ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ МОСКОВСКОЙ ОБЛАСТИ

«ДМИТРОВСКИЙ ТЕХНИКУМ»

ОДОБРЕНО
на заседании ПЦК
_____
«28» августа 2020г.
Протокол № 6

УТВЕРЖДАЮ
Зам. директора по учебно-методической работе
ГБПОУ МО «Дмитровский техникум»
_____ /Н.Е.Горюшкина /
«28» 08 2020г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ПРАКТИКИ

(ПРЕДДИПЛОМНОЙ)

10.02.01 Организация и технология защиты информации

Организация-разработчик: Государственное бюджетное профессиональное образовательное учреждение Московской области «Дмитровский техникум»

СОГЛАСОВАНО
_____
_____ Н. Н. Гостева
«_28_»_____08_____2020 г.

Александровская И.Л.
2021.04.30 10:05:
39+03'00'

Дмитров 2020 г.

Вид практики: Производственная практика (преддипломная)

Способ проведения практики: выездная, проводится в организациях, направление деятельности которых соответствует профилю подготовки обучающихся в соответствии с базами практик для студентов СПО специальности 10.02.01 «Организация и технология защиты информации» на основе договоров, заключаемых между техникумом и этими организациями. Преддипломная практика проводится непрерывно после освоения учебной практики и практики по профилю специальности.

Форма проведения практики: преддипломная практика проводится в форме практической деятельности обучающихся под непосредственным руководством и контролем руководителя практики от техникума и руководителей от организации при проведении производственной практики.

1.ЦЕЛИ ПРАКТИКИ

Целями практики для обучающихся, осваивающих ППССЗ по специальности 10.02.01 «Организация и технология защиты информации», комплексное освоение всех видов профессиональной деятельности по специальностям среднего профессионального образования, формирование общих и профессиональных компетенций, а также приобретение необходимых умений и опыта практической работы по осваиваемой специальности.

Преддипломная практика направлена на углубление первоначального практического опыта обучающегося, развитие общих и профессиональных компетенций, проверку его готовности к самостоятельной трудовой деятельности, а также на подготовку к выполнению выпускной квалификационной работы в организациях различных организационно-правовых форм.

2.МЕСТО ПРАКТИКИ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

2.1. Цикл (раздел) образовательной программы, к которому относится практика

Наименование практики	Цикл (раздел)	Курс
Производственная практика (преддипломная)	ПДП 01 Производственная практика (преддипломная)	4 курс 10.02.01 «Организация и технология защиты информации»

2.2. Логическая взаимосвязь с другими частями образовательной программы.

1. Программа преддипломной практики является частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности СПО 10.02.01 «Организация и технология защиты информации» в части освоения видов профессиональной деятельности специальности и соответствующих профессиональных компетенций.
2. Производственная (преддипломная) практика студентов является завершающим этапом и проводится после освоения ППССЗ СПО и сдачи студентами всех видов промежуточной аттестации, предусмотренных ФГОС.
3. Преддипломная практика реализуется в рамках профессиональных модулей

ПМ.01 – Планирование и организация работ по обеспечению защиты объекта;

ПМ.02. – Организация и технология работы с конфиденциальными документами;

ПМ.03 – Программно-аппаратные и инженерно-технические средства защиты информации;

ПМ.04 – Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих.

2.3. Место проведения преддипломной практики

Практика проводится в учреждениях, специфика работы которых связана с компьютерными информационными технологиями, в отделах информационной безопасности различных предприятий, научно- производственных предприятиях, занимающихся эксплуатацией и разработкой средств информационной безопасности.

При выборе базы практики учитываются следующие факторы: оснащенность современными аппаратно-программными средствами, оснащённость необходимым оборудованием, наличие квалифицированного персонала.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПРИ ПРОХОЖДЕНИИ ПРАКТИКИ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

3.1. Перечень планируемых результатов обучения при прохождении практики, соотнесенных с планируемыми результатами освоения образовательной программы Компетенции обучающегося, совершенствующиеся в ходе производственной (преддипломной) практики и формируемые в результате её прохождения.

Профессиональные компетенции

Основные виды профессиональной деятельности и профессиональные компе-	Наименование видов профессиональной деятельности и профессиональных компетенций
ПМ.01	Участие в планировании и организации работ по обеспечению защиты объекта
ПК 1.1	Участвовать в сборе и обработке материалов для выработки решений по обеспечению защиты информации и эффективному использованию средств обнаружения возможных каналов утечки конфиденциальной информации
ПК 1.2	Участвовать в разработке программ и методик организации защиты информации на объекте
ПК 1.3	Осуществлять планирование и организацию выполнения мероприятий по защите информации
ПК 1.4	Участвовать во внедрении разработанных организационных решений на объектах профессиональной деятельности
ПК 1.5	Вести учет, обработку, хранение, передачу, использование различных носителей конфиденциальной информации
ПК 1.6	Обеспечивать технику безопасности при проведении организационно-технических мероприятий
ПК 1.7	Участвовать в организации и проведении проверок объектов информатизации, подлежащих защите

ПК 1.8	Проводить контроль соблюдения персоналом требований режима защиты информации
ПК 1.9	Участвовать в оценке качества защиты объекта
ПМ.02	Организация и технология работы с конфиденциальными документами
ПК 2.1	Участвовать в подготовке организационных и распорядительных документов, регламентирующих работу по защите информации
ПК 2.2	Участвовать в организации и обеспечивать технологию ведения делопроизводства с учетом конфиденциальности информации
ПК 2.3	Организовывать документооборот, в том числе электронный, с учетом конфиденциальности информации
ПК 2.4	Организовывать архивное хранение конфиденциальных документов
ПК 2.5	Оформлять документацию по оперативному управлению средствами защиты информации и персоналом
ПК 2.6	Вести учет работ и объектов, подлежащих защите
ПК 2.7	Подготавливать отчетную документацию, связанную с эксплуатацией средств контроля и защиты информации
ПК 2.8	Документировать ход и результаты служебного расследования
ПК 2.9	Использовать нормативные правовые акты, нормативно-методические документы по защите информации
ПМ.03	Программно-аппаратные и технические средства защиты информации
ПК 3.1	Применять программно-аппаратные и технические средства защиты информации на защищаемых объектах
ПК 3.2	Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов
ПК 3.3	Проводить регламентные работы и фиксировать отказы средств защиты
ПК 3.4	Выявлять и анализировать возможные угрозы информационной безопасности объектов
ПМ.04	Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих.

По итогам прохождения практики в соответствие с практическим модулем ПМ. 01 – Планирование и организация работ по обеспечению защиты объекта обучающийся должен: Знать:

1. Виды и способы охраны объекта.
2. Особенности охраны персонала организации.
3. Основные направления и методы организации режима охраны объекта.
4. Разрешительную систему доступа к конфиденциальной информации.
5. Принципы действия систем аппаратуры контроля доступа.
6. Принципы построения и функционирования биометрических систем безопасности.
7. Требования и особенности оборудования режимных помещений.
8. Методы проверки персонала по защите информации.
9. Процедура служебного расследования нарушения сотрудниками режима работы с конфиденциальной информацией. Уметь:

1. Организовывать охрану персонала территорий, зданий, помещений и продукции предприятия (организации).
2. Пользоваться аппаратурой систем контроля доступа.
3. Выделять зоны доступа по типу и степени конфиденциальности работ.
4. Определять порядок организации и проведения рабочих совещаний.
5. Использовать методы защиты информации в рекламной и выставочной деятельности.
6. Использовать критерии подбора и расстановки сотрудников подразделений защиты информации.
7. Организовывать работу с персоналом, имеющим доступ к конфиденциальной информации.

Владеть:

1. Терминологией дисциплины «Обеспечение организации системы безопасности предприятия.
2. Методами физической защиты объекта.
3. Методами работы с устройствами контроля доступа к объекту.
4. Навыками организации работы с конфиденциальными материалами.

По итогам прохождения практики в соответствие с практическим модулем ПМ. 02. – Организация и технология работы с конфиденциальными документами обучающийся должен:

Знать:

1. Основные правовые акты в области информационной безопасности и защиты информации.
2. Нормативные акты и методические документы Федеральной службы, Федеральной службы по техническому и экспортному контролю в данной области.
3. Правовые основы защиты конфиденциальной информации по видам тайны.
4. Порядок лицензирования деятельности по технической защите конфиденциальной информации.
5. Правовые основы деятельности подразделений защиты информации;
6. Правовые основы допуска и доступа персонала к защищаемым сведениям.
7. Правовое регулирование взаимоотношений администрации и персонала.
8. Систему правовой ответственности за утечку.
9. Правовые нормы в области защиты интеллектуальной собственности.
10. Порядок отнесения информации к разряду конфиденциальной информации.
11. Порядок разработки, учёта, хранения, размножения и хранения конфиденциальных документов.
12. Организацию конфиденциального документооборота.
13. Технологию работы с конфиденциальными документами.
14. Организацию электронного документооборота.

Уметь:

1. Использовать в профессиональной деятельности нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в этой области.

2. Разрабатывать нормативно-методические материалы по регламентации системы организационной защиты информации.

3. Документировать ход и результаты служебного расследования.

4. Определять состав документируемой конфиденциальной информации. 5. Подготавливать, издавать и учитывать конфиденциальные документы.

6. Составлять номенклатуру конфиденциальных дел.

7. Формировать и оформлять конфиденциальные дела.

8. Организовывать и вести конфиденциальное делопроизводство, в том числе с использованием вычислительной техники.

9. Использовать системы электронного документооборота.

Владеть:

1. Методами ведения учёта и оформления бумажных и электронных носителей конфиденциальной информации;

2. Информационными технологиями электронного документооборота.

По итогам прохождения практики в соответствие с практическим модулем ПМ. 03 – Программно-аппаратные и инженерно-технические средства защиты информации обучающийся должен:

Знать:

1. Виды, источники и носители защищаемой информации.

2. Источники опасных сигналов.

3. Структуру, классификацию и основные технические характеристики каналов утечки информации.

4. Классификацию технических разведок и методы противодействия им.

5. Методы и средства технической защиты информации.

6. Методы сокрытия информации.

7. Программно-аппаратные средства защиты информации.

8. Основные правовые акты в области информационной безопасности и защиты информации.

9. Порядок лицензирования деятельности по технической защите конфиденциальной информации.

10. Правовые нормы в области защиты интеллектуальной собственности.

11. Организацию конфиденциального документооборота.

12. Технологию работы с конфиденциальными документами. Уметь:

1. Работать с техническими средствами защиты информации.

2. Работать с защищёнными автоматизированными системами.

3. Передавать информацию по защищённым каналам связи.

4. Фиксировать отказы в работе средств вычислительной техники. Владеть:

1. Опытом эксплуатации систем и средств защиты информации защищаемых объектов;

2. Методами применения технических средств защиты информации;

3. Методами выявления угроз информационной безопасности.

По итогам прохождения практики в соответствие практическим модулем ПМ. 04 – Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих обучающийся должен: Уметь:

1. Настраивать, удалять и добавлять компоненты (блоки) персональных компьютеров и серверов, заменять на совместимые.

2. Заменять, удалять и добавлять основные компоненты периферийных устройств, оборудования и компьютерной оргтехники.

3. Обеспечивать совместимость компонентов персональных компьютеров и серверов, периферийных устройств и оборудования.

4. Вести отчетную и техническую документацию.

5. Выполнять наладку, монтаж и настройку аппаратного обеспечения.

6. Выполнять инсталляцию и настройку программного обеспечения.

7. Выполнять сопряжение программно-аппаратного комплекса.

8. Выполнять наладку, монтаж и настройку аппаратного обеспечения.

9. Выполнять инсталляцию и настройку программного обеспечения выполнять сопряжение программно-аппаратного комплекса.

10. Удалять и добавлять компоненты (блоки) персональных компьютеров и серверов, заменять на совместимые.

11. Заменять, удалять и добавлять основные компоненты периферийных устройств, оборудования и компьютерной оргтехники.

12. Обеспечивать совместимость компонентов персональных компьютеров и серверов, периферийных устройств и оборудования.

13. Вести отчетную и техническую документацию.

4. ОБЪЕМ ПРАКТИКИ

Общая трудоемкость практики составляет 144 часа, 4 недели.

Наименование раздела (темы, этапа, вида работы)		Семестр	час.
1		2	3
1 Этап. Прибытие на практику. Знакомство с руководителем практики, экскурсия по предприятию. Инструктаж по прохождению практики, по технике безопасности.		8	6
2 Этап. Ознакомление с видами деятельности и общей структурой организации.		8	16
3 Этап. Изучение обязанностей работников среднего звена в основных подразделениях предприятия (юридический отдел, отдел кадров).		8	8
4 Этап. Выполнение отдельных заданий руководителя практики от предприятия.		8	6
5 Этап. Выполнение индивидуального задания по теме дипломной работы.		8	68
6 Этап. Написание дипломной работы с обоснованием выводов.		8	32
7 Этап. Оформление отчета и документов по практике, сдача отчета по практике.		8	8
Дифференцированный зачет (ДЗ)		8	ДЗ
Общая трудоемкость	час.		144
	зач. ед.		4

5. СОДЕРЖАНИЕ ПРАКТИКИ

5.1. Содержание разделов, тем, этапов, видов работ

№ п/п	Наименование раздела, темы, этапа, вида работы	Содержание раздела, темы, этапа, вида работы
1	1-й этап.	1. Прибытие на практику. Знакомство с руководителем практики, экскурсия по предприятию. Инструктаж по прохождению практики, по технике безопасности. Содержание практики, ее задачи, краткое содержание практики по профилю специальности. Содержание отчета и его оформление. Порядок оформления на работу. Вводный инструктаж по технике безопасности. Инструктаж по общим вопросам, охраны труда и техники безопасности, по режиму работы предприятия, знакомство с производственно-хозяйственной деятельностью организации.

2	2-й этап	2. Ознакомление с видами деятельности и общей структурой организации: - общие сведения о предприятии, учредительные документы, виды деятельности, подразделения организации, производственная и организационная структура организации, функциональные взаимосвязи подразделений и служб; - построение организационной структуры отдела; - ознакомление с функциональными областями на предприятии; - ознакомление с методами защиты средств вычислительной техники, защиты информации; - обеспечение информационной и компьютерной безопасности на предприятии; - организация и технология работы с конфиденциальными документами, правовая защита информации на предприятии; - ведение конфиденциального делопроизводства на предприятии организация и сопровождение электронного документооборота; - процедура создания документооборота организаций, учреждений и предприятий в рамках современного законодательства; - комплектование архива организации; - учет документов, проверка их наличия и состояния. управление электронными архивными ресурсами; - планирование и организация работ по обеспечению защиты объекта. обеспечение организации системы безопасности предприятия; - технические средства контроля доступа и безопасности; - основные критерии защищенности информационных автоматизированных систем.
3	3-й этап	3. Изучение обязанностей работников среднего звена в основных подразделениях предприятия (юридический отдел, отдел кадров).
4	4-й этап	4. Выполнение отдельных заданий руководителя практики от предприятия.
5	5- этап	5.Выполнение индивидуального задания по теме дипломной работы. Подбор материалов по индивидуальному заданию для подготовки выпускной квалификационной работы с помощью: - проведения собеседования с клиентами; - консультирования клиентов по интересующим их проблемам; - изучения по заданию руководства учреждения интересующих их проблем и подготовки ответов в виде служебных записок; - изучение нормативно-правовых документов

6 7 8	6-й этап	6. Написание дипломной работы с обоснованием выводов совершенствованию организации защиты информации на объекте прохождения практики.
9	7-й этап	7. Оформление отчета и документов по практике, сдача отчета по практике.

6. ФОРМЫ ОТЧЕТНОСТИ ПО ПРАКТИКЕ

Практика является завершающим этапом освоения профессионального модуля по виду профессиональной деятельности.

Практика завершается дифференцированным зачетом (зачетом с оценкой) при условии:

– положительного аттестационного листа по практике руководителей практики от организации и техникума об уровне освоения профессиональных компетенций;

– наличия положительной характеристики организации на обучающегося по освоению общих компетенций в период прохождения практики;

– полноты и своевременности предоставления дневника практики и отчета о практике в соответствии с заданием на практику.

Результаты прохождения практики представляются обучающимся в техникум и учитываются при прохождении государственной итоговой аттестации.

6.1. Дневник прохождения практики (оформление дневника)

Дневник прохождения преддипломной практики является обязательным отчетным документом, прилагаемым к отчету по практике.

Дневник ведется студентом в ходе практики самостоятельно в соответствии с перечнем этапов содержания практики, рабочей программой производственной (преддипломной) практики.

Несвоевременное заполнение студентом дневника является серьезным нарушением трудовой и учебной дисциплины.

6.2. Отчет по практике (структура, содержание и оформление отчета)

Отчет (пояснительная записка) по производственной практике является обязательным документом, который представляет собой:

1. Теоретический (описательный) материал по каждому этапу содержания практики;

2. Практический материал к теоретической части, оформленный в виде приложений (Приложения 1, 2, 3).

По окончании производственной (преддипломной) практики общим руководителем практики и (или) непосредственным руководителем практики от организации составляется заключение - характеристика на каждого студента.

Отчет студента по практике должен максимально отражать его индивидуальную работу в период прохождения преддипломной практики. Каждый студент должен самостоятельно отразить в отчете требования программы практики и своего индивидуального задания.

Студент должен собрать достаточно полную информацию и документы необходимые для выполнения дипломной работы. Сбор материалов должен вестись целенаправленно,

применительно к теме работы. Отчет по практике должен быть оформлен в соответствии с планом практики.

Обязательным при сдаче отчета является наличие приказа на практику с печатями предприятия, отзыв руководителя практики от предприятия и заключение самого студента по итогам прохождения практики с его предложениями и пожеланиями.

При оформлении отчета по производственной (преддипломной) практике его материалы располагаются в следующей последовательности:

1. Титульный лист.
2. Направление на практику.
3. Индивидуальное задание на преддипломную практику.
4. Дневник о прохождении практики.
5. Аттестационный лист, содержащий сведения об уровне освоения обучающимся профессиональных компетенций, а также характеристика на обучающегося по освоению профессиональных компетенций в период прохождения практики.
6. Отзыв-характеристика руководителя практики от организации.
7. Пояснительная записка: содержание, введение, основная часть, заключение, список используемых источников, приложения.
8. Отчет, дневник, отзыв-характеристика должны быть заверены печатью.

6.3. Защита отчета

Защита отчета проводится в соответствии с требованиями Положения об учебной и производственной практике студентов, осваивающих программы подготовки специалистов среднего звена среднего профессионального образования, утвержденного директором техникума. Дифференцированный зачет (оценка) по практикам выставляется на основании результатов защиты обучающимися отчетов по практике при наличии всех оформленных документов (дневник по практике с печатями, отчет по практике и др.). Положительная оценка по практике вносится в зачетно-экзаменационную ведомость и в зачетную книжку обучающегося за подписью руководителя практики от техникума.

7. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ПРАКТИКЕ

7.1. Перечень компетенций с указанием этапов их формирования и типовые контрольные задания или иные материалы для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Перечень профессиональных компетенций согласно учебного плана ППССЗ по специальности 10.02.01 Организация и технология защиты информации, а также приобретаемые в ходе производственных практик по профессиональным модулям представлены в п. 3.1. настоящей программы.

7.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

	Знания,	

Компетенции	умения навыки и (или) опыт деятельности	Оценочные средства (вопросы, типовые контрольные задания, тесты или иные материалы для оценки знаний, умений, навыков и (или) опыта деятельности)
ПМ.01	Участие в планировании и организации работ по обеспечению защиты объекта	
ПК 1.1	Знания	Контрольные вопросы: 1. Какие существуют виды охраны объекта? 2. Какие существуют способы охраны объекта? 3. Что понимается под каналом утечки информации? 4. Какие существуют технические средства обнаружения каналов утечки информации? 5. Как определяется эффективность использования средств обнаружения возможных каналов утечки информации?
	УМЕНИЯ	Контрольные вопросы:
		1. Как организовывать охрану персонала на территории организации? 2. Как организовывать охрану периметра территории организации? 3. Как организовывать охрану зданий и помещений организации? 4. Как организовывать охрану продукции организации?
	НАВЫКИ	Решение практических задач:
		1. Продемонстрируйте порядок применения досмотрового комплекта «Поиск-2У». 2. Объясните принцип работы измерителя уровня шумовых сигналов «Шорох-тест». 3. Перечислите и опишите ТТХ зонда монитора СРМ-700. 4. Определите канал утечки информации в диапазоне формата GSM-1800 с помощью профессионального приемника AR-3000A. 5. Изложите назначение детектора поля ST-006.
ПК 1.2.	знания	Контрольные вопросы 1 Изложите особенности охраны персонала организации. 2 Какова роль техника по защите информации по обеспечению охраны персонала организации? 3 Изложите основные направления организации режима охраны объекта. 4 Представьте основные методы организации режима охраны объекта. 5 Какими знаниями должен обладать техник по защите информации для участия в разработке программ и методик организации защиты информации на объекте? 6.

	УМЕНИЯ	Контрольные вопросы: 1. Что понимается под аппаратурой систем контроля доступа? 2. Какие вы знаете примеры технических систем контроля доступа? 3. Изложите обобщенную методику применения систем контроля доступа для организации защиты информации в организации. 4. Чем отличается методика выделения зоны доступа по типу конфиденциальности работ от степени конфиденциальности работ? 5. На чем основана методика выделения зоны доступа по типу и степени конфиденциальности работ?
	НАВЫКИ	Решение практических задач: 1. Продемонстрируйте порядок применения комплекса СЗИ НСД Secret Net (v. 4.0, для Windows 95/98). 2. Объясните принцип работы универсального замка крышки корпуса Case Look. 3. Перечислите и опишите тактико-технические данные комплекса аппаратно-программных средств Windows NT 4.0 и Windows 2000/XP/2003 (АПМДЗ) «КРИПТОН-ЗАМОК». 4. Определите возможный канал утечки информации в диапазоне формата GSM-1800 с помощью профессионального приемника AR-5000. 5. Изложите назначение комплекса СЗИ НСД «Аккорд NT/2000» v.2.0 (для ОС Windows NT/2000/XP, PCI).
ПК.1.3.	Знания	Контрольные вопросы: 1. Что понимается под планированием и организацией выполнения мероприятий по защите информации? 2. Изложите основные направления организации режима охраны объекта. 3. Какие вы знаете методы организации режима охраны объект? 4. Что понимается под режимом охраны объекта? 5. Перечислите и опишите классификацию режимов охраны объектов от несанкционированного доступа на его территорию.

	УМЕНИЯ	Контрольные вопросы: 1. Какими умениями должен обладать техник по защите информации для осуществления планирования и организации выполнения мероприятий по защите информации? 2. В чем состоит порядок организации и проведения рабочих совещаний на фирме в процессе осуществления планирования и организации выполнения мероприятий по защите информации? 3. Какие пункты плана должен предусмотреть техник по защите информации в процессе организации выполнения мероприятий по защите информации? 4. Требования каких нормативно-правовых документов необходимо соблюдать при осуществлении планирования и организации выполнения мероприятий по защите информации? 5. Какова роль аппаратуры систем контроля доступа в процессе организации выполнения мероприятий по защите информации?
	НАВЫКИ	Решение практических задач: 1. Продемонстрируйте порядок применения профессионального приемника AR-5000. 2. Объясните принцип работы и порядок применения электронного замка «Соболь PCI-1U». 3. Перечислите и опишите тактико-технические данные и порядок при менения детектора отладки процессов для Windows 9x «НКВД 3.2». 4. Определите возможный канал утечки информации с помощью программы поиска и гарантированного уничтожения информации на дисках «Terrier 3.0». 5. Изложите назначение и порядок применения системы защиты конфиденциальной информации «Secret Disk NG».
ПК 1.4	Знания	Контрольные вопросы: 1. Перечислите и опишите классификацию объектов профессиональной деятельности для обеспечения их информационной безопасности. 2. Изложите основные принципы построения биометрических систем безопасности. 3. Представьте принципы функционирования биометрических систем безопасности. 4. Изложите классификацию биометрических систем безопасности. 5. Какие знания необходимы для техника по защите информации для участия во внедрении разработанных организационных решений на объектах профессиональной деятельности?

	УМЕНИЯ	Контрольные вопросы: 1. Какие умения необходимы для техника по защите информации для участия во внедрении разработанных организационных решений на объектах профессиональной деятельности? 2. Изложите методы защиты информации в процессе реализации рекламной и выставочной деятельности. 3. Приведите сравнительный анализ по критерию эффективности защиты информации в процессе использования этих методов в рекламной и выставочной деятельности. 4. На кого возлагается ответственность за процедуру внедрения разработанных организационных решений на объектах профессиональной деятельности? 5. Изложите роль мероприятий по охране персонала территории, зданий, помещений и продукции организации во внедрении разработанных организационных решений защиты информации на объектах профессиональной деятельности.
	НАВЫКИ	Решение практических задач: 1. Продемонстрируйте порядок применения детектора поля ST-007. 2. Объясните принцип работы и порядок применения универсального поискового прибора D-008. 3. Перечислите и опишите тактико-технические данные и порядок применения зонда монитора СРМ-700. 4. Определите возможный канал утечки информации с помощью поискового приемника «Скорпион». 5. Изложите назначение и порядок применения многофункционального прибора ST-0Знания «Пиранья».
ПК.1.5.	Знания	Контрольные вопросы: 1. Перечислите и опишите классификацию различных видов носителей конфиденциальной информации. 2. Каким видам обработки подвергается информация на различных видах носителей конфиденциальной информации? 3. Какие знания необходимы технику по защите информации для выполнения операций по учету, обработке, хранению, передаче, использовании различных носителей конфиденциальной информации 4. Чем отличаются друг от друга операции учета, обработки, хранения, передачи, использования различных носителей конфиденциальной информации 5. Перечислите и опишите роль разрешительной системы доступа к операциям обработки конфиденциальной информации для работы с различными её носителями.

	УМЕНИЯ	Контрольные вопросы: 1. Как осуществляется учет различных носителей конфиденциальной информации? 2. Как выделять зоны доступа по типу и степени конфиденциальности работ при учете, обработки, хранения, передачи, использования различных носителей конфиденциальной информации? 3. Как определять порядок организации и проведения рабочих совещаний с применением различных носителей конфиденциальной информации? 4. Изложите порядок охраны зданий и помещений, в которых осуществляется учет, обработка, хранение, передача, использование различных носителей конфиденциальной информации 5. Укажите роль аппаратуры систем контроля доступа в здания и помещения, в которых осуществляется учет, обработка, хранение, передача, использование различных носителей конфиденциальной информации.
	НАВЫКИ	Решение практических задач: 1. Продемонстрируйте порядок применения зонда монитора СРМ-700. 2. Объясните принцип работы и порядок применения комплекта для оценки каналов утечки информации ПКУ-6. 3. Перечислите и опишите тактико-технические данные и порядок применения детектора поля ST-007. 4. Определите возможный канал утечки информации с помощью профессионального приемника AR-8200. 5. Изложите назначение и порядок применения нановольт-метра Unipan 237.
ПК.1.6.	Знания	Контрольные вопросы: 1. Изложите методику обеспечения техники безопасности при проведении организационно-технических мероприятий. 2. Какова роль электробезопасности в общей системе техники безопасности при проведении организационно-технических мероприятий по защите информации? 3. Что понимается под организационно-техническими мероприятиями по обеспечению защиты информации на производстве? 4. Какова роль функционирования биометрических систем безопасности при проведении организационно-технических мероприятий по защите информации?

		5. Кто несет ответственность за соблюдение техники безопасности при проведении организационно-технических мероприятий?
	УМЕНИЯ	Контрольные вопросы: 1. Какие умения должен проявить техник по защите информации в процессе обеспечения техники безопасности при проведении организационно-технических мероприятий? 2. Какова очередность операций при проведении организационно-технических мероприятий в организации в процессе обеспечения защиты информации? 3. Какие критерии подбора и расстановки сотрудников подразделений защиты информации необходимо использовать в процессе обеспечения техники безопасности при проведении организационно-технических мероприятий? 4. Каким критериям должен соответствовать техник по защите информации при обеспечении техники безопасности при проведении организационно-технических мероприятий? 5. Какие документы организации – объекта защиты информации необходимо соблюдать в процессе обеспечения техники безопасности при проведении организационно-технических мероприятий по защите информации?
	НАВЫКИ	Решение прикладных задач: 1. Приведите примеры терминов дисциплины «Обеспечение организации системы безопасности предприятия». 2. Представьте два-три примера аппаратных средств физической защиты информации. 3. Какова роль специального программного обеспечения Sedif Pro+ в процессе обеспечения техники безопасности при проведении организационно-технических мероприятий по защите информации? 4. Как можно использовать специальное программное обеспечение для аппаратуры выявления каналов утечки информации АРК-Д6 в процессе обеспечения техники без опасности при проведении организационно-технических мероприятий по защите информации? 5. 5. Изложите тактико-технические данные нелинейного локатора

		«Катран».
ПК.1.7.	Знания	Контрольные вопросы: 1. Какими знаниями должен обладать техник по защите информации для участия в организации и проведении проверок объектов информатизации, подлежащих защите? 2. Какие основные технические средства могут использоваться в процессе организации и проведении проверок объектов информатизации, подлежащих защите? 3. Какие основные типы программного обеспечения необходимо использовать при проведении проверок объектов информатизации, подлежащих защите? 4. Какие направления и методы организации режима охраны объекта проверяются при проведении проверок объектов информатизации, подлежащих защите? 5. Какие виды и способы охраны объекта подлежат контролю в процессе проведения проверок объектов информатизации, подлежащих защите.
	УМЕНИЯ	Контрольные вопросы: 1. Какими умениями должен обладать техник по защите информации в процессе участия в организации и проведении проверок объектов информатизации, подлежащих защите? 2. Как организовывать работу с персоналом, имеющим доступ к конфиденциальной информации для участия в организации и проведении проверок объектов информатизации, подлежащих защите? 3. Какие критерии подбора и расстановки сотрудников подразделений защиты информации используются для участия в организации и проведении проверок объектов информатизации, подлежащих защите 4. Какие методы защиты информации в рекламной и выставочной деятельности подлежат контролю в ходе проведения проверок объектов информатизации, подлежащих защите? 5. Какая основная аппаратура систем контроля доступа должна быть подвержена анализу в ходе организации и проведения

		проверок объектов информатизации, подлежащих защите?
	НАВЫКИ	Решение практических задач: 1. Продемонстрируйте порядок применения детектора СВЧ излучений ДСВЧИ-0Знания. 2. Объясните принцип работы и порядок применения ручного измерителя частоты РИЧ-3. 3. Перечислите и опишите тактико-технические данные и порядок применения логопериодической направленной малогабаритной антенны АРК-А3-2. 4. Определите возможный канал утечки информации с помощью детектора радиопередающих устройств Protect-1203. 5. Изложите назначение и порядок применения скоростного приемника коррелятора SEL SP-81 «Оракул».
ПК.1.8.	Знания	Контрольные вопросы: 1. Перечислите и опишите разновидности методов проверки персонала по защите информации. 2. Изложите особенности реализации методов проверки персонала по защите информации со стороны техника по защите информации. 3. В каких нормативных документах организации изложены требования в отношении соблюдения режима защиты информации? 4. В чем состоит процедура служебного расследования нарушения сотрудниками режима работы с конфиденциальной информацией? 5. В каких случаях необходимо проводить служебное расследование нарушения сотрудниками режима работы с конфиденциальной информацией?
	УМЕНИЯ	Контрольные вопросы: 1. Назовите критерии подбора и расстановки сотрудников подразделений защиты информации для обеспечения соблюдения ими требований режима защиты информации. 2. Кто отвечает за подбор и расстановку сотрудников подразделений защиты информации для обеспечения режима защиты информации в организации? 3. Как влияет организация работы с персоналом, имеющим доступ к конфиденциальной информации на режим защиты информации на предприятии? 4. Какова роль мероприятий по выделению зон доступа по типу и степени конфиденциальности работ на соблюдение персоналом

		требований режима защиты информации? 5. Перечислите и опишите особенности проведения контроля соблюдения персоналом требований режима защиты информации в рекламной и выставочной деятельности организации.
	НАВЫКИ	Решение практических задач: 1. Продемонстрируйте порядок применения средства оценки размеров зоны существования опасного речевого сигнала с помощью многофункционального прибора ST-0Знания «Пиранья». 2. Объясните принцип работы и порядок применения средства контроля электромагнитных излучений, а также сигналов в проводных коммуникациях с помощью комплекта для оценки каналов утечки информации ПКУ-6М. 3. Перечислите и опишите тактико-технические данные и порядок применения средства контроля ИК-излучений с помощью зонда-монитора СРМ-700. 4. Определите возможный канал утечки информации с помощью средства контроля электромеханических параметров проводных коммуникаций портативным цифровым рефлектометром «Рейс». Изложите назначение и порядок применения средства защиты информации - генератора шума ГШК-1000М
ПК.1.9.	Знания	Контрольные вопросы: 1. Что понимается под оценкой качества защиты объекта? 2. Какие критерии применяются для оценки качества защиты объекта? 3. Какова роль применяемых видов и способов охраны объекта в оценке качества защиты объекта? 4. Реализация каких принципов действия систем аппаратуры контроля доступа обеспечивает требуемое качество защиты объекта? 5. Какими знаниями должен обладать техник по защите информации для полноправного участия в оценке качества защиты объекта?
	УМЕНИЯ	Контрольные вопросы: 1. Какими умениями должен обладать техник по защите информации в процессе выделения зон доступа по типу и степени конфиденциальности работ, участвуя в оценке качества защиты объекта?

		2. Как установленный порядок организации и проведения рабочих совещаний в организации влияет на качество защиты объекта? 3. Какую роль играют методы защиты информации в рекламной и выставочной деятельности организации в общей системе оценки качества защиты объекта? 4. Как критерии подбора и расстановки сотрудников подразделений защиты информации влияют на оценку качества защиты объекта? 5. Кто из персонала организации, имеющего доступ к конфиденциальной информации может участвовать в оценке качества защиты объекта?
	НАВЫКИ	Решение практических задач: 1. Продемонстрируйте порядок применения средства оценки размеров зоны существования опасного речевого сигнала с помощью измерителя уровня шумовых сигналов «Шорох-тест». 2. Объясните принцип работы и порядок применения средства контроля электромагнитных излучений, а также сигналов в проводных коммуникациях с помощью аппаратуры выявления каналов утечки информации АРК-Д6. 3. Перечислите и опишите тактико-технические данные и порядок применения многофункционального прибора ST-0Знания «Пиранья». 4. Определите возможный канал утечки информации с помощью средства контроля электромеханических параметров проводных коммуникаций - дифференциальным адаптером проводных линий в речевом диапазоне ДАПЛ-0Знания. 5. Изложите назначение и порядок применения средства защиты информации - генератора шума «Гром-ЗИ-4».
ПМ.02 Организация и технология работы с конфиденциальными документами		
ПК.2.1.	Знания	Контрольные вопросы: 1. Назовите основные правовые акты в области информационной безопасности и защиты информации, которые должен знать техник по защите информации для участия в подготовке организационных и распорядительных документов, регламентирующих работу по защите информации. 2. Какие нормативные акты и методические документы Федеральной службы безопасности, Федеральной службы по техническому и экспортному контролю в данной области

		необходимо использовать в процессе подготовки организационных и распорядительных документов, регламентирующих работу по защите информации? 3. Что относится к основам защиты конфиденциальной информации по видам тайны при подготовке организационных и распорядительных документов, регламентирующих работу по защите информации? 4. Перечислите и опишите порядок лицензирования деятельности по технической защите конфиденциальной информации. 5. Какие правовые основы деятельности подразделений защиты информации должен учитывать техник по защите информации при участии в подготовке организационных и распорядительных документов, регламентирующих работу по защите информации?
	УМЕНИЯ	Контрольные вопросы: 1. Перечислите и опишите обязанности техника по защите информации при формировании и оформлении конфиденциальных дел в процессе участия в подготовке организационных и распорядительных документов, регламентирующих работу по защите информации. 2. Что должен уметь техник по защите информации по составлению номенклатуры конфиденциальных дел в процессе участия в подготовке организационных и распорядительных документов, регламентирующих работу по защите информации 3. Как можно использовать системы электронного документооборота в процессе участия в подготовке организационных и распорядительных документов, регламентирующих работу по защите информации? 4. Изложите обязанности техника по защите информации при использовании в профессиональной деятельности нормативных правовых актов в области информационной безопасности и защиты информации, а также нормативных методических документов Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в этой области в процессе участия в подготовке организационных и распорядительных документов, регламентирующих работу по защите информации. 5. Как должен документировать ход и результаты служебного расследования техник по защите информации в процессе участия в подготовке организационных и распорядительных

		документов, регламентирующих работу по защите информации?
	НАВЫКИ	Решение практических задач: 1. Продемонстрируйте порядок применения профессионального приемника AR-5000. 2. Объясните принцип работы и порядок применения электронного замка «Соболь PCI-1U». 3. Перечислите и опишите тактико-технические данные и порядок применения детектора отладки процессов для Windows 9x «НКВД 3.2». 4. Определите возможный канал утечки информации с помощью программы поиска и гарантированного уничтожения информации на дисках «Terrier 3.0». 5. Изложите назначение и порядок применения системы защиты конфиденциальной информации «Secret Disk NG».
ПК 2.2	Знания	Контрольные вопросы: 1. Изложите основные правовые акты в области информационной безопасности и защиты информации, которые должен знать техник по защите информации для участия в организации и обеспечения технологии ведения делопроизводства с учетом конфиденциальности информации. 2. Назовите нормативные акты и методические документы Федеральной службы безопасности, Федеральной службы потехническому и экспортному контролю, которые должен знать техник по защите информации для участия в организации и обеспечения технологии ведения делопроизводства с учетом конфиденциальности информации. 3. Какие правовые основы защиты конфиденциальной информации по видам тайны должен знать техник по защите информации для участия в организации и обеспечения технологии ведения делопроизводства с учетом конфиденциальности информации. 4. Перечислите позиции порядка лицензирования деятельности по технической защите конфиденциальной информации, которые должен знать техник по защите информации для участия в организации и обеспечения технологии ведения делопроизводства.

	УМЕНИЯ	Контрольные вопросы: 1. Как надо составлять номенклатуру конфиденциальных дел, участвуя в организации и обеспечении технологии ведения делопроизводства с учетом конфиденциальности информации? 2. Изложите процесс документирования хода и результаты служебного расследования, участвуя в организации и обеспечении технологии ведения делопроизводства с учетом конфиденциальности информации? 3. Как надо определять состав документируемой конфиденциальной информации, участвуя в организации и обеспечении технологии ведения делопроизводства с учетом конфиденциальности информации? 4. Изложите порядок подготовки, издания и учета конфиденциальных документов, участвуя в организации и обеспечении технологии ведения делопроизводства с учетом конфиденциальности информации? 5. Как техник по защите информации должен составлять номенклатуру конфиденциальных дел, участвуя в организации и обеспечении технологии ведения делопроизводства с учетом конфиденциальности информации?
	НАВЫКИ	Решение практических задач: 1. Продемонстрируйте порядок применения детектора поля ST-007. 2. Объясните принцип работы и порядок применения универсального поискового прибора D-008. 3. Перечислите и опишите тактико-технические данные и порядок применения зонда монитора СРМ-700. 4. Определите возможный канал утечки информации с помощью поискового приемника «Скорпион». 5. Изложите назначение и порядок применения многофункционального прибора ST-0Знания «Пиранья»
ПК 2.3	Знания	Контрольные вопросы: 1. Назовите правовые основы допуска и доступа персонала к защищаемым сведениям в процессе организации документооборота, в том числе электронного, с учетом конфиденциальности информации. 2. Как осуществляется правовое регулирование взаимоотношений администрации и персонала в процессе организации документооборота, в том числе электронного, с учетом конфиденциальности информации? 3. Что входит в систему правовой ответственности за утечку информации в процессе организации документооборота, в том числе электронного, с учетом конфиденциальности информации? 4. Назовите правовые нормы в области защиты интеллектуальной собственности в процессе организации

		документооборота, в том числе электронного, с учетом конфиденциальности информации. 5. Каков порядок отнесения информации к разряду конфиденциальной информации в процессе организации документооборота, в том числе электронного, с учетом конфиденциальности информации?
	УМЕНИЯ	Контрольные вопросы: 1. Какими умениями должен обладать техник по защите информации в процессе организации документооборота, в том числе электронного, с учетом конфиденциальности информации? 2. Какие нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в этой области должен использовать в профессиональной деятельности техник по защите информации в процессе организации документооборота, в том числе электронного, с учетом конфиденциальности информации? 3 Какие обязанности при составлении номенклатуры конфиденциальных дел должен исполнять техник по защите информации в процессе организации документооборота, в том числе электронного, с учетом конфиденциальности информации? 4 Как должен формировать и оформлять конфиденциальные дела техник по защите информации в процессе организации документооборота, в том числе электронного, с учетом конфиденциальности информации? 5. Должен ли разрабатывать нормативно-методические материалы по регламентации системы организационной защиты информации техник по защите информации в процессе организации документооборота, в том числе электронного, с. учетом конфиденциальности информации?
	НАВЫКИ	Решение практических задач: 1. Продемонстрируйте порядок применения зонда монитора СРМ-700. 2. Объясните принцип работы и порядок применения комплекта для оценки каналов утечки информации ПКУ-6. 3. Перечислите и опишите тактико-технические данные и порядок применения детектора поля ST-007. 4. Определите возможный канал утечки информации с помощью профессионального приемника AR-8200. 5. Изложите назначение и порядок применения нановольт-метра Unipan 237.

ПК.2.4.	Знания	1. Перечислите основные правовые акты в области информационной безопасности и защиты информации при организации архивного хранения конфиденциальных документов. 2. Назовите нормативные акты и методические документы Федеральной службы безопасности, Федеральной службы по техническому и экспортному контролю в данной области при организации архивного хранения конфиденциальных документов. 3. Какие правовые основы защиты конфиденциальной информации по видам тайны должен знать техник по защите информации при организации архивного хранения конфиденциальных документов? 4. Изложите порядок лицензирования деятельности по технической защите конфиденциальной информации при организации архивного хранения конфиденциальных документов. 5. Что относится к правовым основам деятельности подразделений защиты информации при организации архивного хранения конфиденциальных документов?
	УМЕНИЯ	Контрольные вопросы: 1. Изложите технологию формирования и оформления конфиденциальных дел на архивное хранение. 2. Каковы особенности организации и ведения конфиденциального делопроизводства для архивного хранения, в том числе с использованием вычислительной техники? 3. Как возможно использовать системы электронного документооборота для организации архивного хранения конфиденциальных документов? 4. Какими умениями должен обладать техник по защите информации для осуществления возможности разрабатывать нормативно-методические материалы по регламентации системы защиты информации в процессе организации архивного хранения конфиденциальных документов? 5. В чем состоит актуальность использовать в профессиональной деятельности нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности

		Российской Федерации, Федеральной службы по техническому и экспортному контролю в этой области для организации архивного хранения конфиденциальных документов?
	НАВЫКИ	Решение практических задач: 1. Продемонстрируйте порядок применения детектора СВЧ излучений ДСВЧИ-0Знания. 2. Объясните принцип работы и порядок применения ручного измерителя частоты РИЧ-3. 3. Перечислите и опишите тактико-технические данные и порядок применения логопериодической направленной малогабаритной антенны АРК-А3-2. 4. Определите возможный канал утечки информации с помощью детектора радиопередающих устройств Protect-1203. 5. Изложите назначение и порядок применения скоростного приемника коррелятора SEL SP-81 «Оракул».
ПК 2.5.	Знания	Контрольные вопросы: 1. Изложите порядок разработки, учёта, хранения, размножения и хранения конфиденциальных документов в процессе оформления документации по оперативному управлению средствами защиты информации и персоналом. 2. Перечислите и опишите порядок отнесения информации к разряду конфиденциальной информации в процессе оформления документации по оперативному управлению средствами защиты информации и персоналом. 3. В чем состоит организация конфиденциального документооборота в процессе оформления документации по оперативному управлению средствами защиты информации и персоналом? 4. Что представляет собой технология работы с конфиденциальными документами в процессе оформления документации по оперативному управлению средствами защиты информации и персоналом? 5. Назовите правовые нормы в области защиты интеллектуальной собственности в процессе оформления документации по оперативному управлению средствами защиты информации и персоналом.
	УМЕНИЯ	Контрольные вопросы: 1. Перечислите и опишите технологию использования системы электронного документооборота в процессе оформления документации по оперативному управлению средствами защиты информации и персоналом. 2. Какими умениями должен обладать техник по защите

		информации, чтобы разрабатывать нормативно- методические материалы по регламентации системы организационной защиты информации в процессе оформления документации по оперативному управлению средствами защиты информации и персоналом? Н1 3. Какие принципы должны соблюдаться при документировании хода и результатов служебного расследования в процессе оформления документации по оперативному управлению средствами защиты информации и персоналом? 4. Как техник по защите информации должен подготавливать, издавать и учитывать конфиденциальные документы в процессе оформления документации по оперативному управлению средствами защиты информации и персоналом? 5. Перечислите и опишите технологию составления номенклатуры конфиденциальных дел в процессе оформления документации по оперативному управлению средствами защиты информации и персоналом?
	НАВЫКИ	Решение практических задач: 1. Продемонстрируйте порядок применения средства оценки размеров зоны существования опасного речевого сигнала с помощью многофункционального прибора ST-0Знания «Пиранья». 2. Объясните принцип работы и порядок применения средства контроля электромагнитных излучений, а также сигналов в проводных коммуникациях с помощью комплекта для оценки каналов утечки информации ПКУ-6М. 3. Перечислите и опишите тактико-технические данные и порядок применения средства контроля ИК-излучений с помощью зонда и монитора СРМ-700. 4. Определите возможный канал утечки информации с помощью средства контроля электромеханических параметров проводных коммуникаций портативным цифровым рефлектометром «Рейс». 5. Изложите назначение и порядок применения средства защиты информации - генератора шума ГШК-1000М.
ПК 2.6.	Знания	Контрольные вопросы: 1. В чем состоит организация электронного документооборота в процессе ведения учета работ и объектов, подлежащих защите?

		2. Перечислите и опишите порядок лицензирования деятельности по технической защите конфиденциальной информации в процессе ведения учета работ и объектов, подлежащих защите? 3. Что относится к правовым основам допуска и доступа персонала к защищаемым сведениям в процессе ведения учета работ и объектов, подлежащих защите? 4. Перечислите и опишите, что относится к системе правовой ответственности за утечку информации в процессе ведения учета работ и объектов, подлежащих защите? 5. Изложите технологию работы с конфиденциальными документами в процессе ведения учета работ и объектов, подлежащих защите?
	УМЕНИЯ	Контрольные вопросы: 1. Изложите порядок определения состава документируемой конфиденциальной информации при ведении учета работ и объектов, подлежащих защите. 2. Какими умениями должен обладать техник по защите информации при разработке нормативно-методических материалов по регламентации системы организационной защиты информации при ведении учета работ и объектов, подлежащих защите? 3. Как необходимо использовать в профессиональной деятельности нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в этой области при ведении учета работ и объектов, подлежащих защите? 4. Как необходимо использовать системы электронного документооборота при ведении учета работ и объектов, подлежащих защите? 5. Для реализации каких задач необходимо организовывать и вести конфиденциальное делопроизводство, в том числе с использованием вычислительной техники при ведении учета работ и объектов, подлежащих защите?
	НАВЫКИ	Решение практических задач: 1. Продемонстрируйте порядок применения средства оценки размеров зоны существования опасного речевого сигнала с помощью измерителя уровня шумовых сигналов «Шорох-тест». 2. Объясните принцип работы и порядок применения средства контроля электромагнитных излучений, а также сигналов в проводных коммуникациях с помощью аппаратуры выявления каналов утечки информации АРК-Д6.

		3. Перечислите и опишите тактико-технические данные и порядок применения многофункционального прибора ST-0Знания «Пиранья». 4. Определите возможный канал утечки информации с помощью средства контроля электромеханических параметров проводных коммуникаций - дифференциальным адаптером проводных линий в речевом диапазоне ДАПЛ-0Знания. 5. Изложите назначение и порядок применения средства защиты информации - генератора шума «Гром-ЗИ-4».
ПК 2.7.	Знания	Контрольные вопросы: 1. Приведите примеры нормативных актов и методических документов Федеральной службы безопасности, Федеральной службы по техническому и экспортному контролю в данной области при подготовке отчетной документации, связанной с эксплуатацией средств контроля и защиты информации. 2. Какие действия техника по защите информации относится к организации электронного документооборота при подготовке отчетной документации, связанной с эксплуатацией средств контроля и защиты информации? 3. Назовите правовые нормы в области защиты интеллектуальной собственности при подготовке отчетной документации, связанной с эксплуатацией средств контроля и защиты информации. 4. Каков порядок разработки, учёта, хранения, размножения и хранения конфиденциальных документов при подготовке отчетной документации, связанной с эксплуатацией средств контроля и защиты информации? 5. В чем состоит организацию конфиденциального документооборота при подготовке отчетной документации, связанной с эксплуатацией средств контроля и защиты информации?
	УМЕНИЯ	Контрольные вопросы: 1.Представьте порядок составления номенклатуры конфиденциальных дел при подготовке отчетной документации, связанной с эксплуатацией средств контроля и защиты информации. 2. Как необходимо формировать и оформлять конфиденциальные

		дела при подготовке отчетной документации, связанной с эксплуатацией средств контроля и защиты информации? 3. Как можно использовать системы электронного документооборота при подготовке отчетной документации, связанной с эксплуатацией средств контроля и защиты информации? Какими навыками должен обладать техник по защите информации, чтобы подготавливать, издавать и учитывать конфиденциальные документы при подготовке отчетной документации, связанной с эксплуатацией средств контроля и защиты информации? 5. Как должен техник по защите информации определять состав документируемой конфиденциальной информации при подготовке отчетной документации, связанной с эксплуатацией средств контроля и защиты информации?
	НАВЫКИ	Решение практических задач: 1. Продемонстрируйте порядок применения средства оценки размеров зоны существования опасного речевого сигнала с помощью калибратора акустического сигнала CAL-200. 2. Объясните принцип работы и порядок применения средства контроля электромагнитных излучений, а также сигналов в проводных коммуникациях с помощью ручного измерителя частоты CUB. 3. Перечислите и опишите тактико-технические данные и порядок применения зонда монитора СРМ-700. 4. Определите возможный канал утечки информации с помощью средства контроля электромеханических параметров проводных коммуникаций - портативного цифрового рефлектометра «Рейс». 5. Изложите назначение и порядок применения средства защиты информации - прибора комплексной защиты телефонной линии Прокруст-2000.
ПК 2.8.	Знания	Контрольные вопросы: 1. Изложите технологию работы с конфиденциальными документами при документировании хода и результатов служебного расследования. 2. В чем состоит организация электронного документооборота при документировании хода и результатов служебного расследования.

		3. Изложите организацию конфиденциального документооборота при документировании хода и результатов служебного расследования. 4. Каков порядок отнесения информации к разряду конфиденциальной информации при документировании хода и результатов служебного расследования. 5. Какие правовые основы защиты конфиденциальной информации по видам тайны должен соблюдать техник по защите информации при документировании хода и результатов служебного расследования.
	УМЕНИЯ	Контрольные вопросы: 1. Как можно использовать системы электронного документооборота в процессе документирования хода и результатов служебного расследования? 2. Как можно организовывать и вести конфиденциальное делопроизводство, в том числе с использованием вычислительной техники в процессе документирования хода и результатов служебного расследования? 3. Изложите порядок составления номенклатуры конфиденциальных дел в процессе документирования хода и результатов служебного расследования? 4. Какими умениями должен обладать техник по защите информации, чтобы разрабатывать нормативно-методические материалы по регламентации системы организационной защиты информации в процессе документирования хода и результатов служебного расследования? Как можно определять состав документируемой конфиденциальной информации в процессе документирования хода и результатов служебного расследования?
	НАВЫКИ	Решение практических задач: 1. Продемонстрируйте порядок применения средства оценки размеров зоны существования опасного речевого сигнала с помощью измерителя уровня шумовых сигналов «Шорох-тест». 2. Объясните принцип работы и порядок применения средства контроля электромагнитных излучений, а также сигналов в проводных коммуникациях с помощью аппаратуры выявления каналов утечки информации АРК-Д6. 3. Перечислите и опишите тактико-технические данные и порядок применения многофункционального прибора ST-0Знания «Пиранья». 4. Определите возможный канал утечки информации с помощью средства контроля электромеханических параметров проводных

		коммуникаций - дифференциальным адаптером проводных линий в речевом диапазоне ДАПЛ-0Знания. 5. Изложите назначение и порядок применения средства защиты информации - генератора шума «Гром-ЗИ-4».
ПК 2.9.	Знания	Контрольные вопросы: 1. Какие нормативные правовые акты, нормативно-методические документы по защите информации может использовать техник по защите информации при организации электронного документооборота? 2. Какие нормативные правовые акты, нормативно-методические документы по защите информации может использовать техник по защите информации при организации конфиденциального документооборота? 3. Какие нормативные правовые акты, нормативно-методические документы по защите информации может использовать техник по защите информации, работая в пределах системы правовой ответственности за утечку информации? 4. Какие нормативные правовые акты, нормативно-методические документы по защите информации может использовать техник по защите информации, работая в области защиты интеллектуальной собственности? 5. Какие нормативные правовые акты, нормативно-методические документы по защите информации может использовать техник
	УМЕНИЯ	Контрольные вопросы: 1. Как техник по защите информации должен использовать системы электронного документооборота при применении нормативных правовых актов, нормативно-методических документов по защите информации? 2. Как техник по защите информации должен формировать и оформлять конфиденциальные дела при применении нормативных правовых актов, нормативно- методических документов по защите информации? 3. Как техник по защите информации должен организовывать и вести конфиденциальное делопроизводство, в том числе с использованием вычислительной техники при применении нормативных правовых актов, нормативно- методических документов по защите информации? 4. Как техник по защите информации должен определять состав документируемой конфиденциальной информации при применении нормативных правовых актов, нормативно-методических документов по защите информации? 5. Как техник по защите информации должен составлять номенклатуру конфиденциальных дел при применении нормативных правовых актов, нормативно-методических документов по защите информации?

	НАВЫКИ	Решение практических задач: 1. Продемонстрируйте порядок применения комплекса Отбой А. 2. Объясните принцип работы и порядок применения комплекта для оценки каналов утечки информации ПКУ-6М. 3. Перечислите и опишите тактико-технические данные и порядок применения универсального проверочного устройства проводных линий «Улан». 4. Определите возможный канал утечки информации с помощью универсального приемника XPLORER. 5. Изложите назначение и порядок применения широкополосной активной антенны АРК-А7А.
ПМ.03. Программно-аппаратные и технические средства защиты информации		
ПК 3.1.	Знания	Контрольные вопросы: 1. Перечислите и опишите виды, источники и носители защищаемой информации при применении программно-аппаратных и технических средств защиты информации на защищаемых объектах. 2. Что относится к источникам опасных сигналов при применении программно-аппаратных и технических средств защиты информации на защищаемых объектах? 3. Какие методы сокрытия информации вы знаете при применении программно-аппаратных и технических средств защиты информации на защищаемых объектах? 4. Каков порядок лицензирования деятельности по технической защите конфиденциальной информации при применении программно-аппаратных и технических средств защиты информации на защищаемых объектах? 5. Перечислите и опишите технологию работы с конфиденциальными документами при применении программно-аппаратных и технических средств защиты информации на защищаемых объектах?
	УМЕНИЯ	Контрольные вопросы: 1. Какими умениями должен обладать техник по защите информации при применении программно-аппаратных и технических средств защиты информации на защищаемых объектах? 2. Что должен учитывать техник по защите информации, передавая информацию по защищённым каналам связи, при применении программно-аппаратных и технических средств защиты информации на защищаемых объектах

		3. С помощью каких технических средств техник по защите информации может фиксировать отказы в работе средств вычислительной техники при применении программно-аппаратных и технических средств защиты информации на защищаемых объектах? 4. Какие нормативно-правовые документы должен соблюдать техник по защите информации при применении программно-аппаратных и технических средств защиты информации на защищаемых объектах? 5. Какие положения должностной инструкции должен соблюдать техник по защите информации при применении программно-аппаратных и технических средств защиты информации на защищаемых объектах?
	НАВЫКИ	Применение практических вводных: 1. Приведите примеры систем и средств защиты информации при применении программно-аппаратных и технических средств защиты информации на защищаемых объектах. 2. Приведите классификацию методов применения технических средств защиты информации на защищаемых объектах. 3. К реализации какого метода выявления угроз информационной безопасности относится применение средства создания модели системы разграничения доступа «Ревизор-1 XP»?
ПК 3.2.	Знания	Контрольные вопросы: 1. Приведите классификацию технических разведок и методы противодействия им, которые должен учитывать техник по защите информации, участвуя в процессе эксплуатации систем и средств защиты информации защищаемых объектов. 2. Какие методы и средства технической защиты информации должен знать техник по защите информации, участвуя в процессе эксплуатации систем и средств защиты информации защищаемых объектов? 3. Каковы особенности программно-аппаратных средств защиты информации должен учитывать техник по защите информации, участвуя в процессе эксплуатации систем и средств защиты информации защищаемых объектов? 4. Какие правовые норм в области защиты интеллектуальной собственности должен соблюдать техник по защите информации в процессе эксплуатации систем и средств защиты информации защищаемых объектов?

		5. Что представляет собой технология работы с конфиденциальными документами при применении программно-аппаратных и технических средств защиты информации на защищаемых объектах?
	УМЕНИЯ	Контрольные вопросы: 1. Какие умения должен проявить техник по защите информации, участвуя в процессе эксплуатации систем и средств защиты информации защищаемых объектов? 2. Что из нормативных документов в первую очередь должен соблюдать техник по защите информации, участвуя в процессе эксплуатации систем и средств защиты информации защищаемых объектов? 3. Какие каналы утечки информации должен учитывать техник по защите информации, участвуя в процессе эксплуатации систем и средств защиты информации защищаемых объектов? 4. Какие правила ведения электронного документооборота должен выполнять техник по защите информации, участвуя в процессе эксплуатации систем и средств защиты информации защищаемых объектов. 5. Какие виды режима охраны объекта должен обеспечить техник по защите информации, участвуя в процессе эксплуатации систем и средств защиты информации защищаемых объектов?
	НАВЫКИ	Решение практических задач: 1. Продемонстрируйте порядок применения стационарного подавителя диктофонов «Сапфир». 2. Объясните принцип работы и порядок применения генератора шума «Гром-ЗИ-4». 3. Перечислите и опишите тактико-технические данные и порядок применения гибкого эндоскопа ЭТГ-8-0,5. 4. Можно ли определить возможный канал утечки информации с помощью портативного селективного металлодетектора «АКА-7215М»? 6. Изложите назначение и порядок применения обнаружителя скрытых видеокамер по ПЭМИН «Айрис IQ-2V».
ПК 3.3.	Знания	Контрольные вопросы: 1. Что понимается под регламентными работами на средствах

		технической защиты информации? 2. Что понимается под термином «отказы» средств защиты информации? 3. Какие знания должен проявить техник по защите информации при проведении регламентных работ на средствах защиты информации. 4. С помощью каких технических и программных средств техник фиксирует отказы средств защиты информации? 5. Что понимается под вероятностью безотказной работы средств защиты информации?
	УМЕНИЯ	Контрольные вопросы: 1. Какими умениями должен обладать техник по защите информации, работая с техническими средствами защиты информации? 2. Какие регламентные работы необходимо выполнять технику по защите информации, работая с защищёнными автоматизированными системами? 3. Как техник по защите информации должен фиксировать отказы средств защиты информации, передавая информацию по защищённым каналам связи? 4. Какие способы фиксирования отказов в работе средств вычислительной техники могут применяться техником? 5. В чем проявляются умения техника по защите информации в процессе проведения регламентных работ и фиксирования отказов средств защиты информации?
	НАВЫКИ	Контрольные вопросы: 1. Какие навыки приобретает техник по защите информации в процессе эксплуатации систем и средств защиты информации защищаемых объектов? 2. Какие регламентные работы проводятся на технических средствах защиты информации? 3. Как влияют регламентные работы и фиксация отказов средств защиты информации на эффективность выявления угроз информационной безопасности?
ПК 3.4.	Знания	Контрольные вопросы: 1. Какие виды, источники и носители защищаемой информации должен знать техник по защите информации при выявлении и анализе возможных угроз информационной безопасности объектов? 2. Какие методы и средства технической защиты информации позволяют выявлять и анализировать возможные угрозы информационной безопасности объектов? 3. Какие программно-аппаратные средства защиты информации

		способны обеспечить выявление возможных угроз информационной безопасности объектов? 4. Знания каких основных правовых актов в области информационной безопасности и защиты информации помогают технику по защите информации выявлять и анализировать возможные угрозы информационной безопасности объектов? 5. Как организовать конфиденциальный документооборот при выявлении и анализе возможных угроз информационной безопасности объектов?
	УМЕНИЯ	Контрольные вопросы: 1. Какие умения должен проявить техник по защите информации, работая с техническими средствами защиты информации в процессе выявления и анализа возможных угроз информационной безопасности объектов? 2. Какова роль выявления возможных угроз информационной безопасности объектов при работе с защищёнными автоматизированными системами? 3. Как можно выявлять и анализировать возможные угрозы информационной безопасности объектов, передавая информацию по защищённым каналам связи? 4. С помощью каких методов техник по защите информации сможет фиксировать отказы в работе средств вычислительной техники, выявляя и анализируя возможные угрозы информационной безопасности объектов?
	НАВЫКИ	Решение практических задач: 1. Продемонстрируйте порядок применения программы фиксации и контроля исходного состояния программного комплекса «Фикс-2.0.1». 2. Объясните принцип работы и порядок применения комплекса СЗИ НСД Secret Net (v. 4.0, для Windows 2000). 3. Перечислите и опишите тактико-технические данные и порядок применения Отбой Б. 4. Можно ли определить возможный канал утечки информации с помощью портативного цифрового рефлектометра «Рейс»? 5. Изложите назначение и порядок применения универсального проверочного устройства проводных линий «Улан».

7.3. Описание показателей и критериев оценивания компетенций на различных этапах их формирования

7.3.1. Контроль и оценка результатов преддипломной практики

Результаты преддипломной практики определяются программами практик, разрабатываемыми ГБПОУ МО «Дмитровский техникум». В результате освоения производственной практики (преддипломной) обучающиеся проходят промежуточную аттестацию в форме дифференцированного зачета. Текущий контроль результатов освоения практики осуществляется руководителем практики от техникума в процессе выполнения обучающимися работ в организациях, а также сдачи обучающимся отчета по практике.

7.3.2. Шкала оценивания

Оценка	Показатели и критерии оценки	
Отлично	Студент имеет глубокие знания, умения, навыки, демонстрирует полное понимание проблемы, все задания выполнены	Образцовый ответ
Хорошо	Студент имеет полные знания, умения, навыки, демонстрирует значительное понимание проблемы, все задания практики выполнены	Законченный, полный ответ с минимальными недочетами
Удовлетворительно	Студент имеет низкий уровень знаний, умений, навыков, демонстрирует частичное понимание проблемы, большинство заданий практики выполнены	Ответ, содержащий недочеты
Неудовлетворительно	Студент имеет пробелы в знаниях, умениях, навыках, демонстрирует непонимание проблемы, задания практики не выполнены	Минимальный ответ

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

- Текущий контроль успеваемости определяется Положением о промежуточной аттестации обучающихся ГБПОУ МО «Дмитровский техникум».

8. ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ПРИ ПРОХОЖДЕНИИ ПРАКТИКИ

8.1. Основная литература.

1. Алексеев, С.В. Правовое регулирование предпринимательской деятельности: учебное пособие / С.В. Алексеев. - М.: Юнити-Дана, 2015. - 502 с.

Рекомендовано УМЦ. http://biblioclub.ru/index.php?page=book&id=114493

2. Басаков М.И. Документационное обеспечение управления (делопроизводство): Учебник для студентов образовательных учреждений среднего профессионального образования. – Ростов н/Д.: Издательство «Феникс», 2013.-350 с.

3. Вычислительные системы, сети и телекоммуникации: учебное пособие. / А.П. Пятибратов, -М.: Издательство «КноРус», 2013.-376 с.: ил.

4. Гребенюк Е.И., Гребенюк Н.А. Технические средства информатизации. Учебник. 8-е изд., стер. –М.: Издательский центр «Академия», 2013.-352 с. – (Серия: «Среднее профессиональное образование»).

5. Ефремов, И. Информационные технологии в сфере безопасности: практикум: И. Ефремов, В. Солопова; Министерство образования и науки Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Оренбургский государственный институт». - Оренбург: ОГУ, 2013. - 116 с.

http://biblioclub.ru/index.php?page=book&id=259178

6. Загинайлов, Ю.Н. Основы информационной безопасности: курс визуальных лекций / Ю.Н. Загинайлов. - М.: Берлин: Директ-Медиа, 2015. - 105 с.: ил. - Библиогр. в кн. http://biblioclub.ru/index.php?page=book&id=362895

7. Карпенков, С.Х. Технические средства информационных технологий: учебное пособие / С.Х. Карпенков. - 3-е изд., испр. и доп. - М.: Берлин: Директ-Медиа, 2015. - 376 с.: ил., табл. - Библиогр. в кн. Допущено МО РФ http://biblioclub.ru/index.php?page=book&id=275367

8. Лапина, М.А. Информационное право: учебное пособие / М.А. Лапина, А.Г. Ревин, В.И. Лапин; под ред. И.Ш. Килясханов. - М.: Юнити-Дана, 2015. - 336 с.

Рекомендовано УМЦ http://biblioclub.ru/index.php?page=book&id=118624

9. Некраха, А.В. Организация конфиденциального делопроизводства и защита информации: учебное пособие / А.В. Некраха, Г.А. Шевцова; Институт информационных наук и технологий безопасности, Российский государственный гуманитарный институт. - М.: Академический проект, 2012. - 222 с.

Рекомендовано УМО. http://biblioclub.ru/index.php?page=book&id=143604

10. Нестеров, С.А. Основы информационной безопасности: учебное пособие /

С.А. Нестеров; Министерство образования и науки Российской Федерации, Санкт-Петербургский государственный политехнический институт. - СПб: Издательство Политехнического института, 2014. - 322 с.: схем, табл., ил. http://biblioclub.ru/index.php?page=book&id=363040

11. Организация безопасной работы информационных систем: учебное пособие / Ю.Ю. Громов, Ю.Ф. Мартемьянов, Ю.К. Букурако и др.; Министерство образования и науки Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Тамбовский государственный технический институт». - Тамбов: Издательство ФГБОУ ВПО «ТГТУ», 2014. - 132 с.: ил. Утверждено УС. http://biblioclub.ru/index.php?page=book&id=277794

12. Персианов, В.В. Электронное офисное делопроизводство: учебник / В.В. Персианов, Е.З. Киреева, М.Н. Казакова. - М.: Берлин: Директ-Медиа, 2016. - 326 с.: ил. Рекомендовано УМЦ http://biblioclub.ru/index.php?page=book&id=434743

13. Попович, Е. Документационное обеспечение управления персоналом: учебное пособие / Е. Попович; Министерство образования и науки Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Оренбургский государственный институт». - Оренбург: ОГУ, 2014. - 112 с. http://biblioclub.ru/index.php?page=book&id=259328

14. Пятибратов, А.П. Вычислительные системы, сети и телекоммуникации: учебник / А.П. Пятибратов, Л.П. Гудыно, А.А. Кириченко. - 4-е изд., перераб. и доп. - М.: Финансы и статистика, 2013. - 736 с. Рекомендовано МО РФ http://biblioclub.ru/index.php?page=book&id=220195

15. Рогожин, М.Ю. Документационное обеспечение управления: учебно-практическое пособие / М.Ю. Рогожин. - М.: Берлин: Директ-Медиа, 2014. - 384 с. http://biblioclub.ru/index.php?page=book&id=253704

16. Румынина В.В. Правовое обеспечение профессиональной деятельности: Учебник. 9-е изд. стер., - М.: Издательский центр «Академия, 2013.-224 с. 17.

Фомин, Д.В. Компьютерные сети: учебно-методическое пособие по выполнению расчетно-графической работы: учебно-методическое пособие / Д.В. Фомин. - М.: Берлин: Директ-Медиа, 2015. - 66 с.: ил. http://biblioclub.ru/index.php?page=book&id=349050

18. Шаньгин П.П. Информационная безопасность компьютерных систем и сетей: Учебное пособие. – М.: Издательство «Форум», 2013.-416 с. Рекомендовано МО РФ.

8.2. Дополнительная литература

1. Бабаш, А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, 2013. - 136 с.

2. Ефимова, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга. - М.: ЮНИТИ-ДАНА, 2013. - 239 с.

3. Партыка, Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка,
И.И. Попов. - М.: Форум, 2012. - 432 с.

4. Петров, С.В. Информационная безопасность: Учебное пособие / С.В. Петров,
И.П. Слинькова, В.В. Гафнер. - М.: АРТА, 2012. - 296 с.

5. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей:
Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2013. - 416 с.

8.3. Нормативно-правовые документы:

1. Федеральный закон Российской Федерации от 06 апреля 2011 года № 63- ФЗ «Об электронной подписи».
2. Федеральный закон Российской Федерации от 27 июля 2006 года № 149- ФЗ «Об информации, информационных технологиях и о защите информации».
3. Федеральный закон РФ от 04 мая 2011 года № 99-ФЗ «О лицензировании отдельных видов деятельности».
4. Федеральный закон Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных».
5. Федеральный закон Российской Федерации от 21 июля 1993 года № 5485-1 «О государственной тайне».

9. ПЕРЕЧЕНЬ ИНТЕРНЕТ-РЕСУРСОВ, НЕОБХОДИМЫХ ДЛЯ ПРОВЕДЕНИЯ ПРАКТИКИ

1. Официальный сайт ФСТЭК: http://fstec.ru/;
2. Официальный сайт ФСБ: http://www.fsb.ru/;
3. Портал «Центр информационной безопасности»: http://www.bezpeka.com/;
4. Журнал «Информационная безопасность»: http://www.itsec.ru/main.php
5. Электронный портал: http://www.securitylab.ru/

10. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ПРОВЕДЕНИИ ПРАКТИКИ, ВКЛЮЧАЯ ПЕРЕЧЕНЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННО-СПРАВОЧНЫХ СИСТЕМ (ПРИ НЕОБХОДИМОСТИ)

10.1. Перечень информационных технологий, используемых при проведении данной практики:

- технологии электронного обучения:

1. Электронно-библиотечная система «КнигаФонд»
2. Электронно-библиотечная система «BOOK.ru»
3. Научная электронная библиотека eLibrary.ru
4. Федеральная корпоративная электронная библиотека
5. Электронная библиотека системы дистанционного обучения «Прометей»
6. Электронный каталог библиотеки БУКЭП
7. Государственная публичная научно-техническая библиотека России
8. Ассоциация региональных библиотечных консорциумов
10. Институтская информационная система «РОССИЯ»
11. Проект «Полпред»
12. Федеральный портал «Российское образование»
13. Информационная система «Единое окно доступа к образовательным ресурсам»
14. Единая коллекция цифровых образовательных ресурсов
15. Федеральный центр информационно-образовательных ресурсов
16. ACM Digital Library - поисковые системы интернет:

1. yandex.ru – самая популярная поисковая система в России. Имеется расширенный поиск;
2. rambler.ru – одна из популярных русскоязычных поисковых систем;
3. google.ru – одна из популярных систем в России. И по всему миру (google.com);

- электронные образовательные услуги:

1. Официальный сайт Министерства образования и науки Российской Федерации – http://www.mon.gov.ru
2. Федеральный портал «Российское образование» – http://www.edu.ru
3. Информационная система «Единое окно доступа к образовательным ресурсам» – http://window.edu.ru
4. Единая коллекция цифровых образовательных ресурсов – http://school-collection.edu.ru
5. Федеральный центр информационно-образовательных ресурсов – http://fcior.edu.ru. 10.2.
6. Программное обеспечение: А) общее ПО:

пакет программ Microsoft Office 2010, Microsoft Visual Studio 2010, Microsoft SQL Server 2008, WinRar, Антивирус Касперского, Autocad, BPwin, Mathcad Б) специальное ПО:

- Комплекс СЗИ НСД «Аккорд NT/2000» v.2.0 (для ОС Windows NT/2000/XP, PCI);
- АПМДЗ «КРИПТОН-ЗАМОК» (комплекс аппаратно-программных средств, Windows NT 4.0 и Windows 2000/XP/2003;
- Комплекс СЗИ НСД Secret Net (v. 4.0, для Windows 2000;
- «Ревизор-1 XP» (средство создания модели системы разграничения доступа);
- «Ревизор-2 XP» (программа контроля полномочий доступа к информационным ресурсам);
- «Фикс-2.0.1» (программа фиксации и контроля исходного состояния программного комплекса);
- «Фикс-3.0.1» (Программа контроля состояния сертифицированных программных средств защиты информации);
- «НКВД-2.4» (анализатор механизма очистки внешней памяти);
- «НКВД-2.5» (анализатор механизма очистки оперативной памяти);

- Strong Disk Pro - Standard (комплекс для защиты конфиденциальной информации на ПК, ноутбуках и сменных носителях от НСД);
- Secret Disk Server Generation (комплекс для защиты конфиденциальной информации для ПК, 1-5 пользователе);
- Secret Net v. 5.0-C для Windows 2000/2003/XP (комплекс СЗИ НСД);
- «Terrier 3.0» (программа поиска и гарантированного уничтожения информации на дисках);
- «Secret Disk NG» (система защиты конфиденциальной информации);
- «НКВД-2.3» (средство автоматизированного моделирования СРД АРМ для Windows 9x/NT/2000/XP, серт. ФСТЭК России).

10.3. Информационно-справочные системы
ИППС КонсультантПлюс

11. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ПРОВЕДЕНИЯ ПРАКТИКИ

- производственная, методическая и справочная литература;
- персональные компьютеры с доступом к сети Интернет;
- персональные компьютеры с прикладным программным обеспечением; - информационно-справочные системы «Консультант Плюс».