АНО ВО «Межрегиональный открытый социальный институт»

УТВЕРЖДАЮ
Декан факультета экономики и информационной безопасности
_____ Т.А. Сафина
Протокол заседания Совета факультета
№6 от «17» января 2017 г.

ПРОГРАММА ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

Направление подготовки:
10.03.01 Информационная безопасность
Профиль подготовки:
Комплексная защита объектов информатизации

Форма обучения:
очная, очно-заочная

СОГЛАСОВАНО
Технический директор филиала ПАО «Ростелеком» в Республике Марий Эл
_____ С.Г. Ерославов

СОГЛАСОВАНО
Начальник отдела автоматизированных систем управления АО «Марийский машиностроительный завод»
_____ Е.Л. Цивин

Йошкар-Ола, 2017

Содержание:

1. Цели и задачи производственной практики

Производственная практика студентов АНО ВО «Межрегиональный открытый социальный институт» является составной частью образовательной программы высшего образования направления подготовки 10.03.01 Информационная безопасность.

Основная цель производственной практики – закрепление и углубление теоретических знаний по информационной безопасности и защите информации, программно-техническим, организационным и правовым методам обеспечения информационной безопасности, приобретение практических профессиональных навыков и формирование компетенций, опыта самостоятельной профессиональной деятельности.

Основными задачами практики являются:

1. изучение структуры предприятия и действующей на нем системы управления;
2. изучение информационной структуры предприятия, информационных технологий, используемых на предприятии;
3. изучение перспективных разработок на предприятии;
4. закрепление знаний, полученных в процессе обучения, адаптация к рынку труда;
5. совершенствование навыков сбора, систематизации и анализа информации, необходимой для решения практических задач в сфере информационной безопасности;
6. приобретение навыков профессиональной работы и решения практических задач в сфере информационной безопасности.

В процессе прохождения практики студенты овладевают умениями и навыками администрирования подсистемы информационной безопасности объекта и ее обеспечения, знакомятся с профессиональной деятельностью в сфере комплексной защиты объектов информации.

2. Общая характеристика производственной практики

Производственная практика входит в раздел «Б2.П.1 - производственная практика» учебного плана образовательной программы направления подготовки 10.03.01 Информационная безопасность.

В соответствии с учебным планом производственная практика по очной форме обучения проводится на 3 курсе в 6 семестре, а по очно-заочной форме обучения на 4 курсе в 8 семестре. Продолжительность практики составляет 6 недель.

Общая трудоемкость производственной практики составляет 9 зачетных единиц, 324 часа.

Прохождение практики возможно после изучения таких дисциплин, как «Криптографические методы защиты информации», «Основы информационной безопасности», «Программно-аппаратные средства защиты информации», «Системы управления базами данных», «Современные системы стандартизации в области информационной безопасности».

Производственная практика, предусмотренная Федеральным государственным образовательным стандартом высшего образования по направлению подготовки 10.03.01 Информационная безопасность, осуществляется на основе договоров на проведение практики студентов, заключенных между АНО ВО МОСИ и учреждениями (предприятиями, организациями).

Тип производственной практики:

проектно-технологическая практика.

Способы проведения производственной практики:

стационарная, выездная.

Местом прохождения производственной практики могут служить государственные, коммерческие и некоммерческие организации; информационные подразделения предприятий различных сфер деятельности, а также научно-производственные организации.

Студенты очно-заочной формы обучения, работающие по направлению подготовки «Информационная безопасность», как правило, проходят производственную практику по месту работы.

Договоры на проведение практики заключены с Филиалом ООО «Росгосстрах» в РМЭ, ООО «Автограф», Марийским региональный центром повышения квалификации и переподготовки кадров, Управлением федеральной миграционной службы по РМЭ, Главным управлением МЧС России по Республике Марий Эл, Государственным учреждением Республики Марий Эл «Центр занятости населения города Йошкар-Олы», ОАО «Россельхозбанк» (Кировский РФ ОАО «Россельхозбанк»), Маристат.

Общее руководство производственной практикой осуществляет руководитель практики, который обеспечивает взаимодействие АНО ВО МОСИ с организациями и должностными лицами по вопросам, связанным с организацией и прохождением студентами МОСИ производственной практики. Руководитель от базы практики назначается приказом руководителя организации.

Руководитель практики от Института:

- проводит установочную конференцию, в ходе которой знакомит обучающихся с программой практики, системой оценки, заданиями по практике и консультирует по вопросам выполнения заданий программы практики и по написанию отчетов;

- оказывает студенту консультационную помощь по выполнению заданий, осуществляет текущий контроль, посещает базу практики, поддерживает взаимосвязь с обучающимся посредством сети «Интернет», телефонной связи, личного общения;

- ведет учет выхода студентов на практику;

-знакомит руководителей базы практики с программой производственной практики и методикой ее проведения, требованиями к студентам-практикантам и критериями оценки их работы во время практики;

- проводит промежуточную аттестацию;

- оценивает уровень освоения компетенций обучающегося;
- проверяет отчетную документацию;
- изучает вопрос о наличии вакансий с целью дальнейшего трудоустройства выпускников Института.

Руководитель базы практики:

- организует прохождение практики студентом;
- знакомит с организацией и методами работы на конкретном рабочем месте, с охраной труда;
- помогает выполнить задания практики и консультирует по вопросам;
- проверяет ведение студентом дневника и подготовку отчета о прохождении практики;
- осуществляет текущий контроль за практикой студентов;
- подтверждает записи обучающего о выполненных работах в дневнике практики;
- составляет характеристики, содержащие данные о выполнении программы практики и индивидуальных заданий, об отношении студентов к работе.

Студенты при прохождении практики обязаны:

- передать по месту организации практики договор и направление;
- прибыть на место практики в установленные сроки, предъявить направление на практику и получить разрешение руководителя на выполнение функций специалиста, предусмотренного программой практики;
- соблюдать правила и нормы охраны труда, техники безопасности, правила внутреннего распорядка организации;
- составить индивидуальный план своей деятельности на практике и согласовать его со своим руководителем практики;
- в полном объеме выполнить все задания, предусмотренные программой практики;
- собрать необходимую информацию для написания отчета по практике;
- подготовить письменный отчет о прохождении практики и представить его в Институт для защиты в установленные сроки.

В случае производственной необходимости и по желанию студентов руководители организаций могут использовать студентов на штатных должностях с выплатой им заработной платы. По окончанию трудового договора студент может обратиться к руководителю организации или структурного подразделения с просьбой дать ему рекомендацию.

3. Планируемые результаты обучения при прохождении практики

В результате прохождения производственной практики студент должен:

Знать:

- методы и средства проектирования подсистем и средств обеспечения информационной безопасности;

- комплекс мер по обеспечению информационной безопасности;
- правила оформления документов;
- нормативные правовые акты в профессиональной деятельности;

Уметь:

- планировать и осуществлять свою деятельность с учетом результатов анализа, оценивать и прогнозировать последствия своей профессиональной деятельности;
- проводить обоснование соответствующих проектных решений;
- оформлять рабочую техническую документацию;
- определять информационные ресурсы, подлежащие защите;

Владеть:

- навыками поиска методов решения практических задач;
- технологиями системного анализа при ведении проектной деятельности;
- навыками оформления документации в области информационной безопасности;
- навыками проведения анализа информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности;
- навыками выполнения комплекса мер по обеспечению информационной безопасности.

Прохождение данной практики необходимо в качестве предшествующей формы учебной работы для дальнейшего освоения учебных дисциплин, таких как: «Техническая защита информации», «Комплексные системы защиты информации на предприятии», «Защита и обработка конфиденциальных документов», «Организация и управление службой защиты информации на предприятии», «Системы защищенного электронного документооборота».

В результате прохождения данной производственной практики должны быть сформированы следующие компетенции:

Общекультурные компетенции (ОК):

ОК-8 – способностью к самоорганизации и самообразованию;

Общепрофессиональные компетенции (ОПК):

ОПК-5 – способностью использовать нормативные правовые акты в профессиональной деятельности;

ОПК-7 – способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты;

Профессиональные компетенции (ПК):

проектно-технологическая деятельность:

ПК-7 – способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной

безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений;

ПК-8 – способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов;

экспериментально-исследовательская деятельность:

ПК-10 – способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности;

организационно-управленческая деятельность:

ПК-13 – способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации.

4. Структура и содержание производственной практики

Содержание практики определено в соответствии с требованиями ФГОС ВО по направлению подготовки 10.03.01 Информационная безопасность профиль «Комплексная защита объектов информатизации»

Планируемый результат (шифр компетенции)	Задания
Задания, формирующие отдельные компетенции	
ОПК-5, ОПК-7, ПК-8	Провести анализ предприятия (отдела)
ОПК-7, ПК-10	Провести сравнительный анализ подсистем (программных, аппаратных, технических средств защиты информации) по показателям информационной безопасности
ПК-10, ПК-13	Провести поиск оптимальных путей и инструментов решения для проектирования систем защиты информации
ПК-8, ПК-10	Провести проектные расчеты элементов систем обеспечения информационной безопасности
ПК-13	Предложить комплекс мер по улучшению (совершенствованию) системы информационной безопасности предприятия
ПК-7, ПК-8	Обосновать технико-экономические расчеты по предложенным мерам совершенствования системы информационной безопасности предприятия.
ОК-8	Составить план практики, написать отчет

В ходе практики бакалавры отрабатывают следующие виды деятельности:

- сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности;

- поиск оптимальных путей решения для проектирования систем защиты информации;
- подбор эффективных инструментов решения для проектирования систем защиты информации;
- проведение проектных расчетов элементов систем обеспечения информационной безопасности;
- участие в разработке технологической и эксплуатационной документации;

проведение предварительного технико-экономического обоснования проектных расчетов.

Формами деятельности студентов при прохождении практики являются самостоятельная работа, анализ и конспектирование методической литературы, консультации, подготовка отчетной документации, конференции.

1. Подготовительный этап (2 часа).

До начала практики проводится установочная конференция, на которой обозначаются перед студентами конкретные задачи их практической деятельности, структура плана индивидуальной работы, форма и содержание отчетной документации.

2. Основной этап (312 часов).

При прохождении практики студенты должны:

1. Провести анализ предприятия (отдела) по следующим характеристикам:
- типовые структуры предприятия, связи и автоматизации объектов информатизации, оснащенность техническими средствами;
- построение и функционирование операционных систем, систем управления базами данных, локальных и глобальных компьютерных сетей, основных протоколов компьютерных сетей;
- различных носителей конфиденциальной информации, работ и объектов, подлежащих защите;
- организации документооборота, в том числе электронного (при наличии в организации), с учетом конфиденциальности информации;
- оформлении документации по оперативному управлению средствами зашиты информации и персоналом, имеющим доступ к конфиденциальным сведениям.

Результаты оформить ***в виде текста, схем, таблиц.***

2. Провести сравнительный анализ подсистем (программных, аппаратных, технических средств защиты информации) по показателям информационной безопасности. Результаты оформить ***в виде таблицы***

Образец

Объект	Выявленная угроза	Описание угрозы
ОС Windows 7	Угроза аппаратного сброса пароля	Угроза заключается в возможности сброса паролей, установленных в BIOS/UEFI без прохождения процедуры авторизации в

	BIOS	системе путём обесточивания микросхемы BIOS (съёма аккумулятора) или установки перемычки в штатном месте на системной плате (переключение «джампера»). Данная угроза обусловлена уязвимостями некоторых системных (материнских) плат – наличием механизмов аппаратного сброса паролей, установленных в BIOS/UEFI. Реализация данной угрозы возможна при условии наличия у нарушителя физического доступа к системному блоку компьютера
Локальная сеть	Угроза доступа к локальным файлам сервера при помощи URL	Угроза заключается в возможности передачи нарушителем дискредитируемому браузеру запроса на доступ к файловой системе пользователя вместо URL-запроса. При этом браузер выполнит этот запрос с правами, которыми он был наделён при запуске, и передаст данные, полученные в результате выполнения этой операции, нарушителю. Данная угроза обусловлена слабостями механизма проверки вводимых пользователем запросов, который не делает различий между запросами на доступ к файловой системе и URL-запросами. Реализация данной угрозы возможна в случае наличия у нарушителя привилегий на отправку запросов браузеру, функционирующему в дискредитируемой системе

3. Провести поиск оптимальных путей и инструментов решения для проектирования систем защиты информации. Результаты оформить ***в виде таблицы.***

	Объект	Выявленная угроза	Результаты анализа угрозы	Принятые меры

4. Провести проектные расчеты элементов систем обеспечения информационной безопасности. Результаты оформить ***в виде схемы, таблицы.***

5. Предложить комплекс мер по улучшению (совершенствованию) системы информационной безопасности предприятия. Результаты оформить ***в виде текста, схем, таблиц.***

6. Обосновать технико-экономические расчеты по предложенным мерам совершенствования системы информационной безопасности предприятия. Результаты оформить ***в виде схемы, таблицы.***

3. Завершающий этап (10 часов).

После завершения практики студент обязан предоставить руководителю практики от института для защиты отчета по практике: а) характеристику с места практики с подписью и печатью; б) отчет о прохождении практики; в) дневник практики.

Отчет о практике должен содержать сведения о выполненных студентом работах в период практики: результаты исследований с последующими выводами.

5. Формы промежуточной аттестации по итогам производственной практики

Система оценки качества прохождения практики предусматривает следующие виды контроля:

– текущий контроль;

– промежуточная аттестация.

Текущий контроль осуществляется руководителем от базы практики и руководителем от АНО ВО МОСИ. Проводится в форме собеседования, посещения баз практики и предварительной проверки материалов отчета по практике.

Промежуточная аттестация проводится в форме дифференциального зачета. Зачет проводится в виде защиты отчетов по практике и ответов на вопросы.

При проведении промежуточной аттестации обучающегося учитываются результаты текущего контроля.

Руководитель практики от института оценивает уровень сформированности компетенций, качество, полноту, правильность оформления отчетных документов по практике, а также правильность выполнения заданий, расчетов и сделанных выводов.

Порядок защиты отчета по производственной практике

Для допуска к защите практики студент обязан представить руководителю практики от кафедры необходимые документы: характеристику, дневник прохождения практики, отчет студента по практике, материалы, прилагаемые к отчету.

В отчете студент должен указать, как проходила практика, какую она ему принесла пользу в усвоении теоретического материала, какую помощь оказывали руководители практики (преподаватели и практические работники).

Отчет должен отражать отношение студента к изученным материалам и той деятельности, с которой он знакомился, те знания и навыки, которые он приобрел в ходе практики.

Структура письменного отчета по производственной практике состоит из:

– титульного листа;

– содержания;

– введения (указываются цель, задачи, место прохождения практики и сроки ее проведения);

– практической части (включает в себя выполненные задания в полном объеме);

– заключения (приводятся выводы и общие впечатления студента от практики);

– списка литературы;

– приложений.

Объем отчета (без приложений) должен составлять 15 - 20 страниц машинописного текста на одной стороне бумаги. Текст печатается 14 пт. шрифтом с 1,5 интервалом, с соблюдением следующих размеров полей: левое – 30 мм., правое – 10 мм., верхнее – 20 мм., нижнее – 20 мм.

Во время защиты отчета студент должен уметь анализировать те или иные действия и решения, указать, при каком условии они являются законными, обоснованными.

При ненадлежащем оформлении представленных документов (отсутствие характеристики, подписей, печатей, отчета, виз руководителей) защита отчета по практике откладывается с указанием сроков для необходимых исправлений.

Студенты, не получившие зачет по результатам практики, считаются имеющими академическую задолженность.

На защите могут присутствовать представители и руководители от баз (организаций) практики.

Фонд оценочных средств для проведения промежуточной аттестации

1. Назовите методы решения практических задач.
2. Назовите методы и средства проектирования подсистем и средств обеспечения информационной безопасности.
3. Перечислите технологии системного анализа при проведении проектной деятельности.
4. Перечислите правила оформления документации в области информационной безопасности.
5. Назовите различные носители конфиденциальной информации, подлежащие защите.
6. Назовите оптимальные пути и инструменты решения для проектирования систем защиты информации.

7. Перечислите комплексы мер по улучшению (совершенствованию) системы информационной безопасности предприятия.

8. Приведите классификацию угроз информационной безопасности.

9. Назовите концептуальные нормативно-правовые акты России в области защиты информации.

Общая оценка практики

Основные критерии оценки производственной практики:

Отлично	Хорошо	Удовлетворительно	Неудовлетвори-тельно
Качество собранного материала			
Собранный материал полностью обеспечивает выполнение задач и заданий практики; актуален; достаточно полон.	Собранный материал частично обеспечивает выполнение задач и заданий практики; не весь актуален; сравнительно полон.	Собранный материал частично обеспечивает выполнение задач и заданий практики; на половину неактуален; сравнительно полон.	Собранный материал не полон; весьма устаревший; не способствует расширению компетенций и выполнению заданий практики
Качество оформления отдельных элементов и в целом отчета по практике			
Таблицы, иллюстрации и в целом отчет оформлены строго в соответствии с требованиями.	В оформлении таблиц, иллюстраций и в целом отчета допущено не более 5 незначительных неточностей.	В оформлении таблиц, иллюстраций и в целом отчета допущено не более 5-8 незначительных неточностей.	В оформлении таблиц, иллюстраций и в целом отчета допущено не более 8-15 незначительных неточностей. Примечание: в случае наличия в отчете более 15 незначительных неточностей в оформлении и/или отчет оформлен без соблюдения требований, отчет по практике не рекомендуется к защите.
Посещаемость практики студентом			
Студент все дни практики посетил	Студент не посетил 1 день практики	Студент не посетил 2 дня практики	Студент не посетил 3 дня практики. Примечание: при непосещении от 4 и более дней практики студенту не засчитывается прохождение практики
Отношение студента к выполняемой работе			

Студент проявил интерес к работе, исполнительность, аккуратность, дисциплинированность, грамотность, умение работать с современными информационными системами, коммуникабельность, самостоятельность	Студент проявил интерес к работе, исполнительность, аккуратность, дисциплинированность, самостоятельность, коммуникабельность; показал неуверенность умения работать с современными информационными системами	Студент не проявил явного интереса к работе, но был исполнителен, аккуратен, дисциплинирован; показал грамотность, умение работать с современными информационными системами, коммуникабельность, самостоятельность.	Студент не проявил интерес к работе, исполнительность; неаккуратен; не показал умение работать с современными информационными системами, зависим в решении задач практики
Ответы на вопросы			
Студент правильно ответил на 4-5 вопросов. Ответы сформулированы четко, логично и грамотно, отражают всю сущность вопроса.	Студент правильно ответил на 2-3 вопроса. Ответы сформулированы четко, логично и грамотно, отражают всю сущность вопроса.	Студент правильно ответил на 1 вопрос. Ответ сформулирован четко, логично, но допущены незначительные неточности.	Студент не ответил на вопросы, допускает грубые логические ошибки, демонстрируя фрагментарные знания.

Оценка уровня сформированности компетенций

Руководитель практики оценивает уровень сформированности компетенций обучающегося. С этой целью оценивается каждое выполненное задание программы практики: задание выполнено без замечаний – 1 балл, с замечаниями – 0,5 балла. Если студент не выполняет задание – балл не засчитывается.

По балльной системе оцениваются следующие задания:

- проведение анализа предприятия (отдела) по основным характеристикам;
- проведение сравнительного анализа подсистем (программных, аппаратных, технических средств защиты информации) по показателям информационной безопасности;
- проведение поиска оптимальных путей и инструментов решения для проектирования систем защиты информации;
- проведение проектных расчетов элементов систем обеспечения информационной безопасности;
- предложение комплекса мер по улучшению (совершенствованию) системы информационной безопасности предприятия;
- обоснование технико-экономических расчетов по предложенным мерам совершенствования системы информационной безопасности предприятия.

Расчет уровня сформированности компетенций в целом по производственной практике

Уровень сформированности компетенций рассчитывается по следующей формуле:

$$СК=\frac{Б1+Б2+...+Бn}{N} \text{ x } 100\%$$

где Б1+Б2+…….Бn – сумма баллов за выполненные задания, N – количество заданий.

Шкала перевода % сформированности компетенций в оценки

Степень сформированности компетенций	Процентный интервал оценивания	Система оценки
Высокий уровень	80-100%	«отлично»
Продвинутый уровень	65-80%	«хорошо»
Базовый уровень	50-65%	«удовлетворительно»
Низкий уровень	менее 50%	«неудовлетворительно»

Итоговая оценка за производственную практику выводится с учетом общей оценки за практику и оценки уровня сформированности компетенций.

По результатам защиты руководитель практики от кафедры выставляет оценку по четырехбальной системе (отлично, хорошо, удовлетворительно, неудовлетворительно).

6. Учебно-методическое и информационное обеспечение производственной практики

В зависимости от формы, места прохождения практики и конкретных задач практики, которые ставит перед обучающимися руководитель практики от Института, студентам на организационном собрании по практике выдается перечень основной и дополнительной литературы, программного обеспечения и Интернет-ресурсов в целях учебно-методического и информационного обеспечения практики.

Этот перечень может быть дополнен или конкретизирован руководителем практики от учреждения (предприятия, организации), куда направляется обучающийся для прохождения практики.

Литература

Основная учебная литература

1. Коваленко, Ю.Ю. Правовой режим лицензирования и сертификации в сфере информационной безопасности: Учебное пособие / Ю.Ю. Коваленко. – М.: Горячая линия – Телеком, 2012. – 140 с.1.

2. Новиков, В.К. Организационное и правовое обеспечение информационной безопасности: В 2–х частях. Часть 1. Правовое обеспечение информационной безопасности: учеб. пособие / В.К. Новиков. – М.: МИЭТ, 2013. – 184 с.

3. Новиков, В.К. Организационное и правовое обеспечение информационной безопасности: В 2–х частях. Часть 2. Организационное обеспечение информационной безопасности: учеб. пособие / В.К. Новиков. – М.: МИЭТ, 2013. – 172 с.

Дополнительная литература

1. Стрельцов, А.А. Правовое обеспечение информационной

безопасности России: теоретические и методологические основы/ А.А. Стрельцов. – Минск, 2005.

2. Организационно-правовое обеспечение информационной безопасности: учебное пособие / под ред. А.А. Стрельцова. – М.: Академия, 2008. – 256 с.

3. Семкин, С.Н. Основы правового обеспечения защиты информации: учебное обеспечение для вузов / С.Н. Семкин, А.Н. Семкин. – М.: Горячая линия-Телеком, 2008. – 238 с.

Нормативные правовые акты

1. Федеральный закон от 27 июля 2006 г. № 149–ФЗ «Об информации, информационных технологиях и о защите информации».

2. Федеральный закон от 27 июля 2006 г. № 152–ФЗ «О персональных данных».

3. Федеральный закон от 27 декабря 2002 г. № 184–ФЗ «О техническом регулировании».

4. Федеральный закон от 4 мая 2011 г. № 99–ФЗ «О лицензировании отдельных видов деятельности».

5. Федеральный закон от 30 декабря 2001 г. № 195–ФЗ «Кодекс Российской Федерации об административных правонарушениях».

6. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».

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

8. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно–телекоммуникационных сетей международного информационного обмена».

9. Положение о лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации. Утверждено постановлением Правительства Российской Федерации от 3 марта 2012 г. № 171.

10. Положение о лицензировании деятельности по технической защите конфиденциальной информации. Утверждено постановлением Правительства Российской Федерации от 3 февраля 2012 г. № 79

11. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.

12. Положение о сертификации средств защиты информации по требованиям безопасности информации (с дополнениями в соответствии с постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации»). Утверждено приказом председателя Гостехкомиссии России от 27 октября 1995 г. № 199.

13. Положение по аттестации объектов информатизации по требованиям безопасности информации. Утверждено Гостехкомиссией России 25 ноября 1994 г.

14. Пособие по организации технической защиты информации, составляющей коммерческую тайну. Утверждено ФСТЭК России 25 декабря 2006 г.

15. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.

16. Порядок проведения классификации информационных систем персональных данных. Утвержден приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 г. № 55/86/20.

17. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

18. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 83.

19. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 84.

20. Специальные требования и рекомендации по защите конфиденциальной информации (СТР–К). Утверждены приказом Гостехкомиссии России от 2 марта 2001 г. № 282.

21. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

22. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489.

23. Требования в области технического регулирования к продукции, используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа (требования к средствам антивирусной защиты). Утверждены приказом ФСТЭК России от 20 марта 2012 г. №28.

24. Требования в области технического регулирования к продукции, используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа (требования к средствам доверенной загрузки). Утверждены приказом ФСТЭК России от 27 сентября 2013 г. № 119.

25. Требования в области технического регулирования к продукции, используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа (требования к средствам контроля съемных машинных носителей информации). Утверждены приказом ФСТЭК России от 28 июля 2014 г. № 87.

26. Требования к защите персональных данных при их обработке в информационных системах персональных данных. Утверждены постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119.

27. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.

28. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Утвержден Гостехкомиссией России, 1992.

29. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.

30. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. Утвержден Гостехкомиссией России, 1992.

31. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден приказом председателя Гостехкомиссии России от 4 июня 1999 г. № 114.

32. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 2. Программное обеспечение базовых систем ввода¬вывода персональных электронно–вычислительных машин. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.

33. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Утвержден Гостехкомиссией России, 1992.

34. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Утвержден Гостехкомиссией России, 1992.

35. Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к

информации. Утвержден Гостехкомиссией России, 1997.

36. ГОСТ Р 50922–2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.

37. ГОСТ Р 52069.0–2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.

38. ГОСТ Р 51583–2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.

39. ГОСТ Р 51624–2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000.

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

41. ГОСТ Р 52447–2005 Защита информации. Техника защиты информации. Номенклатура показателей качества. Ростехрегулирование, 2005.

42. ГОСТ РО 0043–003–2012 Защита информации. Аттестация объектов информатизации. Общие положения. Росстандарт, 2012.

43. ГОСТ РО 0043–004–2013 Защита информации. Аттестация объектов информатизации. Программа и методики аттестационных испытаний. Росстандарт, 2013.

44. ГОСТ Р 50543–93 Конструкции базовые несущие. Средства вычислительной техники. Требования по обеспечению защиты информации и электромагнитной совместимости методом экранирования. Госстандарт России, 1993.

45. ГОСТ Р 51 188–98 Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство. Госстандарт России, 1998.

46. ГОСТ Р 51241–98 Защита информации. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний. Госстандарт России, 1998.

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

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

49. 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. Росстандарт, 2012.

50. ГОСТ Р ИСО/МЭК 15408–2–2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности (прямое применение ISO/IEC 15408–2:2008). Росстандарт, 2013.

51. ГОСТ Р ИСО/МЭК 15408–3–2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности (прямое применение ISO/IEC 15408–3:2008). Росстандарт, 2013.

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

53. ГОСТ Р ИСО/МЭК 27001–2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования (на основе прямого применения международного стандарта ИСО/МЭК 27001:2005). Ростехрегулирование, 2006.

54. ГОСТ Р ИСО/МЭК 27002–2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. Росстандарт, 2012.

55. ГОСТ Р ИСО/МЭК 27003–2012 Информационная технология. Методы и средства обеспечения безопасности. Руководство по реализации системы менеджмента информационной безопасности. Росстандарт, 2012.

56. ГОСТ 34.602–89 Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы. Госстандарт СССР, 1990.

57. ГОСТ Р 50739–95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Госстандарт России, 1995.

58. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.

59. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.

60. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.

61. Сборник методических документов по технической защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в волоконно–оптических системах передачи (МД по ТЗИ ВОСП–К). Утвержден приказом ФСТЭК России от 15 марта 2012 г. №27.

62. Временная методика оценки защищенности информации ограниченного доступа, обрабатываемой техническими средствами и системами с элементами беспроводных технологий, от утечки по каналу побочных электромагнитных излучений и наводок. Утверждена ФСТЭК России 21 декабря 2007 г.

Интернет – ресурсы

1. ЭБС «Университетская библиотека онлайн» - http://www.BiblioClub.ru
2. Информационно – справочная поисковая система «Консультант Плюс» - http://www.consultant.ru/
3. Информационно – справочная поисковая система «Гарант» - http://www.garant.ru/

7. Материально-техническое обеспечение производственной практики

Ознакомительные лекции и инструктаж обучающихся во время производственной практики проводятся в помещениях, оборудованных учебной мебелью, досками, экраном, видеопроектором, ноутбуком.

Кроме того, материально-техническая база включает:

1. дидактические материалы – презентационные материалы (слайды); учебные видеозаписи; комплекты схем, настенные стенды.
2. технические средства обучения – аудио-, видео-, фотоаппаратура, иные демонстрационные средства; персональный компьютер, множительная техника (МФУ).
3. программные средства обучения: Текстовый редактор MS Word
4. справочно-правовая система «Консультант плюс».
5. словесные средства обучения: учебники; словари; периодические издания.

По месту прохождения практики в профильной организации обучающимся предоставляется рабочее место, оборудованное необходимыми средствами для работы с документами и подготовки письменных материалов к отчету. Место оснащается средствами вычислительной техники и связи.

Обучающиеся в период прохождения практики:

- выполняют индивидуальные задания, предусмотренные программами практики;
- соблюдают правила внутреннего трудового распорядка;
- соблюдают требования охраны труда и пожарной безопасности.

Защита отчетов по практике проводится в аудиториях, оснащенных мультимедийными средствами обучения, и компьютерных классах с выходом в Интернет.

АНО ВО МОСИ для организации производственной практики располагает необходимой материально-технической базой: собственная библиотека с 17 рабочими местами, оснащенная компьютерами с доступом к базам данных и сети Интернет; доступ к электронно-библиотечной системе «Университетская библиотека-online» (http://www.biblioclub.ru/);

компьютерные классы общего пользования с подключенными к Интернет; компьютерные мультимедийные проекторы в аудиториях и другая техника для презентаций учебного материала.