МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рабочая программа практики

# ПРОИЗВОДСТВЕННАЯ ЭКСПЛУАТАЦИОННАЯ ПРАКТИКА

Специальность и специализация
10.05.03 Информационная безопасность автоматизированных систем. Безопасность открытых информационных систем

Год набора на ОПОП
2026

Форма обучения
очная

Вид практики: производственная
Тип практики: эксплуатационная практика

Владивосток 2026

Программа практики «Производственная эксплуатационная практика» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем (утв. приказом Минобрнауки России от 26.11.2020г. №1457) и Порядком организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры (утв. приказом Минобрнауки России от 06.04.2021 г. N245).; Положением по практике обучающихся, осваивающих основные профессиональные образовательные программы высшего образования (утв. приказом Минобрнауки России от 05.08.2020г. N 390).'

Составитель(и):

*Белёв А.В.*

*Долгачев М.В.*

*Етчо С.А.*

*Шумик Е.Г.*

Утверждена на заседании кафедры информационной безопасности от 14.05.2026 , протокол № 8

СОГЛАСОВАНО:

Заведующий кафедрой (разработчика)

Шумик Е.Г.

| ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ | |
|---|---|
| Сертификат | eg_1575874368 |
| Номер транзакции | 0000000000FBCB0A |
| Владелец | Шумик Е.Г. |

Заведующий кафедрой (выпускающей) _____ _____

*подпись* *фамилия, инициалы*

## 1 Цель и планируемые результаты обучения при прохождении практики, соотнесенные с планируемыми результатами освоения ОПОП ВО

Развитие практических навыков в сфере обеспечения информационной безопасности путем участия в реальных проектах, адаптации к корпоративной культуре и освоении особенностей среды и инфраструктуры конкретной организации.

Ознакомление с действующими системами защиты информации предприятия:

Изучить внутреннюю документацию и нормативно-правовые акты предприятия, касающиеся вопросов информационной безопасности.

Провести инвентаризацию и описать существующие средства защиты информации (антивирусные программы, брандмауэр, системы резервного копирования и восстановления данных).

Участие в проведении обследования и анализа угроз информационной безопасности:

Участвовать в формировании карты информационных рисков и угроз для конкретной системы или сервиса предприятия.

Проводить мониторинг инцидентности и составлять отчёты по зафиксированным событиям.

По итогам прохождения практики обучающийся должен продемонстрировать результаты обучения (знания, умения, навыки), соотнесенные с планируемыми результатами освоения ОПОП ВО, приведенные в таблице 1.

Таблица 1 – Компетенции, формируемые в результате прохождения практики

| Название ОПОП ВО, сокращенное | Код и формулировка компетенции | Код и формулировка индикатора достижения компетенции | Результаты обучения по дисциплине | | |
|---|---|---|---|---|---|
| | | | Код результата | Формулировка результата | |
| 10.05.03 «Информационная безопасность автоматизированных систем» (ИБ) | ОПК-14 : Способен осуществлять разработку, внедрение и эксплуатацию автоматизированных систем с учетом требований по защите информации, проводить подготовку исходных данных для технико-экономического обоснования проектных решений | ОПК-14.2к : Представляет проектные решения систем защиты, оформлять проектную документацию и проводит оценку их технико-экономического обоснования. | РД1 | Умение | анализировать проектные решения систем защиты и выявлять основные угрозы |
| | | | РД2 | Умение | оформлять проектную документацию и проводить оценку предложенных решений |
| | | | РД3 | Навык | разработки проектов необходимой документации и отчетов |
| | ОПК-15 : Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности | ОПК-15.1к : Перечисляет этапы разработки политики информационной безопасности для организации; особенности подсистем защиты ОС Windows и | РД4 | Умение | выделить этапы разработки политики информационной безопасности для организации |
| | | | РД5 | Навык | работы с подсистемами защиты ОС Windows и Linux |

| | | | | | |
|---|---|---|---|---|---|
| | автоматизированных систем | Linux; стандартные средства организации виртуальных частных сетей | | | |

## 2 Вид практики, способы и формы её проведения

Вид практики: производственная
Тип практики: эксплуатационная практика
Способ проведения практики: стационарная
Форма проведения практики: Дискретно по видам практики

## 3 Объем практики и ее продолжительность

Объем практики в зачетных единицах с указанием семестра (ОФО)/ курса (ЗФО, ОЗФО) и продолжительности практики по всем видам обучения, приведен в таблице 2.

Таблица 2 – Общая трудоемкость практики

| Название ОПОП ВО | Форма обучения | Часть УП | Семестр/ курс | Трудоемкость (з.е.) | Продолжительность практики |
|---|---|---|---|---|---|
| 10.05.03 Информационная безопасность автоматизированных систем. Безопасность открытых информационных систем | ОФО | С2.Б.П.1 | 8 | 5 | 5 (недель) |

## 4 Место практики в структуре ОПОП ВО

Входными требованиями, необходимыми для освоения программы практики, является наличие у обучающихся компетенций, сформированных при изучении дисциплин и/или прохождении практик «Аудит информационной безопасности», «Безопасность вычислительных сетей», «Безопасность операционных систем», «Безопасность систем баз данных». На данную практику опираются «инженерная защита объектов».

## 5 Содержание практики

### 5.1 Структура (этапы) прохождения практики

Расширенное содержание практики, структурированное по разделам и видам работ с указанием основных действий и последовательности их выполнения, приведено в таблице 3

Таблица 3 – Содержание практики для студентов ОФО

| Этапы практики | Виды работ на практике, включая контактную и иные формы | Содержание и распределение бюджета времени по видам работ | | Форма текущего контроля |
|---|---|---|---|---|
| | | Основные действия | Кол-во часов. | |

| | | | | |
|---|---|---|---|---|
| 1. Подготовительный | Организационное собрание | ознакомление с особенностями прохождения практики;<br>согласование рабочего графика (плана) практики;<br>получение индивидуального задания на практику. | 2 | Задание, согласованное с руководителем практики от предприятия |
| | Инструктаж по технике безопасности | ознакомление с правилами безопасности при выполнении работ;<br>общее ознакомление с технологическим процессом на данном участке работы;<br>ознакомление с опасными зонами работ. | | Отметка в рабочем графике (плане) практики |
| 2. Практический | Общее ознакомление с организацией | Изучение организационного строения предприятия (организаций), назначения отдельных подразделений и служб, а также их взаимодействия. | 6 | Отметка в рабочем графике (плане) практики<br>Отчет по практике |
| | Ознакомление с действующими системами защиты информации предприятия | Изучить внутреннюю документацию и нормативно-правовые акты предприятия, касающиеся вопросов информационной безопасности.<br>Провести инвентаризацию и описать существующие средства защиты информации (антивирусные программы, брандмауэр, системы резервного копирования и восстановления данных). | 42 | Отметка в рабочем графике (плане) практики<br>Отчет по практике |
| | Участие в проведении обследования и анализа угроз информационной безопасности | Участвовать в формировании карты информационных рисков и угроз для конкретной системы или сервиса предприятия.<br>Проводить мониторинг инцидентности и составлять отчёты по зафиксированным событиям. | 42 | Отметка в рабочем графике (плане) практики<br>Отчет по практике |
| | Создание рекомендательных материалов по укреплению информационной безопасности | разработать проектную документацию, содержащую рекомендации по выбору и применению дополнительных средств защиты информации. | 40 | Отметка в рабочем графике (плане) практики<br>Отчет по практике |
| | | обосновать необходимость установки или модификации определенных средств защиты (базовая настройка firewall, политика паролей, использование VPN-технологий). | 14 | Отметка в рабочем графике (плане) практики<br>Отчет по практике |
| | | Проверить наличие следов несанкционированного доступа и предпринять соответствующие профилактические меры. | 30 | Отметка в рабочем графике (плане) практики<br>Отчет по практике |
| | | Оформление проектных решений и проведение их технико-экономического обоснования | 22 | Отметка в рабочем графике (плане) практики<br>Отчет по практике |

| | | | | |
|---|---|---|---|---|
| 3. Заключительный | Подготовка и сдача отчета | Оформление результатов прохождения практики в соответствии с требованиями, представление результатов руководителю, защита отчета | 20 | Защита отчета по практике (ПА) |

- Подготовительный этап: Практика студента осуществляется на основе договора между Университетом и организациями, деятельность которых соответствует профессиональным компетенциям, осваиваемым в рамках образовательной программы. Сроки и содержание практики определяются утвержденными учебными планами и рабочей программой. Методическое руководство практикой осуществляет руководитель практики, назначенный приказом. Инструктаж обучающихся включает: ознакомление с требованиями охраны труда, техники безопасности, пожарной безопасности, правилами внутреннего трудового распорядка и проводится на предприятии.

- Практический:

1. Участие в разработке и оформлении внутренней политики информационной безопасности предприятия:
Анализ существующих корпоративных инструкций и процедур;
Выделение ключевых положений по ограничениям доступа к внутренним базам данных и системам;
Предоставление предложений по внесению изменений в действующие регламентирующие документы;
2. Аудит существующей системы защиты информации на платформе Windows
3. Тестирование механизма VPN-подключения и настройка защищённого соединения
4. Оценка экономического эффекта предложенных мер по усилению защиты
3. Заключительный этап. Включает подготовку и защиту отчета. В отчете представляются материалы выполнения заданий практики. Составление отчета по практике, состоит в компьютерном оформлении и письменном представлении материалов практики; Защита отчета по практике включает краткий доклад, продолжительностью 3 - 5 мин, ответы на вопросы.

**5.2 Задание на практику**

Определяется в соответствии с спецификой деятельности организации и ВКР совместно с руководителем практики от кафедры.

МИНОБРНАУКИ РОССИИ
ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (ВГУЭС)
КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЗАДАНИЕ
на производственную преддипломную практику
Студенту:
Группы:
Срок сдачи:

Содержание отчета по учебной практике по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности

**Введение:** определить цель и задачи практики, основные методы, необходимые для достижения.

**Раздел 1 Общая характеристика организации**

Общее ознакомление с организацией

- наименование организации, организационно-правовая форма, месторасположение, сфера, виды и масштабы деятельности.

-изучение организационного строения базовых предприятий (организаций), назначения отдельных подразделений и служб, а также их взаимодействия.

**Раздел 2 Практический**

1. Участие в разработке и оформлении внутренней политики информационной безопасности предприятия:

Анализ существующих корпоративных инструкций и процедур;

Выделение ключевых положений по ограничениям доступа к внутренним базам данных и системам;

Предоставление предложений по внесению изменений в действующие регламентирующие документы;

2. Аудит существующей системы защиты информации на платформе Windows

3. Тестирование механизма VPN-подключения и настройка защищённого соединения

4. Оценка экономического эффекта предложенных мер по усилению защиты

**Список использованных источников (не менее 15-ти позиций)** с использованием профессиональных баз данных и профессиональных Интернет-ресурсов, в том числе источников на иностранных языках.

## 6 Формы отчетности по практике

По окончании практики студенты должны представить на кафедру отчет о прохождении практики в полном соответствии с программой практики и индивидуальным заданием. Отчет должен соответствовать содержанию практики и индивидуальному заданию. Отчет должен быть подписан студентом, руководителем практики от кафедры, руководителем практики от предприятия и заверен на титульном листе печатью предприятия. К отчету по учебной практике должны быть приложены в обязательном порядке:

1. Рабочий график (план) проведения практики студента ВВГУ;
2. Отзыв-характеристика руководителя практики от предприятия (отзыв должен содержать описание проделанной студентом работы, общую оценку качества его профессиональной подготовки, умение работать в команде, анализировать ситуацию, работать с данными и т.д.);
3. Индивидуальное задание на практику от руководителя кафедры согласованное с руководителем практики от предприяти;

Объем отчета о прохождении практики должен составлять от 20 до 30 печатных страниц (без приложений). Работа оформляется шрифтом Times New Roman (далее: TNR) (размер 12), межстрочный интервал 1,5 остальная текстовая часть работы должна соответствовать требованиям, изложенным в стандарте ВВГУ «Требования к оформлению текстовой части выпускных квалификационных работ, курсовых работ (проектов), рефератов, контрольных работ, отчетов по практикам, лабораторным работам». В приложения к отчету по практике включаются различные документы, раскрывающие специфику деятельности организации, в которой студент проходил практику, характер работы, выполняемой студентом, его достижения.

Это могут быть:

– различные нормативные документы,

– внутренние документы организации и подразделения, где студент проходил практику, скриншоты интерфейса программного обеспечения в области информационной безопасности (публикуется только при получении разрешения от руководителя предприятия). Все приложения должны быть пронумерованы.

В текстовой части отчета по практике должны быть ссылки на соответствующие приложения.

По окончании практики руководитель практики от организации составляет на студента отзыв характеристику, подписывает ее и заверяет печатью.

Аттестация обучающегося по итогам прохождения практики проводится только после сдачи документов по практике на кафедру и фактической защиты отчета. Отчет, удовлетворяющий предъявляемым требованиям к содержанию и оформлению, после исправления замечаний руководителя (если они имеются) допускается к защите. Защита отчета по практике, как правило, представляет собой краткий, 3–5-минутный доклад студента и его ответы на вопросы комиссии. По итогам защиты практики выставляется оценка, о чем делаются соответствующие записи в аттестационной ведомости и зачетной книжке. Эта оценка приравнивается к оценкам по теоретическому обучению и учитывается при подведении итогов общей успеваемости студентов.

При оценивании студента учитываются также: деятельность студента в период практики (степень полноты выполнения программы практики, овладение основными профессиональными умениями и навыками); содержание отзыва- характеристики, содержание и качество оформления отчета, качество доклада и ответы студента на вопросы во время защиты отчета. РАБОТЫ, ОФОРМЛЕННЫЕ НЕ ПО ТРЕБОВАНИЯМ К ЗАЩИТЕ НЕ ДОПУСКАЮТСЯ. При подготовке текста отчета необходимо обратить особое внимание на стиль речи. Он не должен быть публицистическим. Аналитические записки, справки и доклады отличает лаконичность формулировок, безличный стиль, наличие четкой структуры, минимальная описательность, ориентация на прикладную значимость выводов. В отчете не допускаются формулировки с использованием личных местоимений (Я, моё, мне, мною и т.д.)

Отчет подписывается студентом и сдается на выпускающую кафедру за два-три для до даты защиты. Руководитель проверяет отчет, оценивая содержание и оформление, делая на титульном листе запись о допуске/не допуске студента к защите отчета. При необходимости отчет может быть возвращён студенту на доработку. Отчет, в том числе и доработанный студентом, как и все письменные работы студентов проверяются преподавателем в течение 3-х рабочих дней. Защита проводится комиссионно

## 7 Организация практики и методические рекомендации по выполнению заданий

Практика проводится в структурном подразделении университета или профильной организации, с которой у университета заключен договор о проведении данного вида практики. Практика предполагает закрепление и углубление теоретических знаний, полученных в ходе учебного процесса.

Руководитель практики от кафедры:

1. проводит организационное собрание, на котором знакомит студентов с особенностями проведения и с содержанием практики;
2. выдает студенту индивидуальное задание на практику и рабочий график (план);
3. осуществляет контроль за соблюдением сроков проведения практики;
4. осуществляет контроль за соответствием содержания практики установленным требованиям;
5. оказывает методическую помощь (консультирование) обучающимся при выполнении ими индивидуальных заданий;

6. по окончанию практики проводит промежуточную аттестацию в форме защиты отчета по практике;
7. участвует в распределении обучающихся по рабочим местам и видам работ в организации;
8. осуществляет контроль за соблюдением сроков проведения практики и соответствием ее содержания требованиям, установленным ОПОП ВО;
9. выставляет результат промежуточной аттестации в аттестационную ведомость и зачетную книжку студента.

Ответственный от профильной организации или структурного подразделения университета, в котором проходит практику студент:

1. совместно с руководителем практики от образовательной организации разрабатывает рабочий график (план) проведения практики;
2. согласовывает индивидуальные задания, содержание и планируемые результаты практики; - предоставляет студентам рабочее место;
3. проводит инструктаж обучающихся по ознакомлению с требованиями охраны труда, техники безопасности, пожарной безопасности, а также правилами внутреннего трудового распорядка;
4. принимает выполненную работу студента; - оказывает методическую помощь (консультирование) обучающимся при выполнении ими индивидуальных заданий;
5. оценивает результаты прохождения практики обучающимися (отзыв о прохождении практики), Приложение 3. (Отзыв прилагается к отчету по практике).

Студент:

1. предоставляет заявление на практику специалисту кафедры за 3 недели до начала практики;

1. предоставляет договор на практику (в двух экземплярах) в случае прохождения практики на базе не из перечня предприятий – партнеров ВВГУ за 3 недели до начала практики;
2. присутствует на организационном собрании по практике;
3. выполняет задание, полученное от руководителя практики в соответствии с установленными сроками;
4. по завершению практики представляет результаты практики в виде отчета руководителю.
5. соблюдает правила внутреннего трудового распорядка;
6. соблюдает требования охраны труда и пожарной безопасности. Имеет право:
7. получать всю необходимую информацию об организации практики в университете;
8. вносить свои предложения по совершенствованию содержания практики

**Особенности организации обучения для лиц с ограниченными возможностями здоровья и инвалидов**

Практика для обучающихся с ограниченными возможностями здоровья и инвалидов проводится с учетом особенностей их психофизического развития, индивидуальных возможностей и состояния здоровья.

## 8 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по практике

В соответствии с требованиями ФГОС ВО для аттестации обучающихся на соответствие их персональных достижений планируемым результатам обучения по практике созданы фонды оценочных средств (Приложение 1).

## 9 Учебно-методическое и информационное обеспечение практики

### *9.1 Основная литература*

1. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2025. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/562070 (дата обращения: 01.09.2025).

2. Карабцев, С. Н. Операционные системы : учебное пособие / С. Н. Карабцев, В. В. Торгулькин. — Кемерово : КемГУ, 2025 — Часть 2 : Операционные системы семейства Linux — 2025. — 208 с. — ISBN 978-5-8353-3118-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/485072 (дата обращения: 25.05.2026). — Режим доступа: для авториз. пользователей.

3. Козырь, Н. С. Аудит информационной безопасности : учебник для вузов / Н. С. Козырь. — Москва : Издательство Юрайт, 2025. — 36 с. — (Высшее образование). — ISBN 978-5-534-20647-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/581505 (дата обращения: 01.09.2025).

### *9.2 Дополнительная литература*

1. Маршаков Д.В., Фатхи Д.В. Методы и средства криптографической защиты информации. Практический курс : Учебное пособие [Электронный ресурс] : НИЦ ИНФРА-М , 2022 - 76 - Режим доступа: https://znanium.com/catalog/document?id=414013

2. Сборник практических занятий для дисциплины безопасность операционных систем: Практикум : учебное пособие / О. В. Трубиенко, Г. Ю. Потерпеев, В. Е. Петров, Д. П. Абрамов. — Москва : РТУ МИРЭА, 2024 — Часть 2— 2024. — 79 с. — ISBN 978-5-7339-2277-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/448808 (дата обращения: 25.05.2026). — Режим доступа: для авториз. пользователей.

### *9.3 Ресурсы информационно-телекоммуникационной сети "Интернет", включая профессиональные базы данных и информационно-справочные системы (при необходимости):*

1. Образовательная платформа "ЮРАЙТ"
2. Электронная библиотечная система ZNANIUM.COM - Режим доступа: https://znanium.com/
3. Электронно-библиотечная система "ЛАНЬ"
4. Open Academic Journals Index (OAJI). Профессиональная база данных - Режим доступа: http://oaji.net/
5. Президентская библиотека им. Б.Н.Ельцина (база данных различных профессиональных областей) - Режим доступа: https://www.prlib.ru/
6. Информационно-справочная система "Консультант Плюс" - Режим доступа: http://www.consultant.ru/

**10 Описание материально-технической базы, необходимой для проведения практики, и перечень информационных технологий, используемых при проведении практики, включая перечень программного обеспечения (при необходимости)**

Основное оборудование:

- Компьютеры
- Проектор

Программное обеспечение:

- Microsoft Office Professional Plus 2010
- Microsoft Windows 10 Home SL

МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Фонд оценочных средств
для проведения текущего контроля
и промежуточной аттестации по практике

# ПРОИЗВОДСТВЕННАЯ ЭКСПЛУАТАЦИОННАЯ ПРАКТИКА

Специальность и специализация
10.05.03 Информационная безопасность автоматизированных систем. Безопасность открытых информационных систем

Год набора на ОПОП
2026

Форма обучения
очная

Владивосток 2026

## 1 Перечень формируемых компетенций

| Название ОПОП ВО, сокращенное | Код и формулировка компетенции | Код и формулировка индикатора достижения компетенции |
|---|---|---|
| 10.05.03 «Информационная безопасность автоматизированных систем» (ИБ) | ОПК-14 : Способен осуществлять разработку, внедрение и эксплуатацию автоматизированных систем с учетом требований по защите информации, проводить подготовку исходных данных для технико-экономического обоснования проектных решений | ОПК-14.2к : Представляет проектные решения систем защиты, оформлять проектную документацию и проводит оценку их технико-экономического обоснования. |
| | ОПК-15 : Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем | ОПК-15.1к : Перечисляет этапы разработки политики информационной безопасности для организации; особенности подсистем защиты ОС Windows и Linux; стандартные средства организации виртуальных частных сетей |

Компетенция считается сформированной на данном этапе в случае, если полученные результаты обучения по дисциплине оценены положительно (диапазон критериев оценивания результатов обучения «зачтено», «удовлетворительно», «хорошо», «отлично»). В случае отсутствия положительной оценки компетенция на данном этапе считается несформированной.

## 2 Показатели оценивания планируемых результатов обучения

**Компетенция ОПК-14** «Способен осуществлять разработку, внедрение и эксплуатацию автоматизированных систем с учетом требований по защите информации, проводить подготовку исходных данных для технико-экономического обоснования проектных решений»

Таблица 2.1 – Критерии оценки индикаторов достижения компетенции

| Код и формулировка индикатора достижения компетенции | Результаты обучения по дисциплине | | | Критерии оценивания результатов обучения |
|---|---|---|---|---|
| | Код рез-та | Тип рез-та | Результат | |
| ОПК-14.2к : представляет проектные решения систем защиты, оформлять проектную документацию и проводит оценку их технико-экономического обоснования. | РД 1 | Умение | анализировать проектные решения систем защиты и выявлять основные угрозы | выполнение практических заданий |
| | РД 2 | Умение | оформлять проектную документацию и проводить оценку предложенных решений | выполнение заданий практики |
| | РД 3 | Навык | разработки проектов необходимой документации и отчетов | выполнение заданий практики |

**Компетенция ОПК-15** «Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем»

Таблица 2.2 – Критерии оценки индикаторов достижения компетенции

| Код и формулировка индикатора достижения компетенции | Результаты обучения по дисциплине | | | Критерии оценивания результатов обучения |
|---|---|---|---|---|
| | Код рез-та | Тип рез-та | Результат | |
| ОПК-15.1к : перечисляет этапы разработки политики информационной безопасности для организации; особенности подсистем защиты ОС Windows и Linux; стандартные средства организации виртуальных частных сетей | РД 4 | Умение | выделить этапы разработки политики информационной безопасности для организации | выполнение практических заданий |
| | РД 5 | Навык | работы с подсистемами защиты ОС Windows и Linux | выполнение заданий практики |

Таблица заполняется в соответствии с разделом 1 Рабочей программы дисциплины (модуля).

## 3 Перечень оценочных средств

Таблица 3 – Перечень оценочных средств по практике

| Контролируемые планируемые результаты обучения | | Наименование оценочного средства и представление его в ФОС | |
|---|---|---|---|
| | | Текущий контроль | Промежуточная аттестация |
| РД1 | Умение : анализировать проектные решения систем защиты и выявлять основные угрозы | Отчет | Устная защита |
| РД2 | Умение : оформлять проектную документацию и проводить оценку предложенных решений | Отчет | Устная защита |
| РД3 | Навык : разработки проектов необходимой документации и отчетов | Отчет | Устная защита |
| РД4 | Умение : выделить этапы разработки политики информационной безопасности для организации | Отчет | Устная защита |
| РД5 | Навык : работы с подсистемами защиты ОС Windows и Linux | Отчет | Устная защита |

## 4 Описание процедуры оценивания

Качество сформированности компетенций на данном этапе оценивается по результатам текущих и промежуточных аттестаций при помощи количественной оценки, выраженной в баллах. Максимальная сумма баллов по практике равна 100 баллам.

| Оценочное средство | | Итого |
|---|---|---|
| Отчет по практике | Защита отчета | |
| 50 | | 50 |
| | 50 | 50 |

| | | |
|---|---|---|
| 50 | 50 | 100 |

Сумма баллов, набранных студентом по всем видам учебной деятельности в рамках дисциплины, переводится в оценку в соответствии с таблицей.

| Сумма баллов по дисциплине | Оценка по промежуточной аттестации | Характеристика качества сформированности компетенции |
|---|---|---|
| от 91 до 100 | «зачтено» / «отлично» | Студент демонстрирует сформированность дисциплинарных компетенций, обнаруживает всестороннее, систематическое и глубокое знание учебного материала, усвоил основную литературу и знаком с дополнительной литературой, рекомендованной программой, умеет свободно выполнять практические задания, предусмотренные программой, свободно оперирует приобретенными знаниями, умениями, применяет их в ситуациях повышенной сложности. |
| от 76 до 90 | «зачтено» / «хорошо» | Студент демонстрирует сформированность дисциплинарных компетенций: основные знания, умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации. |
| от 61 до 75 | «зачтено» / «удовлетворительно» | Студент демонстрирует сформированность дисциплинарных компетенций: в ходе контрольных мероприятий допускаются значительные ошибки, проявляется отсутствие отдельных знаний, умений, навыков по некоторым дисциплинарным компетенциям, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации. |
| от 41 до 60 | «не зачтено» / «неудовлетворительно» | У студента не сформированы дисциплинарные компетенции, проявляется недостаточность знаний, умений, навыков. |
| от 0 до 40 | «не зачтено» / «неудовлетворительно» | Дисциплинарные компетенции не сформированы. Проявляется полное или практически полное отсутствие знаний, умений, навыков. |

## 5 Примерные оценочные средства

### 5.1 устная защита

Какие основные задачи стояли перед вами в ходе практики?

Каково ваше общее впечатление о месте прохождения практики?

Какие навыки вы приобрели и чему научились в результате прохождения практики?

Какие стандарты и нормы обеспечивали информационную безопасность на предприятии?

Какое программное обеспечение использовалось для защиты информации на предприятии?

Как организованы процессы резервного копирования и восстановления данных?

Какие угрозы информационной безопасности вы выявили в ходе своей работы?

Каковы были причины возникновения выявленных угроз?

Какие меры предложили вы для снижения выявленных рисков?

Какие рекомендации вы подготовили для укрепления информационной безопасности предприятия?

Каким образом осуществляется проверка правомерности действий пользователей?

Почему вы решили включить именно эти меры в свою разработку?

Какую реальную меру защиты вы провели сами?

Какие инструменты использовали для выполнения своего проекта?

Возникли ли сложности при реализации вашего предложения?

Какие экономические показатели были использованы для оценки эффективности предлагаемых мер?

Сколько примерно потребуется средств на реализацию ваших предложений?

Чего ожидать от предложенных мер по снижению убытков вследствие нарушений информационной безопасности?

*Краткие методические указания*

Для ответов на поставленные вопросу студенту необходимо максимально полно ознакомиться как с практическим, так и с теоретическими аспектами исследования

*Шкала оценки*

| Оценка | Баллы* | Описание |
|---|---|---|
| 5 | 40-50 | Раскрыты ответы на вопросы |
| 4 | 20-39 | Ответы корректные, но не полные не может обосновать выбранную позицию |
| 3 | 10-19 | Ответы ошибочны |
| 2 | 0-9 | Ответы на вопрос не даны |