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

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

РАБОЧАЯ ПРОГРАММА ПРАКТИКИ

Вид практики: учебная
Тип практики – учебно-лабораторная 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. УчПрк. 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. УчПрк. 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 утечки

Компетенции	Подкомпетенции, формируемые в дисциплине	Индикаторы достижения подкомпетенций
		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. УчПрк. 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; рассчитывать показатели защищенности акустической речевой информации; проводить оценку защищенности акустической речевой информации от утечки по техническим каналам;

Компетенции	Подкомпетенции, формируемые в дисциплине	Индикаторы достижения подкомпетенций
		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

Учебная практика – учебно-лабораторная практика входит в часть, формируемую участниками образовательных отношений Блока 2 «Практика» образовательной программы.

Учебная 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».

Знания и умения, полученные в результате прохождения учебной практики, используются при прохождении производственной практики.

Способ проведения практики: стационарная. Практика проходит в подразделениях НИУ МИЭТ.

3. ОБЪЁМ ПРАКТИКИ

Объём практики – 6 ЗЕТ (216 ак. часов).

Практика организуется в 8-м семестре в период с 1 по 6 неделю по 36 часов в неделю.

Промежуточная аттестация – зачет с оценкой.

4. СОДЕРЖАНИЕ ПРАКТИКИ

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

Содержание практики соответствует направлению и программе подготовки.

Задачи учебной 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 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:

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»;

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»;

Примечание: 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 52447-2005. Защита информации. Техника защиты информации. Номенклатура показателей качества.

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

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

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-3», «ГШ-2500С», «ЛГШ-503»;

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

системы виброакустической защиты помещений («Соната-3Б»);

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

средства контроля эффективности защиты СВТ от утечки информации по каналам ПЭМИН (FSH, FSL, АИР-3.2, АИР-5.0, RT01022, SMB100A, Я6-122/1);

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

средства контроля защищенности речевой информации от утечки по прямым акустическим и акустовибрационным каналам (ЭКО-Физика 110А, 33521А, В6-17,

«Волна»);

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

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

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. УчПрк.** Способен проводить работы по установке, настройке и испытаниям защищенных технических средств обработки информации.

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

3. ФОС по подкомпетенции **ПК-3. УчПрк.** 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/**.**

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. 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 : б.ц., 300 экз. Шифры: ББК 67.401 - В-63. Экземпляры: Всего: 25, из них: аб-21, чз-3, чз(Архив)-1
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 : б.ц., 300 экз. Шифры: 004.056(075.8) - П-784. Экземпляры: Всего: 40, из них: аб-36, чз-3, чз(Архив)-1
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 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 «Учебная практика - учебно-лабораторная практика» 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 /