МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Дагестанский государственный университет»
Колледж

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

По программе производственной практики

Кафедра специальных дисциплин
Образовательная программа подготовки специалистов среднего профессионального образования

Специальность:
10.02.05 Обеспечение информационной безопасности автоматизированных систем

Форма обучения:
Очная

Статус дисциплины
Входит в обязательный цикл

Махачкала- 2022 г.

Фонд оценочных средств по программе производственной практики составлен в 2022 году в соответствии с требованиями ФГОС СПО специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем от 09.12.2016 №1553

Разработчик(и): Магомедова К.К. - к.ю.н., и.о. зав кафедрой кафедры специальных дисциплин колледжа ДГУ ;
Шахбанова М.И., преподаватель кафедры специальных дисциплин колледжа ДГУ.

Фонд оценочных средств дисциплины рассмотрен и рекомендован к утверждению кафедры специальных дисциплин Колледжа ДГУ.
Протокол № 9 от «_30_» апреля 2022г.
И. о. зав. кафедрой специальных дисциплин

к.ю.н., доцент Магомедова К.К.

Рабочая программа дисциплины согласована с учебно-методическим управлением

«30» 04 2022 г. _____ / Гасангаджиева А.Г. /

Нач. управления цифровых технологий и информационного государственного управления Минцифры РД
(полное наименование организации и должности руководителя)

Гронов Евгений Васильевич
ФИО

(подпись)

М.П.

Фонд оценочных средств (ФОС) является приложением к рабочей программе производственной практики по специальности **10.02.05 Обеспечение информационной безопасности автоматизированных систем** и представляет собой совокупность контрольно-измерительных материалов предназначенных для измерения уровня достижения студентом установленных результатов обучения.

В результате освоения программы производственной практики обучающийся должен обладать предусмотренными ФГОС по специальности СПО **10.02.05 Обеспечение информационной безопасности автоматизированных систем** базовой подготовки следующими умениями, знаниями:

Уметь:

- осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении и компонент систем защиты информации автоматизированных систем.
- организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней;
- производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы.
- настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам
- обеспечивать работоспособность, обнаруживать и устранять неисправности.
- устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации
- устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; устанавливать, настраивать, применять программные и программно- аппаратные средства защиты информации
- диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации
- применять программные и программно-аппаратные средства для защиты информации в базах данных; проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; применять математический аппарат для выполнения криптографических преобразований; использовать типовые программные криптографические средства, в том числе электронную подпись
- применять средства гарантированного уничтожения информации
- применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных
- применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных
- применять технические средства для криптографической защиты информации конфиденциального характера; применять технические средства для уничтожения информации и носителей информации; применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами
- применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных
- применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных
- применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом; применять инженерно-технические средства

физической защиты объектов информатизации

Знать:

- состав и принципы работы автоматизированных систем, операционных систем и сред; принципы разработки алгоритмов программ, основных приемов программирования; модели баз данных; принципы построения, физические основы работы периферийных устройств
- теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации
- порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях
- принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации
- особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных
- особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных
- методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации
- особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации; основные понятия криптографии и типовых криптографических методов и средств защиты информации
- особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации
- порядок технического обслуживания технических средств защиты информации; номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам
- порядок технического обслуживания технических средств защиты информации; Номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам
- физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации; порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации; методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации; номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам
- номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации; структуру и условия формирования технических каналов утечки информации
- номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам
- основные принципы действия и характеристики технических средств физической защиты; основные способы физической защиты объектов информатизации; номенклатуру применяемых средств физической защиты объектов информатизации

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ
по дисциплине
«Информационные технологии в деятельности суда»

1.1. Основные сведения о дисциплине

Общая трудоемкость дисциплины составляет 360 ч.

Вид работы	***Трудоемкость, академических часов***			
	6 семестр	***7 семестр***	***8 семестр***	***Всего***
Общая трудоёмкость	**144**	**144**	**72**	**360**
Контактная работа:	144	144	72	360
Промежуточная аттестация	*дифф. зачет*	*дифф. зачет*	*дифф. зачет*	*дифф. зачет*

1.2. Требования к результатам обучения по дисциплине, формы их контроля и виды оценочных средств

Общие компетенции

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.
ОК 09. Использовать информационные технологии в профессиональной деятельности.
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.

Профессиональные компетенции

ПК 1.1. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.
ПК 1.2. Администрировать программные и программно- аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.
ПК 1.3 Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.
ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.
ПК 2.1. Осуществлять установку и настройку отдельных программных, программно- аппаратных средств защиты информации

ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно- аппаратными средствами
ПК 2.3. Осуществлять тестирование функций отдельных программных и программно- аппаратных средств защиты информации
ПК 2.4 Осуществлять обработку, хранение и передачу информации ограниченного доступа
ПК 2.5 Уничтожать информацию и носители информации с использованием программных и программно- аппаратных средств
ПК 2.6 Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно- аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак
ПК 3.1 Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии требованиями эксплуатационной документации
ПК 3.2 Осуществлять эксплуатацию технических средств защиты информации в соответствии требованиями эксплуатационной документации
ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки
информации ограниченного доступа
ПК 3.4 Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации
ПК 3.5. Организовывать отдельные работы по физической защите объектов информатизации

Наименование профессионального модуля	**Формат практики, индекс**	**Коды формируемых компетенций**	**Объем времени, отведенный на практику (в неделях, часах)**	**Форма аттестации**	**Сроки проведения**
ПМ.01. Эксплуатация автоматизированных систем в защищенном исполнении	концентрированная (ПП.01.01)	ПК 1.1, ПК 1.3, ПК 1.4	4 недели 144 часа	Дифференцированный зачет	Согласно календарному графику учебного процесса на соответствующий учебный год
ПМ.02. Защита информации в автоматизированных системах программами и программно-	концентрированная (ПП.02.01)	ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4, ПК 2.5., ПК 2.6.	4 недели 144 часа	Дифференцированный зачет	Согласно календарному графику учебного процесса на соответствующий

аппаратными средствами					учебный год
ПМ.03. Защита информации техническими средствами	концентрированная (ПП.03.01)	ПК 3.1., ПК 3.2., ПК 3.3., ПК 3.4., ПК 3.5.	2 недели 72 часов	Дифференцированный зачет	Согласно календарному графику учебного процесса на соответствующий учебный год

2. КОНТРОЛЬНЫЕ ЗАДАНИЯ И ИНЫЕ МАТЕРИАЛЫ ОЦЕНКИ

знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций в процессе освоения дисциплины «Информационные технологии в профессиональной деятельности»

Индивидуальные задания по разделам:

Вариант № 1

Опишите способы непосредственного воздействия на носители защищаемой информации. Приведите способы вывода из строя технических средств отображения, хранения, обработки, воспроизведения, передачи информации и средств связи. Опишите виды дестабилизирующего воздействия на защищаемую информацию со стороны источника воздействия — технических средств отображения, хранения, обработки, воспроизведения, передачи информации и средств связи.

Вариант № 2

Составьте документацию на заданное контролируемое помещение, определите возможные разведопасные направления и возможные виды разведки. Составьте план проведения визуального осмотра помещения и выявите объекты, требующие при обследовании использования имеющихся средств видеонаблюдения.

Вариант № 3

Какие виды электрических полей существуют в природе? Каким образом электрические заряды взаимодействуют друг с другом? Назовите источники электрических полей и способы его обнаружения. От чего зависит характер электромагнитного поля в той или иной точке пространства? В чем сущность явления электромагнитной индукции? На какие зоны и по какому принципу подразделяется пространство вокруг источника электромагнитного поля?

Вариант № 4

Каково назначение экранирования в системах обработки и передачи информации? Расскажите об экранировании электрических полей (типы полей, диапазон частот). Какие

способы уменьшения паразитной емкости при экранировании низкочастотных электрических полей Вам известны? Как взаимосвязаны толщина и магнитная проницаемость экрана? Из каких материалов изготавливают экраны против высокочастотных магнитных полей? На каком принципе осуществляется экранирование высокочастотных магнитных полей?

Вариант № 5

Перечислите типы устройств, используемых для перехвата информации с различных типов кабелей. Приведите основные причины утечки информации в волоконно-оптических линиях. Опишите основные причины излучения световой энергии в окружающее пространство в местах соединения оптических волокон. Приведите примеры технических средств защиты от утечки информации по проводному каналу.

Вариант № 6

Что является основой анализа разборчивости речевой информации? Каков диапазон уровней человеческой речи? Какие звуки являются наиболее информативными с точки зрения разборчивости речевой информации? На каком расстоянии от источника производится измерение уровней речи? Что используют для количественной оценки качества перехваченной речевой информации? Приведите примеры технических средств защиты от утечки по вибро-акустическому каналу.

Вариант № 7

Опишите способы перехвата побочных электромагнитных излучений технических средств передачи, обработки, информации ограниченного доступа (ТСПИ). Приведите методы защиты информации от ПЭМИН. Опишите технологию исследования ПЭМИН-монитора.

Вариант № 8

Опишите варианты утечки информации по цепям заземления и электропитания. Приведите меры по предотвращению утечки защищаемой информации по цепям заземления и электропитания. Опишите принцип действия прибора РНИ-1.1

Вариант № 9

Назовите и охарактеризуйте пассивные технические средства защиты телефонной линии. Как осуществляется контроль состояния телефонной линии и обнаружение атак? Приведите методы активной защиты информации в телефонных линиях. Опишите технологию защита речевой информации в IP-телефонии.

Вариант № 10

Опишите оптические каналы утечки информации, способы получения информации в оптическом канале. Опишите технологию работы телевизионных систем наблюдения.

Критерии оценки:

- ***оценка «отлично»*** выставляется студенту, если даны исчерпывающие и обоснованные ответы на все поставленные вопросы, при ответах выделялось главное, развернутый ответ без принципиальных ошибок; логически выстроенное содержание ответа; мысли излагались в логической последовательности; показано умение самостоятельно анализировать факты, события, явления, процессы в их взаимосвязи и диалектическом развитии; полное знание терминологии по данной теме

- ***оценка «хорошо»*** выставляется студенту, если Даны полные, достаточно обоснованные ответы на поставленные вопросы, при ответах не всегда выделялось главное, в основном были краткими, но не всегда четкими; практически полное знание терминологии данной темы

- ***оценка «удовлетворительно»*** выставляется студенту, если даны в основном правильные ответы на все поставленные вопросы, но без должной глубины и обоснования, при решении практических задач студент использовал прежний опыт и не применял новые знания, однако, на уточняющие вопросы даны правильные ответы;

при ответах не выделялось главное; ответы были многословными, нечеткими и без должной логической последовательности; на отдельные дополнительные вопросы не даны положительные ответы

-оценка «неудовлетворительно» - выставляется студенту при неполном и некорректном ответе

Тестовые задания

Раздел 1

Эксплуатация автоматизированных систем в защищенном исполнении

1. Основы информационных систем как объекта защиты.

Выберите правильную последовательность уровней защиты информационной системы:

а) пользовательский -сетевой -локальный -технологический -физический

б) пользовательский -технологический -физический-сетевой -локальный

в) локальный -технологический -физический -пользовательский –сетевой

2. Для чего создаются информационные системы?

а) получения определенных информационных услуг

б) обработки информации

в) все ответы правильные

3. Какие трудности возникают в информационных системах при конфиденциальности?

а) сведения о технических каналах утечки информации являются закрытыми

б) на пути пользовательской криптографии стоят многочисленные технические проблемы

в) все ответы правильные

4. Основными источниками внутренних отказов информационных систем являются:

а) ошибки при конфигурировании системы

б) отказы программного или аппаратного обеспечения

в) выход системы из штатного режима эксплуатации

5. Утечкой информации в информационной системе называется ситуация, характеризуемая:

а) потерей данных в системе 1580436089

б) изменением формы информации

в) изменением содержания информации

6. Угроза информационной системе (компьютерной сети) – это:

а) вероятное событие

б) детерминированное (всегда определенное) событие

в) событие, происходящее периодически

8. Политика безопасности в информационной системе (сети) – это комплекс:

а) руководств, требований обеспечения необходимого уровня безопасности

б) инструкций, алгоритмов поведения пользователя в сети

в) нормы информационного права, соблюдаемые в сети

9. Информационная безопасность автоматизированной системы – это состояние автоматизированной системы, при котором она:

а) с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой — ее наличие и функционирование не создает информационных угроз для элементов самой системы и внешней среды

б) с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой – затраты на еѐ функционирование ниже, чем предполагаемый ущерб от утечки защищаемой информации способна противостоять только информационным угрозам, как внешним так и внутренним способна противостоять только внешним информационным угрозам

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

а) Оранжевая книга

б) Закон «Об информации, информационных технологиях и о защите информации»

в) рекомендации X.800

11.Базовые модели жизненного цикла: (выбрать все верные)

а) каскадная модель

б) поэтапная модель

в) логическая модель

г) спиральная модель

д) интеллектуальная модель

12. Непрерывный процесс, который начинается с момента принятия решения о необходимости создания ИС и заканчивается в момент ее полного изъятия из эксплуатации это:

а) разработка

б) жизненный цикл

в) конфигурация

г) управление проектами

13. Что входит в структуру ЖЦ по стандарту ISO/IEC:

а) организационные процессы

б) основные процессы ЖЦ

в) дополнительные процессы

г) ветвящиеся процессы

14. Структура, определяющая последовательность выполнения и взаимосвязи процессов, действий и задач, выполняемых на протяжении ЖЦ это:

а) проект

б) модель ЖЦ

в) инструкция

г) 1580436089

15. Технологии, базирующиеся на методологиях подготовки

информационных систем и соответствующих комплексах интегрированных инструментальных средств, а также ориентированные на поддержку полного жизненного цикла АС или его основных этапов это:

а) nano-технологии

б) CASE-технологии

в) инновационные технологии

г) информационные технологии

16. В стандарте ISO 12207 описаны ____ основных процессов жизненного цикла программного обеспечения

а) три

б) четыре

в) пять

г) шесть

17. ISO 12207 – базовый стандарт процессов жизненного цикла

а) программного обеспечения

б) информационных систем

в) баз данных

г) компьютерных систем

18. Согласно ISO 12207, процессы, протекающие во время жизненного цикла программного обеспечения, должны быть совместимы с процессами, протекающими во время жизненного цикла

а) автоматизированной системы

б) информационной системы

в) компьютерной системы

г) системы обработки и передачи данных

19. Согласно стандарту ISO 12207 основным процессом жизненного цикла программного обеспечения является

а) приобретение

б) решение проблем

в) обеспечение качества

г) аттестация

20. Согласно стандарту ISO 12207 основным процессом жизненного цикла программного обеспечения является

а) процесс поставки

б) документирования

в) аудит

г) управление конфигурацией

21.Источник угрозы информационной безопасности для автоматизированных систем – это:

а) потенциальный злоумышленник

б) злоумышленник

в) нет правильного ответа

22. Угрозы ИБ в автоматизированных системах можно классифицировать по нескольким критериям:

а) по спектру ИБ
б) по способу осуществления
в) по компонентам АИС

23. По каким компонентам классифицируется угрозы доступности в автоматизированных системах:

а) 1580436089
б) отказ пользователей
в) отказ поддерживающей инфраструктуры
г) ошибка в программе

24. По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы:

а) невозможность и нежелание обслуживающего персонала или пользователя выполнять свои обязанности
б) обрабатывать большой объем программной информации
в) нет правильного ответа

25. Вид источника угрозы ИБ, характер возникновения которого обусловлен действиями субъекта:

а) техногенный источник
б) антропогенный источник
в) стихийный источник.

26. Степень квалификации и привлекательность совершения деяний со стороны источника угрозы (для антропогенных источников), или наличие необходимых условий (для техногенных и стихийных источников):

а) готовность источника
б) фатальность
в) возможность возникновения источника

27. Естественные угрозы безопасности информации в АИС вызваны:

а) ошибками при действиях персонала
б) ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения
в) воздействиями объективных физических процессов или стихийных природных явлений, не зависящих от человека
г) корыстными устремлениями злоумышленников

28. Угрозы ИБ, реализация которых не влечет за собой изменение структуры данных (копирование):

а) естественные угрозы
б) пассивные угрозы
в) активные угрозы
г) искусственные угрозы

29. По каким критериям нельзя классифицировать угрозы:

а) по расположению источника угроз
б) по аспекту информационной безопасности, против которого угрозы направлены в первую очередь
в) по способу предотвращения
г) по компонентам информационных систем, на которые угрозы

нацелены

30. Наиболее распространены угрозы информационной безопасности корпоративной системы:

а) покупка нелицензионного ПО

б) ошибки эксплуатации и неумышленного изменения режима работы системы

в) сознательного внедрения сетевых вирусов

31. Защита информации от несанкционированного доступа - это деятельность по предотвращению:

а) неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа (НСД) к защищаемой информации и получения защищаемой информации злоумышленниками.

б) получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации деятельность по предотвращению получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником либо владельцем информации прав или правил доступа к защищаемой информации.

в) несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

32. Какая из приведенных техник является самой важной при выборе конкретных защитных мер?

а) анализ рисков

б) анализ затрат / выгоды

в) результаты ALE

33. Какие меры по защите информации в автоматизированных системах дают наибольший эффект?

а) организационные

б) технические (аппаратные)

в) программные

г) все в совокупности

д) правильных ответов нет

34. Требования к программному обеспечению АСЗИ включают в себя требования: (выбрать все верные)

а) к алгоритму принятия решения;

б) к системе классификации;

в) к системе команд;

г) к алгоритму обработки событий;

д) к сертификации программного обеспечения;

е) к системе диагностики программного обеспечения.

ж) к оптимизации кода программного обеспечения и средству разработки

з) 1580436089

Раздел 2
Защита информации в автоматизированных системах программами и программно-аппаратными средствами

1. Под СВТ понимается:

а) совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем

б) электронные компоненты, из которых строятся вычислительные системы

в) совокупность программных и технических элементов систем передачи информации, используемая для построения компьютерных систем

2. Под АС понимается:

а) система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций

б) локальная ПЭВМ или компьютерная сеть с установленным системным программным обеспечением и средствами коммуникации

в) автоматизированная система управления обработкой информации с целью выполнения производственных функций организации

3. Под несанкционированным доступом в компьютерной системе понимается:

а) доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств, предоставляемых СВТ или АС

б) доступ к информации с преодолением парольной защиты, фальсификации аутентификационной информации с использованием штатных средств, предоставляемых СВТ или АС

в) реализация угроз безопасности информации с целью ознакомления и/или уничтожения информации с использованием штатных или специальных СВТ

4. К основным функциям СРД относятся:

а) регистрация действий субъекта и активизированного им приложения

б) контроль целостности программной и аппаратной части СРД

в) реакция на попытки НСД

г) управление потоками информации в целях предотвращения записи

е) н носители несоответствующего уровня конфиденциальности.

5. К основным функциям СРД не относятся:

а) реализация правил разграничения доступа субъектов и их процессов к информации и устройствам создания еѐ твердых копий

б) изоляция процесса, выполняемого в интересах субъекта доступа, от других субъектов

в) идентификация и аутентификация субъектов и поддержание

привязки субъекта к процессу, выполняемому для него

6. К функциям обеспечивающих средств для СРД не относятся:

а) учет выходных печатных и графических форм и твердых копий в КС

б) очистка оперативной памяти после завершения работы пользователя с защищаемыми данными

в) реализация правил обмена информацией между субъектами в компьютерных сетях.

7. Идентификация это:

а) однозначное определение уникального имени, под которым пользователь зарегистрирован в КС

б) генерация уникального имени, под которым пользователь будет зарегистрирован в КС

в) проверка уникальности имени зарегистрированного в КС пользователя при запросе доступа к ресурсам КС

8. Аутентификация это:

а) подтверждение подлинности имени, предъявленного пользователем

б) подтверждение заявленных пользователем прав доступа к ресурсам КС

в) проверка наличия введенного имени пользователя в регистрационной базе КС.

9. Авторизация это:

а) процесс наделения пользователя индивидуальным набором привилегий в системе и определение его прав доступа к объектам КС

б) процесс определения набора информационных ресурсов, доступ к которым разрешен пользователю

в) проверка соответствия введенного пользователем пароля его идентификатору.

10. Аудит безопасности КС это:

а) учет возникающих при работе системы событий, связанных с безопасностью информации в ней, и регистрация этих событий в системном журнале

б) учет попыток НСД и регистрация их в системном журнале

в) проверка соответствия защитных функций установленных в АС СЗИ требованиям, предъявляемым к СЗИ в АС

г) учет неудачных попыток ввода пароля и регистрация этих попыток в системном журнале.

11. Укажите наиболее правильную формулировку требований к «идеальной» системе защиты информации (СЗИ).

а) СЗИ должна быть прозрачна для легальных пользователей и создавать непреодолимые трудности для реализации НСД.

б) СЗИ должна обеспечивать уровень защищенности информации, соответствующий требованиям для данного класса АС.

в) СЗИ должна обеспечивать защищенность информации на программном и аппаратном уровне, включать в себя подсистемы, использующие разные технологии ЗИ.

12. Выберите наиболее полное правило, которым следует руководствоваться при выборе паролей:

а) пароли должны трудно подбираться и легко запоминаться

б) в паролях следует использовать буквы и цифры, причем длина пароля должна быть не менее 4 символов

в) в качестве паролей не следует использовать простые слова, имена собственные и т.п.

13. Выберите наиболее правильное описание начального этапа модели «рукопожатия».

а) система генерирует случайное значение , вычисляет и сообщает пользователю.

б) пользователь генерирует случайное значение , вычисляет и вводит в ответ на запрос системы.

в) система генерирует случайное значение , вычисляет и сообщает пользователю.

г) система генерирует случайное значение , вычисляет и сообщает и пользователю.

14. К пассивным устройствам аутентификации не относятся:

а) пластиковые карты с магнитной полоской

б) элементы Touch Memory

в) USB-ключи

15.Уязвимость информационной системы это:

а) любая характеристика, использование которой нарушителем может привести к реализации угрозы

б) ошибки в программном обеспечении, возникновение которых может привести к реализации угрозы

в) количественная и качественная недостаточность средств ЗИ, которая может привести к реализации угрозы.

16.Угрозой информационной системе называется:

а) потенциально возможное событие, действие, процесс или явление, которое может вызвать нанесение ущерба ресурсам системы

б) совокупность программно-аппаратных средств осуществления НСД при наличии методов их использования для нанесения ущерба ресурсам системы

в) возможность использования информации, штатных и нештатных технических средств АС для нанесения ущерба ресурсам системы.

17. Под информационной безопасностью понимается:

а) защищенность информации и поддерживающей инфраструктуры от случайных и преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры

б) комплекс программно-аппаратных средств направленных на защиту от случайных и преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры

в) совокупность мер организационно-технического характера, направленных на защиту от случайных и преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры

18. Сущность комплексного подхода к ЗИ заключается в:

а) сочетании различных мер обеспечения безопасности на законодательном, административном, процедурном и программно-техническом уровнях

б) сочетании различных мер обеспечения безопасности на законодательном и программно-техническом уровнях

в) сочетании различных программно-аппаратных средств защиты АС от НСД.

19.Аспекты обеспечения ИБ:

а) формальный и практический

б) общий и частный

в) программный и аппаратный.

20. Укажите, что не является контекстом ЗИ и соответствующих бизнес процессов:

а) конфиденциальность

б) целостность

в) доступность

г) достоверность.

21. Основная цель сетевой ПБ:

а) контроль сетевого трафика и его использования

б) противодействие попыткам НСД с использованием сетевой инфраструктуры

в) установка и правильная настройка программно-аппаратных СЗИ.

22. Под доверенными понимаются сети, …

а) …над которыми специалисты организации имеют полный административный контроль

б) …на компьютерах которых установлены средства удаленного администрирования

в) …оснащенные программно-аппаратными СЗИ и проходящие регулярные проверки на предмет вирусной активности.

23. Ресурсы (в контексте задачи управления рисками) это:

а) то, что организация ценит и хочет защитить

б) финансовые и информационные активы организации

в) файлы и бумажные документы.

24. Политика информационной безопасности определяет:

а) способы развертывания систем безопасности и поведение пользователей при использовании КС

б) способы настройки межсетевых экранов и антивирусных средств
в) порядок получения доступа пользователей к ресурсам КС организации.

25.Основная цель сетевой ПБ:

а) описание топологии ЛВС и определение мест установки МЭ
б) контроль сетевого трафика и его использования
в) формирование требований к настройке МЭ и антивирусных систем
г) разрешить то, что явно не запрещено
д) запретить то, что явно не разрешено.

26. Выберите пункт из перечисленного ниже, который не относится к службам безопасности:

а) аутентификация
б) целостность
в) информированность.

27. Под доверенными понимаются сети, …

а) …на компьютерах которых установлены средства удаленного администрирования
б) …над которыми специалисты организации имеют полный административный контроль
в) оснащенные программно-аппаратными СЗИ и проходящие регулярные проверки на предмет вирусной активности.

29. Ресурсы (в контексте задачи управления рисками) это:

а) информация и поддерживающие средства для ведения бизнеса
б) базы данных корпоративных информационных систем (бухгалтерских, аналитических и т.п.)
в) файлы и бумажные документы
г) описания устройств и технологических процессов, являющиеся «ноу-хау» организации.

30. Угроза – это …

а) …потенциальная причина нежелательного события, которое может нанести ущерб
б) организации и еѐ объектам
в) …сетевая атака, влекущая нарушение работоспособности КС организации
г) …потенциальная возможность НСД к конфиденциальной информации организации
д) …совокупность вредоносного ПО, распространяющаяся по компьютерным сетям.

31. По характеру воздействия угрозы могут быть…

а) …против доступности, целостности, конфиденциальности
б) …внутренними, внешними
в) …преднамеренными, случайными.

32. Риск безопасности это …

а) …возможность реализации сетевой атаки на ресурсы КС

б) вероятность преодоления системы защиты за произвольный период времени
в) …возможность данной угрозы реализовать уязвимости для нанесения ущерба организации
г) …вероятность начала вредоносного воздействия на ресурсы КС злоумышленником.

33. Классы межсетевых экранов по функционированию на уровнях модели OSI:

а) пакетный фильтр, программно-аппаратный, программный.
б) пакетный фильтр, экранирующий транспорт, прикладной шлюз
в) контроллер состояния протокола, экранирующий транспорт, прикладной шлюз.

34. Список доступа маршрутизатора – это…

а) …набор строк, описывающих доверенные адреса хостов
б) …набор строк, определяющих некие образцы, на соответствие которым проверяются пакеты IP
в) …набор строк, описывающих конфигурацию интерфейсов маршрутизатора.

35. Выберите наиболее правильное утверждение.

а) стандартный ACL может проверять адреса отправителей, получателей и ряд параметров
б) нумерация стандартных ACL выполняется в диапазоне от 100 до 199
в) стандартный ACL может выполнять контроль состояния соединения
г) стандартный ACL может проверять только адреса отправителей.

36. Выберите наиболее правильное утверждение.

а) ключевое слово host означает любой IP-адрес хоста
б) обратная маска 255.255.255.255 определяет единственный IPадрес
в) обратная маска 0.0.0.0 определяет единственный IP-адрес
г) ключевое слово any соответствует WildCard-маске 0.0.0.0.

37.В чем заключается смысл следующего списка доступа?

а) access-list 45 permit 192.168.20.0 0.0.0.255
б) access-list 45 deny host 192.168.20.13
в) трафику сети 192.168.20.0 разрешено проходить через маршрутизатор, за исключением хоста192.168.20.13
г) трафику сети 192.168.20.0 разрешено проходить через маршрутизатор
д) трафику сети 192.168.20.0 запрещено проходить через маршрутизатор, за исключением хоста 192.168.20.13
е) трафику хоста 192.168.20.13 запрещено проходить через маршрутизатор, а остальным хостам сети 192.168.20.0 – разрешено.

38. Выберите наиболее правильное утверждение.

а) расширенный ACL может проверять адреса источников, получателей, тип протокола и порты.

б) расширенный ACL обеспечивает более быструю проверку
пакетов, чем стандартный ACL.
в) допускается размещать более 1 расширенного ACL на интерфейс,
на протокол, на направление.
г) расширенный ACL не может проверить состояние соединения
TCP.

39.В чем заключается смысл следующего выражения?

а) запрещение доступа к хосту с IP-адресом 130.120.110.100
б) разрешение доступа к хосту с IP-адресом 130.120.110.100
в) запрещение доступа к подсети 130.120.110.0 0.0.0.255.
г) access-list 101 deny ip 0.0.0.0 255.255.255.255 130.120.110.100
0.0.0.0

40.Межсетевой экран (Брандмауэр, firewall) – это…

а) Комплекс аппаратных средств
б) Комплекс программных средств
в) Комплекс аппаратных или программных средств
г) Комплекс аппаратных и программных средств

Раздел 3
Защита информации техническими средствами

1. Создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации и специальных воздействий, вызывающих разрушение, уничтожение, искажение информации, а также изменение штатных режимов функционирования систем и средств информатизации и связи относится к:

а) правовым методам защиты информации
б) организационно-техническим методам защиты информации
в) организационно-распорядительным методам защиты информации
г) экономическим методам защиты информации

2. Субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией, называется:

а) собственник информации
б) владелец информации
в) пользователь

3. Форма допуска, требуемая для работы со сведениями особой важности является:

а) первой формой допуска
б) второй формой допуска
в) третьей формой допуска

4. Форма допуска, требуемая для работы с совершенно секретными сведениями является:

а) первой формой допуска
б) второй формой допуска
в) третьей формой допуска

5. Форма допуска, требуемая для работы с секретными сведениями является:

а) первой формой допуска
б) второй формой допуска
в) третьей формой допуска

6. В сфере государственной тайны действует функционально-зональный принцип. Это значит, что:

а) каждый пользователь допускается должностными лицами только к такой информации, которая требуется ему для исполнения должностных обязанностей
б) каждый пользователь допускается должностными лицами только к информации, касающейся зоны его проживания
в) каждый пользователь допускается должностными лицами ко всей информации, к которой у него есть форма допуска

7. Противоправные процессы утечки, утраты, распространения, разглашения, копирования, тиражирования, фальсификации, хранения с целью передачи, удаления информации называется процессом:

а) незаконного оборота информации
б) взлома информации
в) несанкционированного использования информации

8. Форма преднамеренного распространения или мнимого разглашения (утечки) неких планов и намерений, которые не отвечают реальным действиям называется:

а) дезинформация
б) легендирование
в) шпионаж

9. Какое направление защиты в основном применяется для охраны материальных ценностей?

а) инженерно-техническая
б) организационно-техническая
в) организационно-распорядительная
г) нормативно-правовая
д) экономическая

10.Что из нижеперечисленного оборудования может выступать в качестве технического канала связи?

а) инфракрасный светодиод лазерного принтера, посылающий кратковременные
б) вспышки на электризованную поверхность фоточувствительного барабана
в) модулированный по силе тока поток электронов, засвечивающий в определенном
г) порядке пикселы люминофора электронно-лучевой трубки
д) экран компьютерного монитора и глаза пользователя
е) оптический канал связи
ж) все варианты могут быть отнесены к техническим каналам связи
з) контроллер жесткого диска, передающий электрические импульсы, считанные магниторезистивной головкой с поверхности магнитного

носителя, по шлейфу в системную магистраль для копирования в оперативную память

11.Какой канал утечки информации основан на использовании электромагнитной энергии видимого и инфракрасного диапазона?

а) визуально-оптический канал

б) электромагнитный канал

в) виброакустический канал

г) материально-вещественный канал

12.Процесс перехвата и фиксации процесса клавиатурного ввода идентифицирующей информации является примером утечки информации:

а) визуально-оптического канала

б) электромагнитного канала

в) виброакустического канала

г) материально-вещественного канала

13.Какой канал утечки информации включает в себя весь радиодиапазон от сверхнизких до сверхвысокочастотных волн?

а) визуально-оптический канал

б) электромагнитный канал

в) виброакустический канал

г) материально-вещественный канал

14.Электрические сигналы (напряжения, токи), модулированные по закону передаваемого сообщения, протекающие по проводникам и элементам радиоцепей (линиям связи, антеннам, конденсаторам) и возбуждающие в окружающем пространстве электромагнитную энергию является примером утечки информации:

а) визуально-оптического канала

б) электромагнитного канала

в) виброакустического канала

г) материально-вещественного канала

15.Какой канал утечки информации представляет собой фактический побочный прием модулированной акустической энергии, распространяющейся в газообразной, жидкой или твердой средах

а) визуально-оптический канал

б) электромагнитный канал

в) виброакустический канал

г) материально-вещественный канал

16.Примером какого канала утечки информации служит звук голоса человека?

а) визуально-оптического канала

б) электромагнитного канала

в) виброакустического канала

г) материально-вещественного канала

17.По какому признаку делят на классы средства технической разведки (СТР) ?

а) по дальности канала

б) по форме допуска
в) по мощности
г) по степени финансирования

18.Портативные устройства для запечатления информации, скрытно проносимые на территорию объекта нарушителем на своем теле относят к …

а) первому классу СРТ
б) второму классу СРТ
в) третьему классу СРТ

19.Для наблюдения за объектами информатизации из-за пределов их охраняемой или контролируемой территории используются СРТ…

а) первого класса
б) второго класса
в) третьего класса

20.Установите соответствие

Укажите соответствие для всех 2 вариантов ответа:

1) наука о скрытой передаче информации путем сохранения в тайне самого факта передачи
2) наука скрывающая содержимое секретного сообщения

__ стеганография
__ криптография

21.Контроль доступа к информации обеспечивается последовательным использованием таких методов защиты информации…

22.Укажите соответствие для всех 4 вариантов ответа:

1) это комплекс мероприятий, исключающих или ослабляющих возможность неконтролируемого выхода конфиденциальной информации за пределы контролируемой зоны за счет электромагнитных полей побочного характера и наводок
2) это комплекс мероприятий, исключающих или уменьшающих возможность неконтролируемого выхода конфиденциальной информации за пределы контролируемой зоны в виде производственных или промышленных отходов
3) это комплекс мероприятий, исключающих или уменьшающих возможность выхода конфиденциальной информации за пределы контролируемой зоны за счет акустических полей
4) это комплекс мероприятий, исключающих или уменьшающих возможность выхода конфиденциальной информации за пределы контролируемой зоны за счет распространения световой энергии

__ защита информации от утечки по акустическому каналу
__ Защита информации от утечки по визуально-оптическому каналу
__ Защита информации от утечки по электромагнитным каналам
__ Защита информации от утечки по материально-вещественному каналу

Критерии и шкала оценивания результатов тестирования (20 вопросов)

Оценка **«отлично»** - 18-20 правильных ответов;
оценка «**хорошо»** - 15-17 правильных ответов;
оценка **«удовлетворительно»** - 12-14 правильных ответов;
оценка **«неудовлетворительно»** - 9-11 правильных ответов/

Контрольные вопросы

1. Компоненты автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации
2. Средства защиты информации прикладного и системного программного обеспечения Программное обеспечение с соблюдением требований по защите информации
3. Средства антивирусной защиты для корректной работы программного обеспечения по заданным шаблонам
4. Инструкции пользователей о соблюдении требований по защите информации при работе с программным обеспечением
5. Средства защиты информации программного обеспечения
6. Встроенные средства защиты информации программного обеспечения
7. Своевременное обнаружение признаков наличия вредоносного программного обеспечения
8. Обслуживание средств защиты информации в компьютерных системах и сетях
9. Обслуживание систем защиты информации в автоматизированных системах
10. Участие в проведении регламентных работ по эксплуатации систем защиты информации автоматизированных систем
11. Проверка работоспособности системы защиты информации автоматизированной системы
12. Контроль соответствия конфигурации системы защиты информации автоматизированной системы ее эксплуатационной документации
13. Контроль стабильности характеристик системы защиты информации автоматизированной системы
14. Ведение технической документации, связанной с эксплуатацией систем защиты информации автоматизированных систем
15. Участие в работах по обеспечению защиты информации при выводе из эксплуатации автоматизированных систем
16. Анализ принципов построения систем информационной защиты производственных подразделений.
17. Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы.
18. Участие в диагностировании, устранении отказов и обеспечении работоспособности программно-аппаратных средств обеспечения информационной безопасности;
19. Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении
20. Участие в обеспечении учета, обработки, хранения и передачи конфиденциальной информации

21. Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами при выполнении задач практики.
22. Участие в монтаже, обслуживании и эксплуатации технических средств защиты информации
23. Участие в монтаже, обслуживании и эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения
24. Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съёма, и утечки по техническим каналам
25. Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами.
26. Изучение порядка применения нормативных правовых актов
27. Изучение нормативных методических документов по обеспечению информационной безопасности техническими средствами
28. Выявление технических каналов утечки информации
29. Применение существующих способов выявления опасности целостности информации
30. Анализ объектов информатизации предприятий, учреждений, организаций
31. Анализ ресурсов обеспечения инженерно-технической защиты информации
32. Изучение основных этапов проектирования системы защиты информации техническими средствами
33. Проектирование рабочих проектов по системам пожарно-охранной сигнализации, видеонаблюдения, СКУД
34. Оформление технической и технологической документации
35. Выявление физических лиц и организаций из Перечня организаций и физических лиц, в отношении которых имеются сведения об их причастности к экстремистской деятельности или терроризму
36. Выявление операций, подлежащих обязательному контролю, с ценной сделки 600 000 рублей и выше
37. Выявление операций по открытию счетов, приобретению и продаже ценных бумаг обществами, имеющими стратегическое значение для оборонно-промышленного комплекса и безопасности Российской Федерации, а также обществами, находящихся под их прямым или косвенным контролем
38. Выявление операций по получению (зачислению) некоммерческой организацией ценных бумаг от иностранных государств, международных и иностранных организаций, иностранных граждан и лиц без гражданства, а равно по расходованию (списанию) ценных бумаг указанной организацией
39. Выявление операции с ценными бумагами, если хотя бы одной из сторон является физическое или юридическое лицо, имеющее соответственно регистрацию, место жительства или место нахождения в государстве (на территории), которое (которая) не выполняет рекомендации ФАТФ, либо если указанные операции проводятся с использованием счета в банке, зарегистрированном в указанном государстве (на указанной территории

Критерии оценки:

оценка «отлично» выставляется студенту, если даны исчерпывающие и

обоснованные ответы на все поставленные вопросы, при ответах выделялось главное, развернутый ответ без принципиальных ошибок; логически выстроенное содержание ответа; мысли излагались в логической последовательности; показано умение самостоятельно анализировать факты, события, явления, процессы в их взаимосвязи и диалектическом развитии; полное знание терминологии по данной теме

оценка «хорошо» выставляется студенту, если Даны полные, достаточно обоснованные ответы на поставленные вопросы, при ответах не всегда выделялось главное, в основном были краткими, но не всегда четкими; практически полное знание терминологии данной темы

оценка «удовлетворительно» выставляется студенту, если даны в основном правильные ответы на все поставленные вопросы, но без должной глубины и обоснования, при решении практических задач студент использовал прежний опыт и не применял новые знания, однако, на уточняющие вопросы даны правильные ответы; при ответах не выделялось главное; ответы были многословными, нечеткими и без должной логической последовательности; на отдельные дополнительные вопросы не даны положительные ответы

оценка «неудовлетворительно» - выставляется студенту при неполном и некорректном ответе

Примерный перечень вопросов для защиты отчета

1. Какие знания, умения и навыки были приобретены в результате прохождения производственной практики, преддипломной?
2. Какие задания удалось выполнить в ходе прохождения практики, а какие вызвали затруднений?
3. Какие материалы практики были собраны по теме вашей работы в ходе прохождения производственной практики, преддипломной?
4. Назовите основные правила работы
5. Как вы проходили практику в целом?
6. Каким образом руководитель по практике от организации проверял и корректировал Вашу работу?

Критерии оценки:

оценка «отлично» - студент глубоко и всесторонне усвоил программный материал;

- уверенно, логично, последовательно и грамотно его изложил; отчёт соответствует заданию практики; опираясь на знания основной и дополнительной литературы, тесно привязывает усвоенные научные положения с практической деятельностью юриста; делает логически обоснованные выводы и обобщения;

оценка «хорошо» - студент твердо усвоил программный материал, грамотно и по существу излагает его, опираясь на знания основной литературы; не допускает существенных неточностей; увязывает усвоенные знания с практической деятельностью юриста; делает выводы и обобщения; владеет системой юридических понятий.

оценка **«удовлетворительно»** - студент усвоил только основной программный материал, по существу излагает его, опираясь на знания только основной литературы; допускает несущественные ошибки и неточности; испытывает затруднения в практическом применении юридических знаний; затрудняется в формулировании выводов и обобщений.

оценка «неудовлетворительно» - отсутствие отчёта

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ
ПМ.01 Эксплуатация автоматизированных систем в защищенном исполнении

ПМ.02
Защита информации в автоматизированных системах программами и программно-аппаратными средствами

№ п/п	Разделы (этапы) практики	Кол-во часов/ недель			Форма контроля (Компетенции)
		Всего	аудиторные		
			практические	консультации	
ПМ.01 Эксплуатация автоматизированных систем в защищенном исполнении					
1	Организационные вопросы оформления, установочная лекция, инструктаж по технике безопасности, распределение по рабочим местам	6	4	2	Отчет, дневник практики (ПК 1.1-1.6)
2	Участие в ведении основных этапов проектирования системы безопасности автоматизированных систем. Эксплуатация компонентов подсистем безопасности автоматизированных систем, их диагностики, устранение отказов и восстановление работоспособности.	30	28	2	Отчет, дневник практики (ПК 1.1-1.6)
3	Участие в организации работ по эксплуатации подсистем и средств безопасности автоматизированных систем. Администрирование подсистем безопасности автоматизированных информационных систем.	36	34	2	Отчет, дневник практики (ПК 1.1-1.6)
4	Ознакомление с особенностями функционирования систем обеспечения безопасности орган	36	34	2	Отчет, дневник практики (ПК 1.1-1.6)
5	Установка компонентов подсистем безопасности автоматизированных информационных систем	30	28	2	
	Оформление отчета по практике	6	4	2	Отчет, дневник практики (ПК 1.1-1.6)
	Защита отчета		Отчет	5	Защита отчета
Итого		144			

1	Организационные вопросы оформления, установочная лекция, инструктаж по технике безопасности, распределение по рабочим местам	12	8	4	Отчет, дневник практики (2.1-2.6)
2	Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами. Диагностика, устранение отказов и восстановления работоспособности программно-аппаратных средств обеспечения информационной безопасности.	60	56	4	Отчет, дневник практики (2.1-2.6)

3	Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации. Осуществлять обработку, хранение и передачу информации ограниченного доступа. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств. Мониторинг эффективности программно-аппаратных средств обеспечения информационной безопасности; обеспечения учета, обработки, хранения и передачи конфиденциальной информации.	36	32	4	Отчет, дневник практики (2.1-2.6)
4	Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак. Решение технических задач, возникающих при аттестации объектов, помещений, программ, алгоритмов; применения нормативных правовых актов по обеспечению информационной безопасности программно-	24	20	4	Отчет, дневник практики (2.1-2.6)

	аппаратными средствами.				
5	Оформление отчета по практике	12	8	4	Отчет, дневник практики (2.1-2.6)
6	Защита отчета				Отчет
Итого		144			
ПМ.03 Защита информации техническими средствами					
1	Организационные вопросы оформления, установочная лекция, инструктаж по технике безопасности, распределение по рабочим местам	6	4	2	Отчет, дневник практики (ПК 3.1-3.5)
2	Применять инженерно-технические средства обеспечения информационной безопасности. Выбор технических средств обеспечения информационной безопасности.	30	28	2	(ПК 3.1-3.5)
3	Участвовать в эксплуатации инженерно-технических средств обеспечения информационной безопасности, в проверке их	18	16	2	(ПК 3.1-3.5)

	технического состояния, в проведении технического обслуживания и текущего ремонта, устранении отказов и восстановлении работоспособности. Определение видов и способов технической защиты информационной безопасности.				
4	Выявление и устранение недостатков инженерно-технических средств обеспечения информационной безопасности; соблюдение правил эксплуатации оборудования. Определение технологических возможностей.	12	10	2	(ПК 3.1-3.5)
5	Оформление отчета п практике	6	4	2	(ПК 3.1-3.5)
6	Защита отчета				Отчет
	Итого	72			
	Итого:	360 часов			

4. ПРОВЕРОЧНЫЙ МАТЕРИАЛ ПО ИТОГАМ ПРОХОЖДЕНИЯ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

1. **Путёвка с отметками** о прибытии на место практики и убытии, скреплённая печатями органа, в котором пройдена практика.
2. **Заполненный дневник** производственной практики, преддипломной за каждый рабочий день недели (с подписью руководителя от организации на каждой странице заверенной печатью).
3. **Характеристика** на студента с базы прохождения практики, заверенная подписью и печатью руководителя практики.
4. **Письменный отчёт** о прохождении практики, в котором обобщается весь ход практики, выполнение заданий и других запланированных мероприятий согласно календарному плану прохождения практики, выявленные предложения и недостатки в ходе прохождения практики;

Содержание отчёта должно представлять собой освещение всех включённых в календарном плане вопросов.

Введение:

- место, дата начала, дата окончания, продолжительность практики, её руководители от кафедры и места прохождения практики;

- цели и задачи прохождения практики.

Основную часть (отдельно по каждому месту прохождения практики):

- описание текущей деятельности соответствующего органа (организации) прохождения практики и своей работы в процессе практики;
- описание практических задач, выполненных студентом за время прохождения практики;
- проблемы и сложные вопросы, возникшие во время прохождения практики.

Заключение:

- умения и навыки, приобретённые за время прохождения практики;
- выводы о практической значимости для себя пройдённой практики;
- предложения по совершенствованию и организации практики.

Требования к содержанию отчета. Ко времени окончания практики студент составляет развернутый отчет о проделанной работе. Отчет готовится равномерно в течение всего периода практики. При написании отчета студент обязан систематизировать выполненную работу в том порядке, в каком она осуществлялась (в дневнике), раскрыть выполненные в ходе практики виды работ с учетом программы практики. Отчет вместе с приложениями к нему брошюруется. Отчет должен быть написан с соблюдением правил грамматики и с учетом особенностей научной речи - точности и однозначности терминологии и стиля. Примечание: Не употреблять личные местоимения "Я" и "МЫ". Например, вместо "я предполагаю" следует указывать "предполагается, что" и т.д.

Требования к оформлению отчета. Текст располагается на одной стороне листа белой бумаги формата А4 электронным способом и должен соответствовать следующим требованиям: шрифт Times New Roman; высота букв (кегль) - 14, начертание букв - нормальное; межстрочный интервал - полуторный; форматирование - по ширине. Параметры страницы: верхнее поле - 20 мм, нижнее поле - 20 мм, левое поле - 30 мм, правое поле - 10 мм. Страницы отчета следует нумеровать арабскими цифрами, соблюдая сквозную нумерацию по всему тексту работы. Номер страницы проставляют в середине верхнего поля без точки в конце. Титульный лист включается в общую нумерацию страниц отчета, но номер страницы не проставляется. Диаграммы, графики, схемы, чертежи, фотографии и другое, именуются рисунками, которые нумеруются последовательно сквозной нумерацией под рисунком, текст названия располагается внизу рисунка. Приложения оформляются как продолжение отчета на последующих его страницах, которые не нумеруются. Каждое приложение начинают с новой страницы, в правом верхнем углу которой указывают слово «Приложение» с последовательной нумерацией арабскими цифрами, например, Приложение 1, Приложение 2 и т.д.

Отчёт должен обязательно содержать приложение:

- материалы, собранные студентом в период прохождения практики

Критерии оценки

Оценка за производственную практику выставляется на основании оценки руководителя практики на предприятии.

оценка «отлично» Выполнение программы практики в полном объеме, без замечаний; получение знаний, умений и способностей, определенных программой практики и планом практики, освоение планируемых компетенций в полном объеме.

оценка «хорошо» Выполнение программы практики в полном объеме, с

незначительными замечаниями, касающимися отсутствия детального анализа документов прилагаемых к отчету; получение знаний, умений и способностей, определенных программой практики и планом практики, полное освоение планируемых компетенций.

оценка «удовлетворительно» Выполнение программы практики не в полном объеме, с отсутствием детального анализа документов прилагаемых к отчету; получение знаний, умений и способностей, определенных программой практики и планом практики, не полное освоение планируемых компетенций.

оценка «неудовлетворительно» Не выполнение программы практики; отсутствие знаний, умений и способностей, определенных программой практики и планом практики, неполное освоение планируемых компетенций.