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

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

РАБОЧАЯ ПРОГРАММА ПРАКТИКИ

Вид практики: производственная
Тип практики – эксплуатационная практика

Направление подготовки – 10.03.01 «Информационная безопасность»
Направленность (профиль) – «Техническая защита информации»

2021

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ

Практика участвует в формировании следующих компетенций:

Компетенция ПК-1 «Способен проводить работы по установке, настройке и испытаниям защищенных технических средств обработки 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 B/6 «Проведение работ по установке и техническому обслуживанию защищенных технических средств обработки информации».

Компетенции	**Подкомпетенции, формируемые на практике**	**Индикаторы достижения подкомпетенций**
ПК-1. «Способен проводить работы по установке, настройке и испытаниям защищенных технических средств обработки информации»	ПК-1. ПрПрк. Способен проводить работы по установке, настройке и испытаниям защищенных технических средств обработки информации	**Знания** методические документы, национальные стандарты в области защиты информации ограниченного доступа и эксплуатации защищенных технических средств обработки информации (ЗТСОИ); технические каналы утечки информации, возникающие при обработке информации ЗТСОИ; способы и средства защиты ЗТСОИ от утечки информации по техническим каналам; способы реализации несанкционированного доступа к информации и специальных программных воздействий на информацию и ее носители в автоматизированных системах; методы и средства защиты АС от несанкционированного доступа к информации и специальных программных воздействий на нее; технические описания и инструкции по эксплуатации защищенных технических средств обработки информации; порядок организации технического обслуживания защищенных технических средств обработки информации.

		Умения: производить установку, настройку и испытания средств защиты ЗТСОИ от утечки информации по техническим каналам; производить установку, настройку и испытания средств защиты ЗТСОИ от несанкционированного доступа к информации. **Опыт практической деятельности:** установки и настройки средств защиты ЗТСОИ.

Компетенция ПК-2 «Способен проводить контроль эффективности защиты информации от утечки за счет побочных электромагнитных излучений и наводок» сформулирована на основе профессионального стандарта «Специалист по технической защите информации», утверждённый приказом Минтруда России от 01.11.2016 № 599н. Регистрационный № 844.

Обобщенная трудовая функция D/6 «Проведение контроля защищенности информации».

Трудовая функция D/02.6 «Проведение контроля защищенности информации от утечки за счет побочных электромагнитных излучений и наводок».

Компетенции	**Подкомпетенции, формируемые в дисциплине**	**Индикаторы достижения подкомпетенций**
ПК-2. Способен проводить контроль эффективности защиты информации от утечки за счет побочных электромагнитных излучений и наводок	ПК-2. ПрПрк. Способен проводить контроль эффективности защиты информации от утечки за счет побочных электромагнитных излучений и наводок	**Знания:** нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации; технические каналы утечки информации, отрабатываемой техническими средствами (ТС); способы и средства защиты информатизации от утечки за счет ПЭМИН; средства контроля защищенности информации от утечки за счет побочных электромагнитных излучений и наводок (ПЭМИН); методики измерения ПЭМИН ТС; методики расчета радиусов опасных зон ПЭМИН; методики расчета показателей защищенности информации от

Компетенции	Подкомпетенции, формируемые в дисциплине	Индикаторы достижения подкомпетенций
		утечки за счет ПЭМИН; отчетные документы, оформляемые по результатам контроля защищенности информации от утечки за счет ПЭМИН. **Умения:** проводить измерение электрической и магнитной составляющей побочных электромагнитных излучений (ПЭМИ) технических средств обработки информации (ТСОИ) в различных режимах их работы с использованием контрольно-; измерительной аппаратуры проводить измерение наводок ПЭМИ ТСОИ в различных режимах их работы с использованием контрольно- измерительной аппаратуры; рассчитывать радиусы опасных зон побочных электромагнитных излучений и наводок; проводить испытания ТСОИ (с использованием технических средств) с цепью проверки защищенности информации от утечки за счет ПЭМИН; проводить оценку защищенности информации от утечки за счет ПЭМИН; рассчитывать показатели защищенности информации от утечки за счет ПЭМИН; оформлять протоколы оценки защищенности информации от утечки за счет ПЭМИН. **Опыт практической деятельности:** контроля эффективности защиты информации от утечки за счет ПЭМИН.

Компетенция ПК-3 «Способен проводить контроль эффективности защиты акустической (речевой) информации от утечки по техническим каналам» сформулирована на основе профессионального стандарта «Специалист по технической защите информации», утверждённый приказом Минтруда России от 01.11.2016 № 599н. Регистрационный № 844.

Обобщенная трудовая функция D/6 «Проведение контроля защищенности информации».

Трудовая функция D/03.6 «Проведение контроля защищенности акустической речевой информации от утечки по техническим каналам».

Компетенции	Подкомпетенции, формируемые в дисциплине	Индикаторы достижения подкомпетенций
ПК-3. Способен проводить контроль эффективности защиты акустической (речевой) информации от утечки по техническим каналам	ПК-3. ПрПрк. Способен проводить контроль эффективности защиты акустической (речевой) информации от утечки по техническим каналам	**Знания:** нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации; технические каналы утечки акустической речевой информации (прямые акустические, вибрационные, акустооптические, акустоэлектрические, акустоэлектромагнитные); средства и методики контроля защищенности информации от утечки по акустическим, вибрационным и акустооптическим каналам; средства и методики контроля подверженности технических средств акустоэлектрическим и акустоэлектромагнитным преобразованиям; отчетные документы, оформляемые по результатам контроля защищенности акустической речевой информации от утечки по техническим каналам. **Умения:** проводить контроль защищенности акустической речевой информации от утечки техническим каналам;

Компетенции	Подкомпетенции, формируемые в дисциплине	Индикаторы достижения подкомпетенций
		рассчитывать показатели защищенности акустической речевой информации; проводить оценку защищенности акустической речевой информации от утечки по техническим каналам; оформлять протоколы оценки защищенности акустической речевой информации от утечки по техническим каналам. **Опыт практической деятельности:** контроля эффективности защиты акустической (речевой) информации от утечки по техническим каналам.

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 в 8-м семестре 4 курса.

Прохождение практики базируется на знаниях и умениях, полученных при изучении дисциплин: «Защита информации от утечки по техническим каналам», «Программно-аппаратные средства защиты информации», «Основы управления информационной безопасностью» и в ходе учебной практики.

Знания и умения, полученные в результате прохождения производственной практики, используются подготовке ВКР и в дальнейшей профессиональной 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 – 9 ЗЕТ (324 ак. часов).

Практика организуется в 8-м семестре в период с 7 по 12 неделю по 54 часа 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;
- нормативно-правовые акты в области защиты информации;
- национальные и международных стандарты в защиты информации;
- нормативные, методические и специальные документы ФСТЭК России и ФСБ России в области 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;
- методики контроля защищенности информации от несанкционированного доступа;

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;
- проведения контроля эффективности защиты информации от утечки за счет ПЭМИН;
- проведения контроля эффективности защиты акустической речевой информации от утечки по техническим каналам.

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 учебной практике:

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:

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

Примечание: Документы изучаются в действующих редакциях с внесенными изменениями

– **национальные стандарты:**

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

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

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.

– **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», «VNG-012M»;

помехоподавляющие фильтры (ЛФС-100);

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

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

средства контроля эффективности защиты СВТ от утечки информации по каналам ПЭМИН (FSV, НБА-02, НРА-02, RT01022);

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

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

программные и программно-аппаратные средства защиты автоматизированных систем 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», «Сканер-ВС», «XSpider»).

2. Получить опыт практической деятельности:

№ п/п	Типы (задачи) выполняемых работ	Код формируемой компетенции
1.	Установка, настройка и испытания средств защиты ЗТСОИ от утечки информации по техническим каналам.	ПК-1
2.	Установка, настройка и испытания средств защиты ЗТСОИ от несанкционированного доступа к информации.	
3.	Измерение электрической и магнитной составляющей ПЭМИ ТСОИ в различных режимах их работы с использованием контрольно-; измерительной аппаратуры.	ПК-2
4.	Измерение наводок ПЭМИ ТСОИ в различных режимах их работы с использованием контрольно- измерительной аппаратуры.	
5.	Расчет радиусов опасных зон ПЭМИН.	
6.	Испытания ТСОИ (с использованием технических средств) с цепью проверки защищенности информации от утечки за счет ПЭМИН.	
7.	Оценка защищенности информации от утечки за счет ПЭМИН.	
8.	Расчет показателей защищенности информации от утечки за счет ПЭМИН.	
9.	Оформление протоколов оценки защищенности информации от утечки за счет ПЭМИН.	
10.	Контроль защищенности акустической речевой информации от утечки техническим каналам.	ПК-3
11.	Расчет показателей защищенности акустической речевой информации.	
12.	Оценка защищенности акустической речевой информации от утечки по техническим каналам.	
13.	Оформление протоколов оценки защищенности акустической речевой информации от утечки по техническим каналам.	

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:

Отчеты о выполнении практико-ориентированных заданий.

Выполняемая студентами работа в ходе 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 работы по установке, настройке и испытаниям защищенных технических средств обработки информации».

2. ФОС по подкомпетенции **ПК-2** ПрПрк. «Способен проводить контроль эффективности защиты информации от утечки за счет побочных электромагнитных излучений и наводок».

3. ФОС по подкомпетенции **ПК-3** ПрПрк. «Способен проводить контроль эффективности защиты акустической (речевой) информации от утечки по техническим каналам».

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

7. ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ

Литература

1. Воеводин В.А., Хорев А.А. Аудит информационной безопасности автоматизированных систем : учебное пособие; под редакцией А.А. Хорева. - Москва : МИЭТ, 2021. - 208 с. - ISBN 978-5-7256-0974-5 .

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. 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.

5. 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.

6. 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.

7. 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: 15.03.2021). - ISBN 978-5-9912-0233-6.

8. 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.

9. 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. ЗАЩИТА ИНФОРМАЦИИ. INSIDE : информационно-методический журнал / Издательский дом "Афина". - Санкт-Петербург : ИД Афина, 2004 - . - URL: http://elibrary.ru/contents.asp?titleid=25917 (дата обращения: 15.03.2021). - Режим доступа: по подписке (2017-2021). - ISSN 2413-3582. - Текст : электронный : непосредственный.

2. 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.

3. 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.

4. 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.

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

Учебная практика проводится 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 - эксплуатационной практики» по направлению подготовки 10.03.01 «Информационная безопасность», направленности (профилю) «Техническая защита информации» 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 /