Министерство науки и высшего образования Российской Федерации
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Российский экономический университет имени Г.В. Плеханова»
МОСКОВСКИЙ ПРИБОРОСТРОИТЕЛЬНЫЙ ТЕХНИКУМ

РАБОЧАЯ ПРОГРАММА

Производственная ПП.03.01 Применение инженерно-технических средств обеспечения информационной безопасности

Профессиональный ПМ.03 Применение инженерно-технических средств обеспечения информационной безопасности

код, специальность 10.02.03 Информационная безопасность автоматизированных систем

Москва 2017

СОГЛАСОВАНА:
Цикловой методической комиссией «Профессиональных модулей 10.02.03»

Протокол № **1-17/18-ЗК**
от «31»__08__2017года
Председатель цикловой методической комиссии

_____
М.С. Прищеп

Разработана в соответствии с требованиями Федерального государственного образовательного стандарта по специальности среднего профессионального образования **10.02.03 Информационная безопасность автоматизированных систем**

Заместитель директора по учебной работе _____ Д.А. Клопов

Заместитель директора по производственному обучению _____ Е.А. Ермашенко
подпись

УТВЕРЖДЕНА:
Директор техникума _____ А.В. Чурилов
подпись

Составители (авторы):

Прищеп Михаил Сергеевич, преподаватель ФГБОУ ВО «РЭУ им. Г.В.Плеханова»

СОГЛАСОВАНО:
с работодателем:

Ведущий инженер ООО «ПК Аквариус» _____ И.В. Сотников
Подпись Инициалы Фамилия

Лист актуализации

рабочей программы производственной практики

В рабочую программу производственной практики на 2018/19 уч. год внесены следующие изменения:

1. На основании Указа Президента РФ от 15.01.2018 года №215 на титульном листе исправлено Министерство образования и науки Российской Федерации на Министерство науки и высшего образования Российской Федерации

Дата актуализации: 30.08.2018 г

СОДЕРЖАНИЕ

1 . ПАСПОРТ ПРОГРАММЫ ПРАКТИКИ ПО ПРОФЕССИОНАЛЬНОМУ МОДУЛЮ

ПМ.03 Применение инженерно-технических средств обеспечения информационной безопасности

ПП.03.01 Применение инженерно-технических средств обеспечения информационной безопасности

1.1. Область применения программы практики

Программа практики является составной частью Программы подготовки специалистов среднего звена, обеспечивающей реализацию ФГОС СПО.

Практика является частью учебного процесса и направлена на формирование у студентов практических профессиональных умений, приобретение первоначального практического опыта по основным видам профессиональной деятельности для последующего освоения ими общих и профессиональных компетенций по избранной специальности:

- ***Общие компетенции:***

ОК 1. Понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности.

ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.

ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.

ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.

ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.

ОК 6. Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.

ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.

ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.

ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

ОК 10. Формулировать задачи логического характера и применять средства математической логики для их решения.

ОК 11. Владеть основными методами и средствами разработки программного обеспечения.

ОК 12. Производить инсталляцию и настройку автоматизированных информационных систем, выполнять в автоматизированных информационных системах регламентные работы по обновлению, техническому сопровождению и восстановлению при отказах.

- ***Профессиональные компетенции:***

ПК 3.1. Применять инженерно-технические средства обеспечения информационной безопасности.

ПК 3.2. Участвовать в эксплуатации инженерно-технических средств обеспечения информационной безопасности, в проверке их технического состояния, в проведении технического обслуживания и текущего ремонта, устранении отказов и восстановлении работоспособности.

ПК 3.3. Участвовать в мониторинге эффективности применяемых инженерно-технических средств обеспечения информационной безопасности.

ПК 3.4. Решать частные технические задачи, возникающие при проведении всех видов плановых и внеплановых контрольных проверок, при аттестации объектов, помещений, технических средств.

ПК 3.5. Применять нормативные правовые акты, нормативно-методические документы по обеспечению информационной безопасности инженерно-техническими средствами.

1.2. Цели и задачи практики – требования к результатам освоения практики, формы отчетности

В ходе освоения программы практики студент должен:

иметь практический опыт:

- выявление технических каналов утечки информации;
- использование основных методов и средств инженерно-технической защиты информации;
- диагностики, устранение отказов и восстановления работоспособности инженерно-технических средств обеспечения информационной безопасности;
- участия в мониторинге эффективности инженерно-технических средств

обеспечения информационной безопасности;

- решения частных технических задач, возникающих при аттестации объектов, помещений, технических средств;

уметь:

- применять технические средства защиты информации;
- использовать средства охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения;
- использовать средства защиты информации от несанкционированного съёма и утечки по техническим каналам;
- применять нормативные правовые акты, нормативные методические документы по обеспечению информационной безопасности техническими средствами;

знать:

- физику возникновения технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации;
- номенклатуру и характеристики аппаратуры, используемой для съема, перехвата и анализов сигналов в технических каналах утечки информации;
- основные методы и средства технической защиты информации, номенклатуру применяемых средств защиты информации от несанкционированного съёма и утечки по техническим каналам;
- номенклатуру применяемых средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения

По окончании практики студент сдаёт отчет в соответствии с содержанием тематического плана практики и по форме, установленной в МПТ ФГБОУ ВО «РЭУ им. Г.В. Плеханова».

Итоговая аттестация проводится в форме - **дифференцированного зачёта.**

1.3. Количество часов на освоение программы практики

Рабочая программа практики рассчитана на прохождение студентами практики в объеме **108** часов.

2. РЕЗУЛЬТАТЫ ПРАКТИКИ

Код формируемой компетенции	Наименование компетенции
1	**2**
ПК 3.1.	Применять инженерно-технические средства обеспечения информационной безопасности.
ПК 3.2	Участвовать в эксплуатации инженерно-технических средств обеспечения информационной безопасности, в проверке их технического состояния, в проведении технического обслуживания и текущего ремонта, устранении отказов и восстановлении работоспособности.
ПК 3.3	Участвовать в мониторинге эффективности применяемых инженерно-технических средств обеспечения информационной безопасности.
ПК 3.4	Решать частные технические задачи, возникающие при проведении всех видов плановых и внеплановых контрольных проверок, при аттестации объектов, помещений, технических средств.
ПК 3.5	Применять нормативные правовые акты, нормативно-методические документы по обеспечению информационной безопасности инженерно-техническими средствами.

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИКИ

3.1 Тематический план практики

Наименование профессионального модуля	Коды формируемых компетенций	Объем времени, отводимый на практику	Сроки проведения практики
1	**2**	**3**	**4**
Применение инженерно-технических средств обеспечения информационной безопасности	ПК 3.1.	***3 недели – 108 часов***	***8 семестр***
	ПК 3.2		
	ПК 3.3		
	ПК 3.4		
	ПК 3.5		

3.2. Содержание практики

Наименование разделов и тем	Содержание освоенной учебной информации, виды работ, выносимые на практику в соответствии с рабочими программам профессиональных модулей	Объем часов	Уровень освоения	Коды профессиональных компетенций
1	2	3	4	5
Раздел 1. Организационно-подготовительный этап прохождения практики на предприятии		**10**	**4**	
Тема 1.1. Инструктаж по прохождению производственной практики и правилам безопасности работы на предприятии.	***Содержание выполняемых работ***			
	Знакомство с общими функциональными обязанностями, правилами техники безопасности на предприятии, на конкретном рабочем месте, при работе с электрическими приборами (устройствами)	**10**		**ПК 3.1-3.6**
Раздел 2. Ознакомление со структурой и характером деятельности подразделения		**10**	**4**	
Тема 2.1. Ознакомление с организацией работы на предприятии или в структурном подразделении	***Содержание выполняемых работ***			
	Знакомство с режимом работы, формой организации труда и правилами внутреннего распорядка, структурными подразделениями предприятия, штатным расписанием; с принципами управления, руководства и осуществления должностных обязанностей	**5**		**ПК 3.1-3.6**
Тема 2.2. Ознакомление с должностными и функциональными обязанностями	***Содержание выполняемых работ***			
	Изучение прав и обязанностей сотрудника, должностной инструкции, регламентирующей его деятельность; знакомство с правами и обязанностями других сотрудников и руководителей; согласование с руководителем практики задание, постановку целей и задач практики	**5**		**ПК 3.1-3.6**

Раздел 3. Работа на рабочих местах или в подразделениях предприятия		**88**	**4**	
Тема 3.1. Ознакомление: с организацией информационного обеспечения подразделения; с процессом защиты на уровне проектирования и эксплуатации информационных средств; с методами планирования и проведения мероприятий по созданию (разработке) проекта (подсистемы) информационной среды предприятия для решения конкретной задачи.	***Содержание выполняемых работ***	**10**		
	Ознакомление с производственными характеристиками и показателями деятельности предприятия. Изучение новых технологических средств в современных информационных системах, применяемых на предприятии. Изучение основных проектных решений по информационным системам на предприятии (в организации).Ознакомление с методологией проектирования, внедрения и эксплуатации актуальных информационных систем. Изучение технологии сбора, регистрации и обработки информации на данном предприятии. Проектирование подсистем защиты. Обеспечения защиты информации от несанкционированного доступа			**ПК 3.1-3.6**
Тема 3.2. Изучение структурных и функциональных схем предприятия, организации деятельности подразделения; порядка и методов ведения делопроизводства; требований к техническим, программным средствам, средствам защиты информации используемым на предприятии.	***Содержание выполняемых работ***	**10**		
	Изучение основ финансов, организации денежного обращения и кредитования предприятия, приобретение навыков использования финансово-кредитного механизма с целью повышения эффективности работы предприятия и составления финансового плана. Изучение схем защиты денежных транзакций через сеть интернет Изучение организации расчета заработной платы на предприятии, приобретение навыков проектирования трудовых процессов с учетом комплекса технических, экономических, психофизиологических и социальных факторов, оценка затрат и результатов труда.			**ПК 3.1-3.6**

Тема 3.3. Выполнение производственных заданий	***Содержание выполняемых работ***	**58**		
	Приобретение практических навыков работы на конкретных рабочих местах. Выявление технических каналов утечки информации; использование основных методов и средств инженерно-технической защиты информации; диагностики, устранение отказов и восстановления работоспособности инженерно-технических средств обеспечения информационной безопасности; участия в мониторинге эффективности инженерно-технических средств обеспечения информационной безопасности; решение частных технических задач, возникающих при аттестации объектов, помещений, технических средств;			**ПК 3.1-3.6**
Тема 3.4. Сбор и анализ материалов для оформления отчетной документации по практике.	***Содержание выполняемых работ***	**10**		
	Сбор материалов для отчета, подготовка отчетной документации по практике			**ПК 3.1-3.6**
Итоговая аттестация	Сдача отчета в соответствии с содержанием тематического плана практики и по форме, установленной в МПТ ФГБОУ ВО «РЭУ им. Г.В. Плеханова».			
Всего		**108**		

Для характеристики уровня освоения учебного материала используются следующие обозначения:
1. – ознакомительный (узнавание ранее изученных объектов, свойств);
2. – репродуктивный (выполнение деятельности по образцу, инструкции или под руководством)
3. – продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач)

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРАКТИКИ

4.1 Требования к документации, необходимой для проведения практики.

Для проведения практики в учебном заведении разработана следующая документация:

- рабочая программа практики;
- календарно-тематический план;
- приказ о назначении руководителя практики от образовательного учреждения
- договоры с предприятиями по проведению практики;
- приказ о распределении студентов по базам практики;
- план-график консультаций и контроля за выполнением студентами программы практики (при проведении практики на предприятии);
- график защиты отчетов по практике.

4.2 Требования к учебно-методическому обеспечению практики.

В целях реализации требований к учебно-методическому обеспечению практики разработаны и утверждены:

- Задания на практику;
- Методические рекомендации для студентов по выполнению видов работ на практике;
- Методические рекомендации по формированию отчетов по практике;
- Методические рекомендации по оформлению дневника по практике;
- Критерии оценки прохождения практики и защиты отчетов.

4.3. Требования к материально-техническому обеспечению практики

1. *Индивидуальное задание / Практические работы/лабораторные работы:*
2. *Компьютерный класс, оснащенный презентационной техникой (проектор, экран, компьютер/ноутбук, ...), пакетами ПО общего назначения (текстовые редакторы, графические редакторы, ...), специализированным ПО: ..., выходом в Интернет с доступом к электронным базам данных и т.п.;*

Лекции / экскурсии:

1. *Комплект электронных презентаций/слайдов;*
2. *Аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук, ...) и соответствующим программным обеспечением (ПО) и т.п.;*

4.4. Информационное обеспечение обучения.

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1. Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс] : Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013 (http://znanium.com/catalog.php?bookinfo=405000)
2. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: ИНФРА-М, 2012. - 416 с. (http://znanium.com/catalog.php?bookinfo=335362)

Дополнительные источники:

1. В.И. Грекул, Г.Н. Денищенко, Н.Л. Коровкина Проектирование информационных систем: учебное пособие – М.: Интернет-Университет Информационных Технологий; БИНОМ. Лаборатория знаний, 2008. – 300 с.
2. А.И. Болдырев, И.В. Василевский, С.Е. Сталенков Методические рекомендации по поиску и нейтрализации средств негласного съема информации: практическое пособие – М.: 2001 г.
3. В.А. Галатенко Основы информационной безопасности. Курс лекций. Учебное пособие – М.: Интернет-университет информационных технологий, 2004 г.
4. В.И. Ярочкин Информационная безопасность. Учебник – М.: Академический проект, 2004 г.
5. Д. Скляров Искусство защиты и взлома информации – СПб.: БХВ-Петербург, 2004 г.
6. А. Торокин Инженерно-техническая защита информации: учебное пособие для студентов – М.: Гелиос-АРВ, 2005 г.

4.5 ТРЕБОВАНИЯ К РУКОВОДИТЕЛЮ ПРАКТИКИ

Руководителем практики от техникума назначается педагогический работник, имеющий высшее образование, соответствующее профилю проводимой практики

4.5.1 Руководитель практики от образовательного учреждения:

1. разрабатывает тематику заданий для студентов;
2. проводит консультации со студентами перед направлением их на практику с разъяснением целей, задач и содержания практики;
3. принимает участие в распределении студентов по рабочим местам или перемещении их по видам работ;
4. осуществляет контроль правильного распределения студентов в период практики; формирует группы в случае применения групповых форм проведения практики;
5. проводит индивидуальные и групповые консультации в ходе практики;
6. оказывает методическую помощь студентам при выполнении ими заданий и сборе материалов к отчету по практике;
7. контролирует выполнение требований охраны труда, безопасности жизнедеятельности и пожарной безопасности;

4.5.2 Руководитель практики от организации:

1. согласовывает программу практики, планируемые результаты практики, задание на практику;
2. участвует в организации и проведении зачета по практике и экзамена квалификационного по профессиональному модулю;
3. участвуют в организации и оценке результатов освоения общих и профессиональных компетенций, освоенных студентами в период прохождения практики;
4. проводит инструктаж студентов по ознакомлению с требованиями охраны труда, безопасности жизнедеятельности и пожарной безопасности

4.6 Требования к соблюдению техники безопасности и пожарной безопасности

Регламентация требований по пожарной безопасности и техники безопасности осуществляется внутренними локальными актами техникума

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРАКТИКИ ПО ПРОФЕССИОНАЛЬНОМУ МОДУЛЮ

По результатам усвоения программы практики студенты представляют руководителю практики от техникума отчет, дневник и отзыв на студента-практиканта от руководителя базы практики.

По окончании практики студент защищает дневник, отчет с дифференцированной оценкой в присутствии комиссии, назначаемой заместителем директора по производственному обучению. Комиссия по защите дневников и отчетов должна состоять не менее чем из двух членов. В зависимости от места защиты дневника, отчета в состав комиссии входят: руководитель практики от техникума, руководитель практики от базы практики, председатель ЦМК спецдисциплин и профессиональных модулей. Руководитель практики от техникума входит в состав комиссии и при защите отчетов в организации. Защита дневников и отчетов проводится в организации или в техникуме (если группа размещена по разным объектам практики). На базах практики защита должна проводиться в последний день практики. В техникуме председателем комиссии по защите дневников и отчетов по практике является заместитель директора по производственному обучению.

При оценке итогов работы студента на практике учитываются содержание и правильность оформления студентом дневника и отчета по практике, отзывы руководителей практики от организации, качество ответов на вопросы в ходе защиты отчета.

Зарегистрированные и защищенные дневники, отчеты хранятся в техникуме в течение трех лет в соответствии с номенклатурой дел.

Аттестация студента по итогам прохождения практики проводится только после сдачи документов по практике и фактической защиты отчета.

Зачет по результатам практики принимает комиссия, назначенная заведующим практикой и состоящая из преподавателей-руководителей практики. Защита отчета по практике, как правило, представляет собой краткий, 8-10-минутный доклад студента и его ответы на вопросы членов комиссии.

После защиты отчета руководитель практики от техникума дает свое заключение о заполнении дневника, отчета, выполнении программы практики и ставит по итогам дифференцированную оценку по пятибалльной шкале (5 «отлично», 4 «хорошо», 3 «удовлетворительно», 2 «неудовлетворительно»). Оценка одновременно проставляется в ведомость, зачетную книжку студента и «Дневник студента по производственной практике».

Результаты (освоенные профессиональные компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ПК 3.1. Применять инженерно-технические средства обеспечения информационной безопасности.		
В результате освоения данной компетенции студент должен: **иметь практический опыт:** – выявления технических каналов утечки информации; **уметь:** – применять технические средства защиты информации; – использовать средства охраны и безопасности, инженерной защиты и	– определение и нормализация отношений между объектами – выбор архитектуры и типового клиента доступа в соответствии с технологией разработки – демонстрация нормализации и установки отношений между объектами данных	Экспертная оценка результатов деятельности – обучающегося Экспертная оценка результатов деятельности – обучающегося

Результаты (освоенные профессиональные компетенции)	Основные показатели оценки результата	Формы и методы контроля и оценки
технической охраны объектов, систем видеонаблюдения; **знать:** – физику возникновения технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информа-ции;	– изложение правил установки отношений между объектами баз данных – выбор методов описания и построения схем баз данных – изложение основных принципов проектирования баз данных	Экспертная оценка результатов деятельности – обучающегося
ПК 3.2. Участвовать в эксплуатации инженерно-технических средств обеспечения информационной безопасности, в проверке их технического состояния, в проведении технического обслуживания и текущего ремонта, устранении отказов и восстановлении работоспособности.		
В результате освоения данной компетенции студент должен: **иметь практический опыт:** – использования основных методов и средств инженерно-технической защиты информации;	– демонстрация построения концептуальной, логической и физической моделей данных с помощью утилиты автоматизированного проектирования базы данных – выбор и использование утилит автоматизированного проектирования баз данных – демонстрация навыков разработки и модификации серверной и клиентской части базы данных в инструментальной оболочке	Экспертная оценка результатов деятельности – обучающегося
уметь: – использовать средства защиты информации от несанкционированного съёма и утечки по техниче-ским каналам; – применять нормативные – нормативные методические документы по обеспечению информационной безопасности техническими средствами; – пользоваться контрольно-испытательной и измерительной аппаратурой;	– демонстрация методов манипулирования данными – выбор типа запроса к СУБД – демонстрация построения запроса к СУБД – демонстрация навыков построения запросов SQL к базе данных; – демонстрация навыков изменения базы данных (в соответствии с ситуацией)	Экспертная оценка результатов деятельности – обучающегося
знать:		

Результаты (освоенные профессиональные компетенции)	Основные показатели оценки результата	Формы и методы контроля и оценки
– номенклатуру и характеристики аппаратуры, используемой для съема, перехвата и анализа сигналов в технических каналах утечки информации;	– выбор технологии разработки базы данных исходя из её назначения – изложение основных принципов проектирования баз данных	Экспертная оценка результатов деятельности – обучающегося
ПК 3.3. Участвовать в мониторинге эффективности применяемых инженерно-технических средств обеспечения информационной безопасности.		
В результате освоения данной компетенции студент должен: **иметь практический опыт:** – диагностики, устранения отказов и восстановления работоспособности инженерно-технических средств обеспечения информационной безопасности;	– выбор технологии разработки базы данных, исходя из требований к её администрированию – демонстрация навыков разработки и модификации серверной и клиентской части базы данных в инструментальной оболочке с возможностью её администрирования	Экспертная оценка результатов деятельности – обучающегося
уметь: – составлять измерительные схемы; – подбирать по справочным материалам измерительные средства;	– выбор сетевой технологии и, исходя из неё, методов доступа к базе данных – демонстрация навыков построения запросов SQL к базе данных с учётом распределения прав доступа – демонстрация навыков изменения прав доступа в базе данных (в соответствии с ситуацией); – демонстрация навыков правильного использования программных средств защиты	Экспертная оценка результатов деятельности – обучающегося
знать: – номенклатуру применяемых средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения;номенклатуру применяемых средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения;	– определение вида и архитектуры сети, в которой находится база данных – определение модели информационной системы	Экспертная оценка результатов деятельности – обучающегося
ПК 3.4. Решать частные технические задачи, возникающие при проведении всех видов плановых и внеплановых контрольных проверок, при аттестации объектов, помещений, технических средств.		

Результаты (освоенные профессиональные компетенции)	Основные показатели оценки результата	Формы и методы контроля и оценки
В результате освоения данной компетенции студент должен: **иметь практический опыт:** – участия в мониторинге эффективности инженерно-технических средств обеспечения информационной безопасности; **уметь:** – измерять с заданной точностью физические величины;	– демонстрация навыков правильного использования программных средств защиты – демонстрация навыков внесения изменения в базу данных для защиты информации – выбор сетевой технологии и, исходя из неё, методов доступа к базе данных – выбор и настройка протоколов разных уровней для передачи данных по сети – демонстрация устранения ошибок межсетевого взаимодействия в сетях – демонстрация использования сетевых устройств для защиты данных базы данных при передаче по сети	Экспертная оценка результатов деятельности – обучающегося Экспертная оценка результатов деятельности – обучающегося
знать: – способы контроля доступа к данным и управления привилегиями – основные методы и средства защиты данных в базах данных – модели и структуры информационных систем – основные типы сетевых топологий, приемы работы в компьютерных сетях – информационные ресурсы компьютерных сетей – технологии передачи и обмена данными в компьютерных сетях – основы разработки приложений баз данных	– выбор архитектуры и типового клиента доступа в соответствии с технологией разработки базы данных – изложение основных принципов проектирования баз данных – изложение построения концептуальной, логической и физической моделей данных	Экспертная оценка результатов деятельности – обучающегося
ПК 3.5. Применять нормативные правовые акты, нормативно-методические документы по обеспечению информационной безопасности инженерно-техническими средствами.		
В результате освоения данной компетенции студент должен: **иметь практический опыт:** – решения частных технических задач, возникающих при аттестации объектов, помещений,		

Результаты (освоенные профессиональные компетенции)	Основные показатели оценки результата	Формы и методы контроля и оценки
технических		