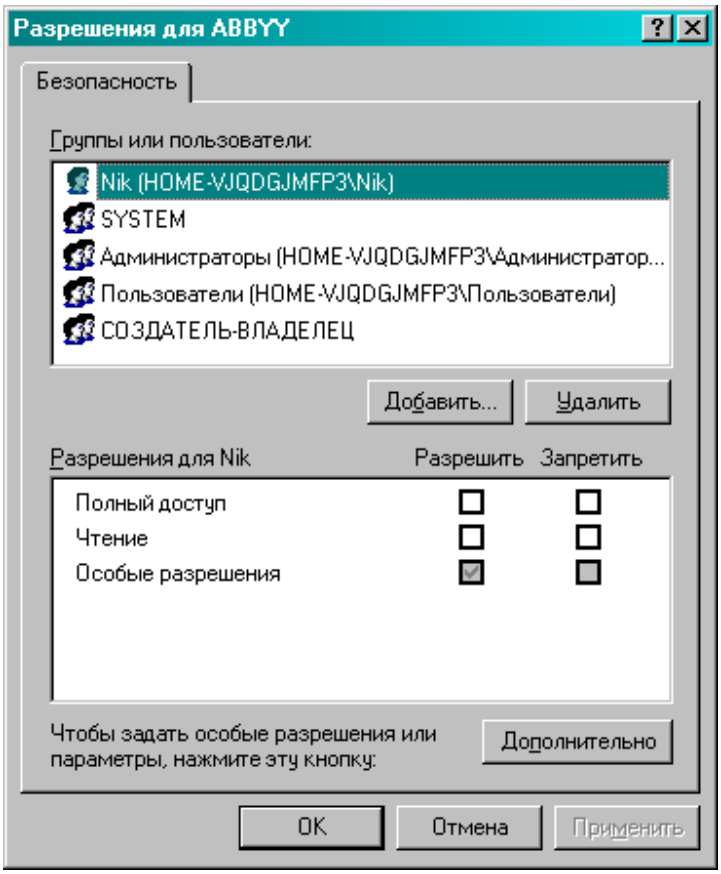


Рис. 2.2. Задание разрешений для папок

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).

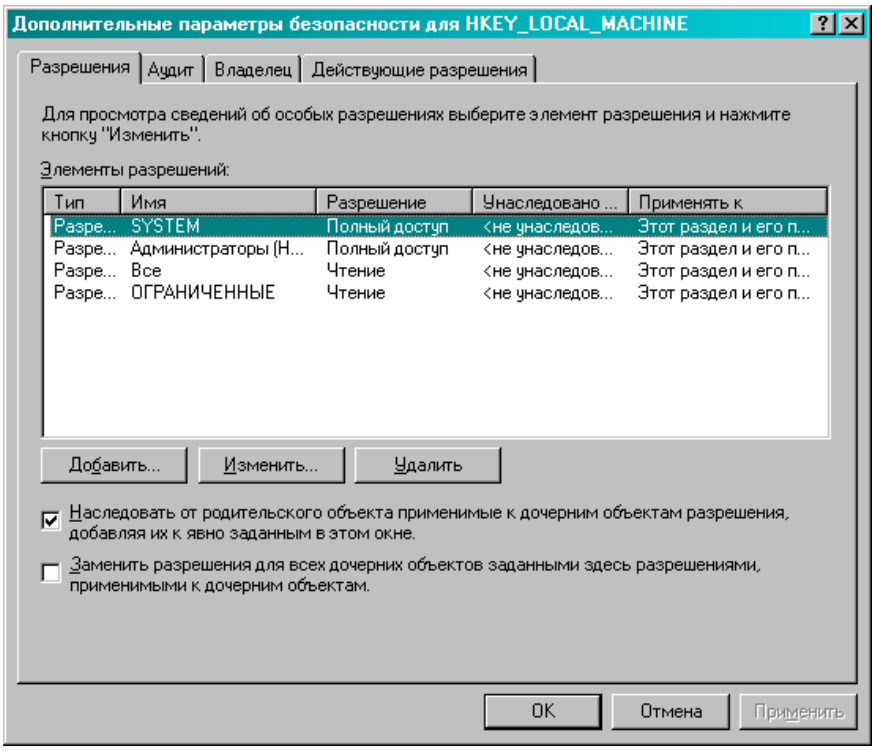


Рис. 2.3. Окно дополнительных параметров безопасности

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

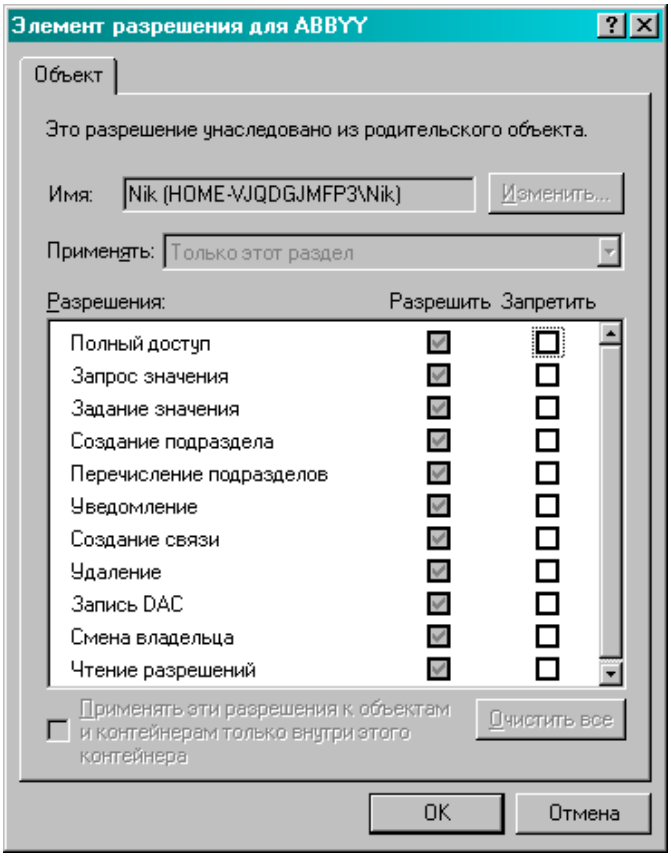


Рис. 2.4. Разрешения/запрет для доступа к объекту

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).

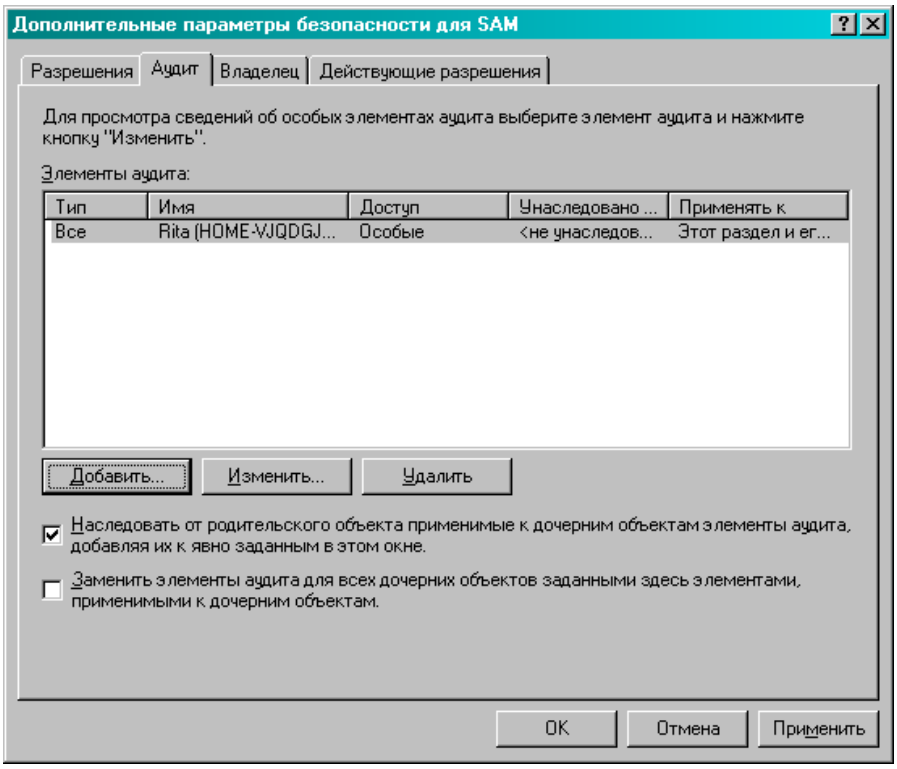


Рис. 2.5. Дополнительные параметры безопасности

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.

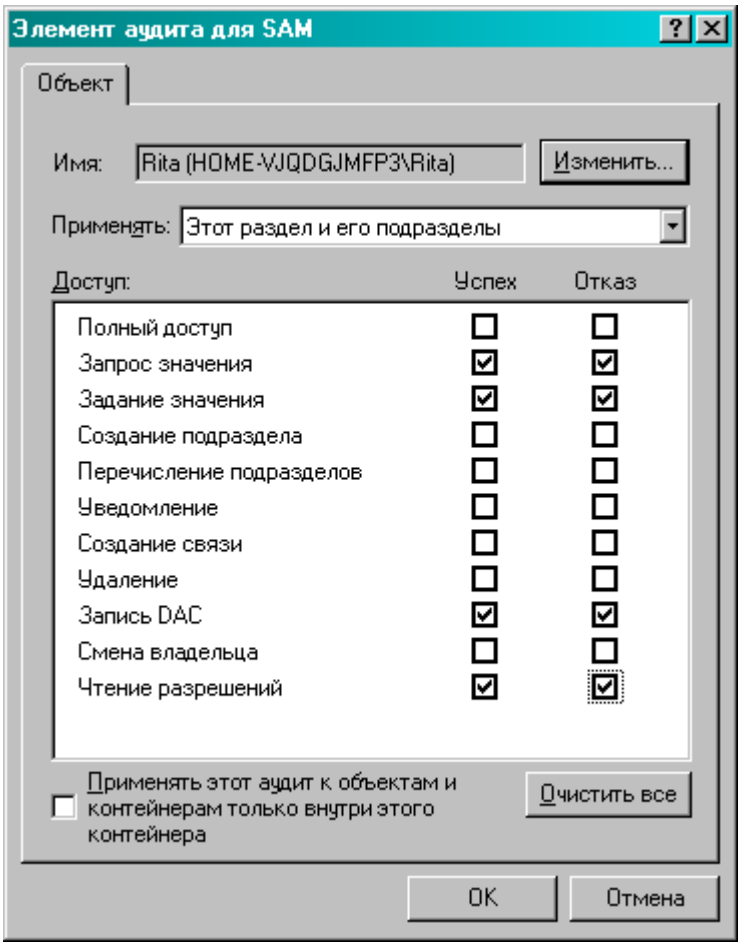


Рис. 2.6. Аудит для отмеченного раздела реестра

.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»

Задача 1. Защита документа в Microsoft Excel. Изучить возможности ограничения просмотра и изменения пользователями данных в электронных таблицах.

Задания:

1. Открыть несколько книг, скрыть одну из них.

2. Отобразить скрытую книгу

3. Скрыть лист.

4. Скрыть изображение столбца.

5. Отобразить скрытый столбец.

6. Скрыть изображение строки.

7. Отобразить скрытую строку.

Задача 2. Работа с реестром ОС. Изучить основные принципы работы с реестром, освоить редактор реестра, научиться создавать резервные копии как реестра целиком, так и его отдельных ключей

Задания:

1. Сохранить значение всей ветви HKEY_CLASSES_ROOT.

2. Включе HKEY_CLASSES_ROOT найтиветвьlnkfile. Одним из ее параметров является IsShortcut. Удалите его. Аналогичную процедуру повторите с ветвью piffile. Перезагрузите компьютер. Обратите

внимание, что исчезли все стрелки с ярлыков программ.

3. Восстановить значение ветви HKEY_CLASSES_ROOT.

4. Создать резервную копию файла реестра.

5. Откройте ключ реестра HKEY_CURRENT_USER, а затем его подключите \ControlPanel\Desktop. Добавьте к открытому ключу новое строковое значение с именем MenuShowDelay. Дважды щелкните мышью, указав на это значение и введите число 1. Затем перезагрузите систему. Теперь меню, запрашиваемые с панели задач, будут появлять-ся гораздо быстрее.

6. Восстановите реестр с резервной копии.

7. С помощью программы MicrosoftBackup создать копию реестра, а затем по этой копии восстановить реестр.

8. Перезагрузите систему и убедитесь, что она функционирует нормально.

Задача 3. Использование архиваторов для защиты информации.

Задания:

1. Выделить группы архивируемых файлов в WinRAR.

2. Создать различных типов архивов в WinRAR и работа с ними.

3. Выполнить шифрование информации в WinRAR.

Задача 4. Изучение основных принципов уничтожения и восстановления информации на магнитных дисках, знакомство с используемыми утилитами, входящими в пакет NortonUtilities.

Задания:

1. Написать командный файл, при запуске которого произойдет затирание файлов с расширением BAK на жестком диске C. Использовать программу WipeInfo.

2. Удалить на жестком диске несколько файлов, а затем попытаться с помощью программы UnErase восстановить их. Поэкспериментировать для случая, когда файлы удаляются вместе с подкаталогами, содержащими их.

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

Тема 2. Становление и развитие понятия «информационная безопасность»

4. Связь ИБ с информатизацией общества.

5. Базовые уровни обеспечения ИБ и защиты информации.

Тема 3. Правовой уровень обеспечения информационной безопасности

6. Основные федеральные органы, генерирующие в Российской Федерации нормативно-правовые акты в сфере ИБ и защиты информации.
7. Роль в России Межведомственной комиссии по защите государственной тайны в формировании перечня сведений, составляющих государственную тайну. Место коммерческой тайны в системе предпринимательской деятельности.
8. Основания и методика отнесения сведений к коммерческой тайне.
9. Степени конфиденциальности сведений, составляющих коммерческую тайну.
10. Методика формирования на фирме перечня сведений, относящихся к коммерческой тайне.

Тема 4. Информационная безопасность в системе национальной безопасности РФ

11. Понятие национальной безопасности
12. Виды защищаемой информации
13. Соотношение безопасности личности, общества и государства.
14. Роль информационной безопасности

Тема 5. Основы государственной политики РФ в области информационной безопасности

15. Национальные интересы РФ в информационной сфере
16. Виды угроз национальной безопасности РФ
17. Какие возможные сценарии подрыва национальных интересов РФ

Тема 6. Информационная война, методы и средства её ведения

18. Информационное оружие, его классификация и возможности
19. Целостности и доступности информации
20. Причины, виды, каналы утечки и искажения информации

Тема 7. Методы и средства обеспечения ИБ объектов информационной сферы

21. Что такое ИБ (Информационная Безопасность)
22. Правовые, организационно-технические и экономические методы обеспечения ИБ
23. Модели, стратегии и системы
24. обеспечения ИБ

Тема 8. Основные угрозы информационной безопасности

25. Классификация угроз безопасности по цели реализации угрозы, принципу, характеру и способу её воздействия.
26. Особенности угроз воздействия на объект атаки в зависимости от его состояния и используемых средств атаки.
27. Основные методы и каналы несанкционированного доступа к информации в информационной системе (ИС).
28. Базовые принципы защиты от несанкционированного доступа к информации в соответствии с нормативно-правовыми документами России.
29. Задачи по защите ИС от реализации угроз.

Тема 9. Административный уровень обеспечения информационной безопасности

30. Концепция ИБ, её цели и этапы построения.
31. Политика информационной безопасности (ПИБ) как основа административных мер по защите информации на предприятии.
32. Структура документа, характеризующего политику безопасности, и основные этапы разработки ПИБ.
33. Задачи, решаемые при анализе рисков для ИС.
34. Базовые методики, используемые для оценки рисков.
35. Основные стандарты в области разработки ПИБ и анализа рисков.
36. Базовые инструментальные средства для анализа рисков и управления рисками.
37. Основные принципы реализации ПИБ.

Тема 10. Программно-технический уровень обеспечения защиты информации

38. Программные сервисы защиты информации в ИС.
39. Идентификация и аутентификация пользователей как передовой рубеж защиты информации.
40. Базовые методы парольной аутентификации. Модели разграничения доступа к информации.
41. Протоколирование и аудит (активный и пассивный) ИС, их основные цели и особенности.
42. Базовые методы криптографического преобразования данных.
43. Потоковое и блочное шифрование.
44. Процедура формирования электронной подписи.
45. Экранирование информации в информационно-телекоммуникационных сетях (ИТС).
46. Основные сервисы защиты в ИТС.
47. 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
Уровень1. 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

7. Ресурсное обеспечение дисциплины

Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства	1. Microsoft Windows (лицензионное программное обеспечение) 2. Microsoft Office (лицензионное программное обеспечение) 3. Google Chrome (свободно распространяемое программное обеспечение) 4. Kaspersky Endpoint Security (лицензионное программное обеспечение) 5. Спутник (свободно распространяемое программное обеспечение отечественного производства) 6. AnyLogic (свободно распространяемое программное обеспечение) 7. Microsoft Visual Studio (лицензионное программное обеспечение) 8. iTALC (свободно распространяемое программное обеспечение) 9. ArgoUML (свободно распространяемое программное обеспечение) 10. ARIS EXPRESS (свободно распространяемое программное обеспечение) 11. Erwin (свободно распространяемое программное обеспечение) 12. Inkscape (свободно распространяемое программное обеспечение) 13. Maxima (свободно распространяемое программное обеспечение) 14. Microsoft SQL Server Management Studio (лицензионное программное обеспечение) 15. Microsoft Visio (лицензионное программное обеспечение) 16. MPLAB (свободно распространяемое программное обеспечение) 17. Notepad++ (свободно распространяемое программное обеспечение) 18. Oracle VM VirtualBox (свободно распространяемое программное обеспечение) 19. Paint .NET (свободно распространяемое программное обеспечение) 20. SciLab (свободно распространяемое программное обеспечение) 21. WinAsm (свободно распространяемое программное обеспечение) 22. GNS 3 (свободно распространяемое программное обеспечение) 23. Консультант+ (лицензионное программное обеспечение отечественного производства) 24. Prolog (свободно распространяемое программное обеспечение) 25. Microsoft Project (лицензионное программное обеспечение) 26. 1С:Предприятие 8.3 (лицензионное программное обеспечение) 27. «Антиплагиат.ВУЗ» (лицензионное программное обеспечение)
Современные профессиональные базы данных	1. Консультант+ (лицензионное программное обеспечение отечественного производства) 2. http://www.garant.ru (ресурсы открытого доступа)
Информационные справочные системы	1. https://elibrary.ru - Научная электронная библиотека eLIBRARY.RU (ресурсы открытого доступа) 2. https://www.rsl.ru - Российская Государственная Библиотека (ресурсы открытого доступа) 3. https://link.springer.com - Международная реферативная база данных научных изданий Springerlink (ресурсы открытого доступа) 4. https://zbmath.org - Международная реферативная база данных научных изданий zbMATH (ресурсы открытого доступа)
Интернет-ресурсы	1. http://window.edu.ru - Информационная система "Единое окно доступа к образовательным ресурсам" 2. https://openedu.ru - «Национальная платформа открытого образования» (ресурсы открытого доступа)

Материально-техническое обеспечение	Учебные аудитории для проведения: занятий лекционного типа, обеспеченные наборами демонстрационного оборудования и учебно-наглядных пособий, обеспечивающих тематические иллюстрации, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, помещения для самостоятельной работы, оснащенные компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду организации, помещения для хранения и профилактического обслуживания учебного оборудования. Лаборатории и кабинеты: 1. Учебная аудитория Кабинет информатики Компьютерный класс, включая оборудование: Комплекты учебной мебели, демонстрационное оборудование – проектор и компьютер, учебно-наглядные пособия, обеспечивающие тематические иллюстрации, доска, персональные компьютеры

8. Учебно-методические материалы

№	Автор	Название	Издательство	Год издания	Вид издания	Кол-во в библио-теке	Адрес электронного ресурса	Вид доступа
1	2	3	4	5	6	7	8	9
9.1 Основная литература								
9.1.1	Метелица Н.Т.	Вычислительные сети и защита информации	Южный институт менеджмента	2013	учебное пособие	-	http://www.iprbookshop.ru/25962.html	по логину и паролю
9.1.2	Шаньгин В.Ф.	Информационная безопасность и защита информации	Профобразование	2019	учебное пособие	-	http://www.iprbookshop.ru/87995.html	по логину и паролю
9.1.3	Суворова Г.М.	Информационная безопасность	Вузовское образование	2019	учебное пособие	-	http://www.iprbookshop.ru/86938.html	по логину и паролю
9.2 Дополнительная литература								
9.2.1	Громов Ю.Ю. Карпов И.Г. Нурутдинов Г.Н. Гриднев В.А. Однолько В.Г. Лобанов С.М.	Системы и сети передачи информации	Тамбовский государственный технический университет, ЭБС АСВ	2012	учебное пособие	-	http://www.iprbookshop.ru/64573.html	по логину и паролю
9.2.2	Ковган Н.М.	Компьютерные сети	Республиканский институт профессионального образования (РИПО)	2019	учебное пособие	-	http://www.iprbookshop.ru/93384.html	по логину и паролю
9.2.3	Фомин Д.В.	Информационная безопасность	Вузовское образование	2018	учебно-методическое пособие	-	http://www.iprbookshop.ru/77320.html	по логину и паролю

9. Особенности организации образовательной деятельности для лиц с ограниченными возможностями здоровья

В МФЮА 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 МФЮА 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 университете комплекса необходимых условий обучения для данной категории обучающихся. Информация о специальных условиях, созданных для обучающихся с ограниченными возможностями здоровья, размещена на сайте университета (http://www.mfua.ru/sveden/objects/#objects).

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 МФЮА 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 МФЮА 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.

Год начала подготовки студентов - 2021