МИНОБРНАУКИ РОССИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Национальный исследовательский университет
«Московский институт электронной техники»

УТВЕРЖДАЮ
Проректор по учебной работе
_____ И.Г.Игнатова
«23» марта 2021 г.

РАБОЧАЯ ПРОГРАММА ПРАКТИКИ

Вид практики: производственная
Тип практики – эксплуатационная практика

Направление подготовки – 10.04.01 «Информационная безопасность»
Направленность (профиль) – «Аудит информационной безопасности»

2021

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ

Практика участвует в формировании следующих компетенций/подкомпетенций:

Компетенция ПК-1 «Способен проводить аттестацию автоматизированных систем, средств обработки информации на соответствие требованиям безопасности информации» сформулирована на основе профессионального стандарта «Специалист по технической защите информации», утверждённый приказом Минтруда России от 01.11.2016 № 599н. Регистрационный № 844.

Обобщенная трудовая функция G/7. Проведение аттестации объектов на соответствие требованиям по защите информации.

Трудовая функция G/01.7. Проведение аттестации объектов вычислительной техники на соответствие требованиям по защите информации.

ОПК	**Подкомпетенции, формируемые на практике**	**Индикаторы достижения подкомпетенций**
ПК-1. Способен проводить аттестацию автоматизированных систем, средств обработки информации на соответствие требованиям безопасности информации	ПК-1. ПрПрк. Способен проводить аттестацию автоматизированных систем, средств обработки информации на соответствие требованиям безопасности информации	**Знания** нормативные документы ФСТЭК России по контролю эффективности защиты информации от утечки по техническим каналам, организации аттестации объектов информатизации; методы и средства контроля эффективности защиты выделенных помещений от утечки речевой информации по техническим каналам; методики аттестационных испытаний объектов СВТ по оценке защищенности информации от утечки по техническим каналам; организацию аттестации объектов информатизации по требованиям безопасности информации. **Умения:** разрабатывать программы и методики аттестационных испытаний объектов информатизации по требования безопасности информации; проводить контроль выполнения норм защищенности СВТ от утечки информации по техническим каналам;

ОПК	Подкомпетенции, формируемые на практике	Индикаторы достижения подкомпетенций
		рассчитывать показатели защищенности СВТ от утечки информации по техническим каналам; оформлять протоколы и заключения по результатам аттестационных испытаний объектов информатизации по требованиям безопасности информации. **Опыт практической деятельности:** разработки программы и методики аттестационных испытаний объектов информатизации по требования безопасности информации; проведения аттестационных испытаний объектов информатизации по оценке защищенности информации от утечки по техническим каналам; оформления протоколов и заключения по результатам аттестационных испытаний объектов информатизации по требованиям безопасности информации.

Компетенция ПК-2 «Способен проводить аттестацию выделенных (защищаемых) помещений на соответствие требованиям безопасности информации» сформулирована на основе профессионального стандарта «Специалист по технической защите информации», утверждённый приказом Минтруда России от 01.11.2016 № 599н. Регистрационный № 844.

Обобщенная трудовая функция G/7. Проведение аттестации объектов на соответствие требованиям по защите информации.

Трудовая функция G/02.7. Проведение аттестации выделенных (защищаемых) помещений на соответствие требованиям по защите информации.

Компетенции	Подкомпетенции, формируемые в дисциплине	Индикаторы достижения подкомпетенций
ПК-2. Способен проводить	ПК-2. ПрПрк. Способен проводить аттестацию	**Знания:** нормативные документы ФСТЭК

Компетенции	Подкомпетенции, формируемые в дисциплине	Индикаторы достижения подкомпетенций
аттестацию выделенных (защищаемых) помещений на соответствие требованиям безопасности информации	выделенных (защищаемых) помещений на соответствие требованиям безопасности информации	России по контролю эффективности защиты информации от утечки по техническим каналам, организации аттестации объектов информатизации; методы и средства контроля эффективности защиты выделенных помещений от утечки речевой информации по техническим каналам; методики аттестационных испытаний выделенных помещений по оценке защищенности информации от утечки по техническим каналам; организацию аттестации выделенных помещений по требованиям безопасности информации. **Умения:** разрабатывать программы и методики аттестационных испытаний выделенных помещений по требования безопасности информации; проводить контроль выполнения норм защищенности СВТ от утечки информации по техническим каналам; рассчитывать показатели защищенности СВТ от утечки информации по техническим каналам; проводить контроль выполнения норм защищенности речевой информации от утечки по техническим каналам; рассчитывать показатели защищенности речевой информации от утечки по техническим каналам; проводить специальную техническую проверку

Компетенции	Подкомпетенции, формируемые в дисциплине	Индикаторы достижения подкомпетенций
		выделенного помещения с целью выявления электронных устройств перехвата речевой информации; оформлять протоколы и заключения по результатам аттестационных испытаний объектов информатизации (выделенных помещений) по требованиям безопасности информации. **Иметь практический опыт:** разработки программы и методики аттестационных испытаний объектов информатизации по требования безопасности информации; проведения аттестационных испытаний выделенных помещений на соответствие требованиям безопасности информации; оформления протоколов и заключения по результатам аттестационных испытаний выделенных помещений по требованиям безопасности информации.

Компетенция ПК-3 «Способен проводить аудит информационной безопасности» сформулирована на основе проекта новой редакции профессионального стандарта 064.033 «Специалист по защите информации в автоматизированных системах», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 15 сентября 2016 г. № 522н (зарегистрирован Министерством юстиции Российской Федерации 28 сентября 2016 г., регистрационный № 43857).

Обобщенная трудовая функция D/7. Аудит информационной безопасности автоматизированной системы.

Трудовая функция D/01.7. Подготовка к проведению аудита информационной безопасности автоматизированной системы.

Трудовая функция D/02.7. Проведение аудита информационной безопасности автоматизированной системы.

Компетенции	Подкомпетенции, формируемые в дисциплине	Индикаторы достижения подкомпетенций

Компетенции	Подкомпетенции, формируемые в дисциплине	Индикаторы достижения подкомпетенций
ПК-3. Способен проводить аудит информационной безопасности	ПК-3.ПрПрк. Способен проводить аудит информационной безопасности автоматизированных систем	**Знания** порядок разработки и содержание технического задания на проведение аудита информационной безопасности автоматизированной системы (АС); структуру и порядок подготовки конкурсной документации на проведение аудита информационной безопасности АС; требования к содержанию программы и методики аудита информационной безопасности АС. порядок и методики проведения аудита информационной безопасности АС; состав и требования к содержанию документов, оформляемых по результатам аудита информационной безопасности АС. **Умения:** проводить предварительное обследование объекта информатизации; разрабатывать техническое задание на проведение аудита информационной безопасности АС; разрабатывать конкурсную документацию на проведение аудита информационной безопасности АС; разрабатывать программу и методики аудита информационной безопасности АС. проводить аудит информационной безопасности АС в соответствие с

Компетенции	Подкомпетенции, формируемые в дисциплине	Индикаторы достижения подкомпетенций
		разработанными методиками; состав и требования к содержанию документов, оформляемых по результатам аудита информационной безопасности АС. **Опыт практической деятельности:** проведения аудита информационной безопасности АС.

2. МЕСТО ПРАКТИКИ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Производственная практика – эксплуатационная практика входит в часть, формируемую участниками образовательных отношений Блока 2 «Практика» образовательной программы.

Производственная практика представляет собой вид учебных занятий, непосредственно ориентированных на профессионально-практическую подготовку обучающихся. Практика проводится во 2-м семестре 1 курса и в 3-м семестре 2 курса.

Прохождение практики базируется на знаниях и умениях, полученных при изучении дисциплин: «Технологии защиты информации от несанкционированного доступа», «Технологии защиты информации от утечки по техническим каналам», «Контроль защищённости информации от утечки по техническим каналам», «Организация аудита информационной безопасности».

Знания и умения, полученные в результате прохождения практики, используются при подготовке ВКР и в практической деятельности.

Способ проведения практики: стационарная. Практика проходит в подразделениях НИУ МИЭТ, а также в подразделениях организаций и предприятий, осуществляющих деятельность в области защиты информации и обеспечении информационной безопасности.

3. ОБЪЁМ ПРАКТИКИ

Объём практики – 21 ЗЕТ (756 ак. часов). Из них: 9 ЗЕТ (324 ч.) – во 2-м семестре; 12 ЗЕТ (432 ч.) – в 3-м семестре.

Практика организуется в 2-м семестре в период с 1 по 16 неделю (по 20 -21 часов в неделю), в 3 семестре, в период с 1 по 16 неделю (в среднем по 27 часов в неделю).

Промежуточная аттестация в каждом семестре – зачет с оценкой.

4. СОДЕРЖАНИЕ ПРАКТИКИ

Целью практики является формирование всех компетенций, указанных в п.1, и получение профессиональных умений и опыта профессиональной деятельности, независимо от места прохождения практики.

Содержание практики соответствует направлению и программе подготовки.

Задачи производственной практики.

В процессе учебной практики **студент должен**:

Изучить:

- мероприятия по охране труда и технике безопасности на предприятии, инструкции по правилам и мерам безопасности при работе на оборудовании;
- национальные и международных стандарты в области информационной безопасности и защиты информации;
- нормативные, методические и специальные документы ФСТЭК России и ФСБ России в области информационной безопасности и защиты информации;
- нормативно-правовые акты в области информационной безопасности и защиты информации;
- организационно-распорядительные документы по защите информации в организации;
- эксплуатационную документацию на системы и средства защиты информации от утечки по техническим каналам;
- эксплуатационную документацию на программные и программно-технические средства защиты информации от несанкционированного доступа и программно-математических воздействий;
- средства контроля эффективности защиты информации от утечки по техническим каналам;
- методики контроля защищенности информации от утечки по техническим каналам;
- средства контроля защищенности информации от несанкционированного доступа и программно-математических воздействий;
- методики контроля защищенности информации от несанкционированного доступа и программно-математических воздействий;

получить опыт практической деятельности:

- выполнения работ по установке и настройке средств защиты информации от утечки по техническим каналам;
- выполнения работ по установке и настройке программных и программно-технических средств защиты информации от несанкционированного доступа и программно-математических воздействий;
- проведения аттестационных испытания объектов информатизации на соответствие требованиям по защите информации от утечки по техническим каналам;
- проведения аттестационных испытаний объектов информатизации по требованиям защиты информации от несанкционированного доступа;
- проведения аудита информационной безопасности автоматизированных систем.

Индивидуальное задание на производственную практику составляется для каждого студента индивидуально с учетом целей и задач практики, профиля подразделения, в котором он проходит практику.

Индивидуальное задание составляется руководителем практики от организации (кафедры), утверждается заведующим кафедрой «Информационная безопасность» университета и выдается студенту в начале прохождения практики.

Пример типового задания по производственной практики:
на 2-й семестр

В процессе производственной практики **студент должен**:

1. Изучить:

– мероприятия по охране труда и технике безопасности на предприятии, инструкции по правилам и мерам безопасности при работе на оборудовании;

нормативные правовые акты:

Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Федеральный закон от 27 июля 2006 г. N 152-ФЗ «О персональных данных»;

Закон Российской Федерации от 21 июля 1993 г. N 5485-1 «О государственной тайне»;

Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;

Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера»;

Указ Президента Российской Федерации от 30 ноября 1995 г. № 1203 «Об утверждении Перечня сведений, отнесенных к государственной тайне»;

Постановление Правительства Российской Федерации от 3 ноября 1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти»;

Постановление Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации»;

Постановление Правительства Российской Федерации от 15 апреля 1995 г. № 333 «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны»;

Постановление Правительства Российской Федерации от 21 ноября 2011 г. № 957 «Об организации лицензирования отдельных видов деятельности»;

Постановление Правительства Российской Федерации от 3 марта 2012 г. № 171 «О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации»;

Постановление Правительства Российской Федерации от 3 февраля 2012 г. № 79 «О лицензировании деятельности по технической защите конфиденциальной информации»;

Постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной

инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений»;

Постановление Правительства Российской Федерации от 17 февраля 2018 г. № 162 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;

Приказ ФСТЭК России от 20 мая 2020 г. № 75 «Об утверждении Порядка согласования субъектом критической информационной инфраструктуры Российской Федерации с Федеральной службой по техническому и экспортному контролю подключения значимого объекта критической информационной инфраструктуры Российской Федерации к сети связи общего пользования»;

Приказ ФСТЭК России от 21 декабря 2017 г. № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»;

Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации »;

Приказ ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»;

Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

Приказ ФСТЭК России от 31 августа 2010 г. № 489 «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования».

* *Документы изучаются в действующих редакциях с внесенными изменениями*

– **специальные нормативные документы:**

Методический документ. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). ФСТЭК России, 2008 г.

Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008 г.

Методический документ. Методика оценки угроз безопасности информации. Утвержден ФСТЭК России 5 февраля 2021 г.

Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации. Решение председателя Гостехкомиссии России от 25 июля 1997 г.

Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Решение председателя Гостехкомиссии России от 30 марта 1992 г.

Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Решение председателя Гостехкомиссии России от 30 марта 1992 г.

Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. Решение председателя Гостехкомиссии России от 30 марта 1992 г.

Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Решение председателя Гостехкомиссии России от 30 марта 1992 г.

Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Одобрены решением коллегии Гостехкомиссии России от 2 марта 2001 г. № 7.2, дсп.

Временная методика оценки защищённости конфиденциальной информации, обрабатываемой основными техническими средствами и системами, от утечки за счёт наводок на вспомогательные технические средства и системы и их коммуникации, Гостехкомиссия России, 2002, дсп.

Временная методика оценки защищенности основных технических средств и систем, предназначенных для обработки, хранения и (или) передачи по линиям связи конфиденциальной информации, Гостехкомиссия России, 2002, дсп.

Временная методика оценки защищенности помещений от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам», Гостехкомиссия России, Москва, 2002, дсп.

Временная методика оценки помещений от утечки речевой конфиденциальной информации по каналам электроакустических преобразований во вспомогательных технических средствах и системах», Гостехкомиссия России, Москва, 2002, дсп.

Требования к средствам контроля машинных носителей информации. Утверждены приказом ФСТЭК России от 28.07.2014 № 87, дсп

Требования к межсетевым экранам. Утверждены приказом ФСТЭК России от 09.02.2016 № 9, дсп

Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 06.12.2011 № 638, дсп

Требования к средствам антивирусной защиты. Утверждены приказом ФСТЭК России от 20.03.2012 №28, дсп

Требования к средствам доверенной загрузки. Утверждены приказом ФСТЭК России от 27.09.2013 №119дсп Утвержден приказом ФСТЭК России от 27.09.2013 г. № 119, дсп.

– **национальные стандарты:**

ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования.

ГОСТ Р 50922-2006. Защита информации. Основные термины и определения

ГОСТ 0043-003-2012. Защита информации. Аттестация объектов информатизации. Общие положения, дсп.

ГОСТ 0043-004-2013. Защита информации. Аттестация объектов информатизации. Программа и методика аттестационных испытаний, дсп.

ГОСТ 22505-97. Совместимость технических средств электромагнитная. Радиопомехи индустриальные от радиовещательных приемников, телевизоров и другой бытовой радиоэлектронной аппаратуры. Нормы и методы испытаний.

ГОСТ 30373-95/ГОСТ Р 50414-92 Совместимость технических средств электромагнитная. Оборудование для испытаний. Камеры экранированные. Классы, основные параметры, технические требования и методы испытаний.

ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования

ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

ГОСТ Р 51583-2014. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения.

ГОСТ Р 52069.0-2013. Защита информации. Система стандартов. Основные положения

ГОСТ Р 52447-2005. Защита информации. Техника защиты информации. Номенклатура показателей качества.

ГОСТ Р 52448-2005. Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения.

ГОСТ Р 52863-2007. Защита информации. Автоматизированные системы в защищенном исполнении. Испытания на устойчивость к преднамеренным силовым электромагнитным воздействиям. Общие требования.

ГОСТ Р 53109-2008. Система обеспечения информационной безопасности сети связи общего пользования. Паспорт организации связи по информационной безопасности.

ГОСТ Р 53110-2008. Система обеспечения информационной безопасности сети связи общего пользования. Общие положения

ГОСТ Р 53111-2008. Устойчивость функционирования сети связи общего пользования. Требования и методы проверки.

ГОСТ Р 53112-2008. Защита информации. Комплексы для измерений параметров побочных электромагнитных излучений и наводок. Технические требования и методы испытаний.

ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения.

ГОСТ Р 53115-2008. Защита информации. Испытание технических средств обработки информации на соответствие требованиям защищенности от несанкционированного доступа. Методы и средства.

ГОСТ Р 56093-2014. Защита информации. Автоматизированные системы в защищенном исполнении. Средства обнаружения преднамеренных силовых электромагнитных воздействий. Общие требования.

ГОСТ Р 56103-2014. Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения.

ГОСТ Р 56115-2014. Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования.

Рекомендации по стандартизации Р 50.1.050-2004. Защита информации. Система обеспечения качества техники защиты информации. Общие положения.

Рекомендации по стандартизации Р 50.1.053-2005. Информационные технологии. Основные термины и определения в области технической защиты информации.

Рекомендации по стандартизации Р 50.1.056-2005. Техническая защита информации. Основные термины и определения.

СНиП 23-03-2003. Защита от шума;

– **положения:**

Положение по аттестации объектов информатизации по требованиям безопасности информации от 25 ноября 1994 г.

– **эксплуатационную документацию на:**

системы пространственного и линейного электромагнитного зашумления: «Гном-3М», «ГШ-2500С», «ЛГШ-503»;

помехоподавляющие фильтры (ФСП-1Ф-10А, ФП-9, ЛФС-100);

системы виброакустической защиты помещений («Шорох-5Л», «Соната-4Б»);

средства защиты ВТСС от утечки информации по акустоэлектрическим каналам (МП-1А, МП-5, МП-8, «Гранит-8»);

средства контроля эффективности защиты СВТ от утечки информации по каналам ПЭМИН (FSH, FSL, АИР-3.2, АИР-5.0, «Волна», RT01022, SMB100A, Я6-122/1, ИС-10/1, 33210A, U1253B, 33521A, U34405A, DSO1052B);

средства контроля подверженности ВТСС акустоэлектрическим преобразованиям (ЭКО-Физика 110А с предусилителем Р-301, 33521A, В6-17, «Прибой»);

средства контроля защищенности речевой информации от утечки по прямым акустическим и акустовибрационным каналам (ЭКО-Физика 110А, 33521A, В6-17, «Волна»);

программные и программно-аппаратные средства защиты автоматизированных систем от несанкционированного доступа к информации («Secret Net», «Dallas Lock», «Страж NT», «Панцир-К», «Застава», «Соболь», Антивирус Касперского, Антивирус Dr.Web);

средства контроля защищенности автоматизированных систем от несанкционированного доступа к информации («Ревизор 1 XP, «Ревизор 2 XP», «Terrier», «ФИКС», «Сканер-ВС»).

2. Получить опыт практической деятельности:

№ п/п	Типы (задачи) выполняемых работ	Код формируемой компетенции
1.	Выполнение работ по установке и настройке средств защиты СВТ от утечки информации по техническим каналам.	ПК-1
2.	Выполнение работ по установке и настройке программных и программно-технических средств защиты информации от несанкционированного доступа и программно-математических	

№ п/п	Типы (задачи) выполняемых работ	Код формируемой компетенции
	воздействий.	
3.	Разработки программ и методик аттестационных испытаний объектов информатизации на соответствие требованиям безопасности информации.	
4.	Проведение аттестационных испытания объектов СВТ на соответствие требованиям по защите информации от утечки по техническим каналам.	
5.	Проведение аттестационных испытаний объектов СВТ по требованиям защиты информации от несанкционированного доступа.	
6.	Подготовки заключений по результатам аттестационных испытаний объектов информатизации на соответствие требованиям безопасности информации и аттестатов соответствия.	
7.	Выполнение работ по установке и настройке средств защиты ВП от утечки информации по техническим каналам.	ПК-2
8.	Разработки программ и методик аттестационных испытаний ВП на соответствие требованиям безопасности информации.	
9.	Проведение аттестационных испытания ВП на соответствие требованиям по защите информации от утечки по техническим каналам.	
10.	Подготовки заключений по результатам аттестационных испытаний объектов информатизации на соответствие требованиям безопасности информации и аттестатов соответствия.	

на 2-й семестр

1. Изучить:

– **национальные стандарты:**

ГОСТ Р 54581-2011 / ISO/IEC TR 15443-1:2005. Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности ИТ. Часть 1. Обзор и основы.

ГОСТ Р 54582-2011 / ISO/IEC TR 15443-2:2005. Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности информационных технологий. Часть 2. Методы доверия.

ГОСТ Р 54583-2011 / ISO/IEC TR 15443-3:2007. Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности информационных технологий. Часть 3. Анализ методов доверия.

ГОСТ Р 56045-2014. Информационная технология. Методы и средства обеспечения безопасности. Рекомендации для аудиторов в отношении мер и средств контроля и управления информационной безопасностью

ГОСТ Р ИСО/МЭК 13335-1-2006. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий.

ГОСТ Р ИСО 7498-1-99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель.

ГОСТ Р ИСО 7498-2-99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации.

ГОСТ Р ИСО/МЭК ТО 13335-5-2006. Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети

ГОСТ Р ИСО/МЭК 15408-1-2012. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.

ГОСТ Р ИСО/МЭК 15408-2-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности.

ГОСТ Р ИСО/МЭК 15408-3-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности.

ГОСТ Р ИСО/МЭК ТО 15446-2008. Информационная технология. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности.

ГОСТ Р ИСО/МЭК ТО 18044-2007. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности.

ГОСТ Р ИСО/МЭК 18045-2013. Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий.

ГОСТ Р ИСО/МЭК ТО 19791-2008. Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем.

ГОСТ Р ИСО/МЭК 21827-2010. Информационная технология. Методы и средства обеспечения безопасности. Проектирование систем безопасности. Модель зрелости процесса.

ГОСТ Р ИСО/МЭК 27000-2012. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология.

ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

ГОСТ Р ИСО/МЭК 27002-2012. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента безопасности.

ГОСТ Р ИСО/МЭК 27003-2012. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности.

ГОСТ Р ИСО/МЭК 27004-2011. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения.

ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.

ГОСТ Р ИСО/МЭК 27006-2008. Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности.

ГОСТ Р ИСО/МЭК 27007-2014. Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности.

ГОСТ Р ИСО/МЭК 27013-2014. Информационная технология. Методы и средства обеспечения безопасности. Руководство по совместному использованию стандартов ИСО/МЭК 27001 и ИСО/МЭК 20000-1.

ГОСТ Р ИСО/МЭК 27033-1-2011. Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции.

ГОСТ Р ИСО/МЭК 27033-3-2014. Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления.

ГОСТ Р ИСО/МЭК 27034-1-2014. Информационная технология. Методы и средства обеспечения безопасности. Безопасность приложений. Часть 1. Обзор и общие понятия.

ГОСТ Р ИСО/МЭК 27037-2014. Информационная технология. Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме.

- **эксплуатационную документацию на:**

программные и программно-аппаратные средства защиты автоматизированных систем от несанкционированного доступа к информации («Secret Net», «Dallas Lock», Антивирус Касперского, Антивирус Dr.Web);

программные и программно-аппаратные средства защиты вычислительных сетей от несанкционированного доступа к информации («Застава», ViPNet Network Security);

средства контроля защищенности автоматизированных систем от несанкционированного доступа к информации («Ревизор 1 XP, «Ревизор 2 XP», «Terrier», «ФИКС», «Сканер-ВС»);

сканеры безопасности («Сканер-ВС», «XSpider»)

система контроля защищенности и соответствия стандартам «MaxPatrol».

2. Получить опыт практической деятельности:

№ п/п	Типы (задачи) выполняемых работ	Код формируемой компетенции
1.	Выполнение работ по установке и настройке программных и программно-технических средств защиты АС от несанкционированного доступа к информации и программно-математических воздействий.	ПК-3
2.	Разработки программ и методик аудита информационной безопасности АС на соответствие требованиям безопасности информации.	
3.	Проведение аудита информационной безопасности АС на соответствие требованиям безопасности информации.	

№ п/п	Типы (задачи) выполняемых работ	Код формируемой компетенции
4.	Подготовки заключений по результатам аудита информационной безопасности АС на соответствие требованиям безопасности информации.	

5. ФОРМЫ ОТЧЕТНОСТИ СТУДЕНТА

Обязательные:

Комплект документов: индивидуальное задание на практику, рабочий график (план) прохождения практики, отчет студента о результатах практики, отзыв руководителя практики с рекомендуемой оценкой.

Дополнительные:

Документы, разработанные при подготовке и проведении аттестации объектов информатизации и аудита информационной безопасности АС.

Выполняемая студентами работа в ходе практики ежедневно отражается в журнале (табель-календаре) прохождения практики.

Правильность, своевременность и аккуратность заполнения журнала являются обязанностью студента и учитываются при выставлении оценки за практику.

Студент, полностью выполнивший программу практики, получивший положительный отзыв от руководителя структурного подразделения, где он ее проходил, допускается до сдачи зачета по практике.

Прием зачета по практике производит комиссия под председательством руководителя производственная практики от организации (кафедры). В состав комиссии входят руководители практики от подразделений, где проходили практику студенты.

Оценка выполненной работы производится по системе аттестации принятой в университете на основе отзыва руководителя практики, содержания и качества оформления отчета.

Оценка по практике приравнивается к оценкам по теоретическому обучению и учитывается при подведении итогов общей успеваемости студентов.

Студенты, не выполнившие программу практики по уважительной причине, направляются на практику вторично, в свободное от учебы время. Студенты, не выполнившие программу практики без уважительной причины, или получившие неудовлетворительную оценку при защите отчета, могут быть отчислены из университета как имеющие академическую задолженность в порядке, предусмотренном Уставом университета.

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕРКИ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

1. ФОС по подкомпетенции **ПК-1** ПрПрк. «Способен проводить аттестацию автоматизированных систем, средств обработки информации проведении аудита информационной безопасности»

2. ФОС по подкомпетенции **ПК-2** ПрПрк. «Способен проводить аттестацию выделенных (защищаемых) помещений на соответствие требованиям безопасности информации».

3. ФОС по подкомпетенции **ПК-3.ПрПрк** «Способен проводить аудит информационной безопасности автоматизированных систем»

Фонды оценочных средств представлены отдельными документами и размещены в составе УМК практики электронной информационной образовательной среды ОРИОКС// URL: http://orioks.miet.ru/**.**

ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ

Литература

1. Воеводин, В. А. Аудит информационной безопасности автоматизированных систем учебное пособие / В. А. Воеводин, А. А. Хорев; Министерство образования и науки РФ, Национальный исследовательский университет "МИЭТ"; под редакцией А.А. Хорева. - Москва : МИЭТ, 2021. - 208 с. - ISBN 978-5-7256-0974-5 : - Текст : непосредственный.
2. Мельников, Д. А. Информационная безопасность открытых систем: учебник / Д. А. Мельников. - Москва : Флинта : Наука, 2014. - 448 с. - URL: https://e.lanbook.com/book/48368 (дата обращения: 16.03.2021). - ISBN 978-5-9765-1613-7; ISBN 978-5-02-037923-7.
3. Организационное и правовое обеспечение информационной безопасности : Учебник и практикум для бакалавриата и магистратуры / Т.А. Полякова, А.А. Стрельцов, С.Г. Чубукова, В.А. Ниесов; Под ред. Т. А. Поляковой, А. А. Стрельцова. - М. : Юрайт, 2018. - 325 с. - (Бакалавр и магистр. Академический курс). - URL: https://urait.ru/bcode/413158 (дата обращения: 15.03.2021). - ISBN 978-5-534-03600-8. - Текст : электронный.
4. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х ч.: Учеб. пособие. Ч. 1 :Правовое обеспечение информационной безопасности/ В.К. Новиков; Министерство образования и науки РФ, Национальный исследовательский университет "МИЭТ". - М. : МИЭТ, 2013. - 184 с. - Имеется электронная версия издания. - ISBN 978-5-7256-0733-8.
5. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х ч.: Учеб. пособие. Ч. 2 Организационное обеспечение информационной безопасности/ В.К. Новиков; Министерство образования и науки РФ, Национальный исследовательский университет "МИЭТ". - М. : МИЭТ, 2013. - 172 с. - ISBN 978-5-7256-0738-3.
6. Воеводин, В. А. Правовые основы аудита информационной безопасности: учебное пособие / В. А. Воеводин, П. Л. Пилюгин; Министерство образования и науки РФ, Национальный исследовательский университет "МИЭТ". - Москва : МИЭТ, 2021. - 180 с. - ISBN 978-5-7256-0961-5 - Текст : непосредственный.
7. Программно-аппаратные средства защиты информации : учебное пособие / В. А. Воеводин, А. В. Душкин, А. Н. Петухов, А. А. Хорев; Министерство образования и науки РФ, Национальный исследовательский университет "МИЭТ"; под редакцией А.А. Хорева. - Москва : МИЭТ, 2021. - 280 с. - ISBN 978-5-7256-0972-1 : Текст :

непосредственный.

8. Программно-аппаратные средства защиты информации : учебно-методическое пособие / А. В. Душкин, О. Р. Лукманова, А. Н. Петухов, А. А. Хорев; Министерство образования и науки РФ, Национальный исследовательский университет "МИЭТ"; под редакцией А.А. Хорева. - Москва : МИЭТ, 2021. - 216 с. - ISBN 978-5-7256-0958-5 : Текст : непосредственный.

9. Зайцев А.П. Технические средства и методы защиты информации : Учебник / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков. - 7-е изд., испр. и доп. - М. : Горячая линия-Телеком, 2018. - 444 с. - URL: https://e.lanbook.com/book/111057 (дата обращения: 16.03.2021). - ISBN 978-5-9912-0233-6.

10. Управление безопасностью критических информационных инфраструктур : учебное пособие / А. Н. Петухов, П. Л. Пилюгин, А. В. Душкин, Ю. А. Губсков; Министерство образования и науки РФ, Национальный исследовательский университет "МИЭТ"; под редакцией А.В. Душкина. - Москва : МИЭТ, 2021. - 208 с. - ISBN 978-5-7256-0973-8 : - Текст : непосредственный.

11. Хорев А.А. Техническая защита информации : Учеб. пособие: В 3-х т. Т. 1 : Технические каналы утечки информации / А.А. Хорев; М-во образования и науки РФ, Федеральное агентство по образованию, МИЭТ(ТУ). - М. : НПЦ Аналитика, 2008. - 436 с. - ISBN 978-59901488-1-9 .

Периодические издания

1. Безопасность информационных технологий : научный журнал / ФГАОУ ВО "Национальный исследовательский ядерный университет "МИФИ". - Москва : НИЯУ МИФИ, 1994 - . - URL: https://bit.mephi.ru/index.php/bit/index (дата обращения: 10.03.2021). - Режим доступа: свободный. - ISSN 2074-7128 (Print); 2074-7136 (Online). - Текст : электронный.

2. Вестник УрФО. Безопасность в информационной сфере: научный журнал/ Южно-Уральский государственный университет (национальный исследовательский университет). – Челябинск: УРГУ, 2011 - 2018. - URL: http://info-secur.ru/index.php/ojs/issue/archive (дата обращения: 16.03.2021). - Режим доступа: свободный. - ISSN 2225-5435 (Print). - Текст: электронный.

3. Information Security / Информационная безопасность». – URL: http://www.itsec.ru/articles2/allpubliks (дата обращения: 15.03.2021). – Текст: электронный.

4. Вопросы кибербезопасности – URL: http://cyberrus.com/ (дата обращения: 15.03.2021). – Текст: электронный.

5. Защита информации. Inside : информационно-методический журнал / Издательский дом "Афина". - Санкт-Петербург : ИД Афина, 2004 - . - URL: http://elibrary.ru/contents.asp?titleid=25917 (дата обращения: 10.03.2021). - Режим доступа: по подписке (2017-2021). - ISSN 2413-3582. - Текст : электронный

6. Jet Info. / Инфосистемы Джет. – URL: http://www.jetinfo.ru (дата обращения: 15.03.2021). – Режим доступа: свободный.

7. Информация и безопасность: научный журнал / ФГБОУ ВО "Воронежский государственный технический университет" (ВГТУ). - Воронеж : ВГТУ, 1998 - . - URL: https://www.elibrary.ru/title_about_new.asp?id=8748 (дата обращения: 15.03.2021). - Режим доступа: для зарегистрированных пользователей. - ISSN 1682-7813. - Текст : электронный.

7. ПЕРЕЧЕНЬ ПРОФЕССИОНАЛЬНЫХ БАЗ ДАННЫХ, ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ

1. eLIBRARY.RU: Научная электронная библиотека: сайт. - Москва, 2000 -. - URL: https://www.elibrary.ru (дата обращения: 16.03.2021). – Текст: электронный.
2. ЛАНЬ: электронно-библиотечная система: сайт. – Санкт-Петербург,2010 -. - URL: https://e.lanbook.com (дата обращения: 10.03.2021). - Текст: электронный.
3. ФСТЭК России: Государственный реестр сертифицированных средств защиты информации. – Москва, 2014. - . - URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii (дата обращения: 10.03.2021). - Текст: электронный.
4. ФСТЭК России: Банк данных угроз безопасности информации. – Москва, 2014. - . - URL: https://bdu.fstec.ru/ (дата обращения: 10.03.2021). - Текст: электронный.
5. Бюро научно-технической информации «Техника для спецслужб»: сайт. – URL: http://www.bnti.ru/about.asp (дата обращения: 15.03.2021). – Текст : электронный.

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

Производственная практика проводится в организациях (на предприятиях), имеющих лицензии ФСТЭК России в области защиты информации, а также в лабораториях кафедры «Информационная безопасность» и аудиториях МИЭТ в соответствии с планом занятий.

Место прохождения практики должно быть оснащено техническими и программными средствами необходимыми для выполнения целей и задач практики: портативными и/или стационарными компьютерами с необходимым программным обеспечением и выходом в Интернет, в том числе предоставляется возможность доступа к информации, размещенной в открытых и закрытых специализированных базах данных.

Конкретное материально-техническое обеспечение практики и права доступа студента к информационным ресурсам определяется руководителем практики, исходя из технического задания на практику.

9. СИСТЕМА КОНТРОЛЯ И ОЦЕНИВАНИЯ

Для оценки успеваемости студентов по практике используется накопительная балльная система. Баллами оцениваются: выполнение каждого контрольного мероприятия в семестре и промежуточная аттестация, проводимая в форме публичной защиты результатов.

По сумме баллов выставляется итоговая оценка. Структура и график контрольных мероприятий доступен в ОРИОКС// URL: http://orioks.miet.ru/ .

РАЗРАБОТЧИК

Заведующий кафедрой «Информационная безопасность»
доктор технических наук, профессор _____ А.А.Хорев

Рабочая программа «Производственной практики – эксплуатационная практика» по направлению подготовки 10.04.01 «Информационная безопасность», направленность (профиль) «Аудит информационной безопасности» разработана на кафедре «Информационная безопасность» и утверждена на заседании кафедры 17 марта 2021 года, протокол № 3.

Заведующий кафедрой «Информационная безопасность»
доктор технических наук, профессор _____ А.А.Хорев

ЛИСТ СОГЛАСОВАНИЯ

Рабочая программа согласована с Центром подготовки к аккредитации и независимой оценки качества
Начальник АНОК _____ / И.М. Никулина /

Рабочая программа согласована с библиотекой МИЭТ
Директор библиотеки _____ / Т.П. Филиппова /