МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
**«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**
**(МОСКОВСКИЙ ПОЛИТЕХ)**

Факультет информационных технологий

УТВЕРЖДАЮ
Декан факультета
информационных технологий
/Д. Г. Демидов/
"28" апреля 2022 г.

# РАБОЧАЯ ПРОГРАММА ПРАКТИКИ

# Производственная практика (проектно-технологическая)

Направление подготовки
**10.04.01 «Информационная безопасность»**

Профиль
**«Системы управления информационной безопасностью»**

Квалификация
**Магистр**

Формы обучения
**Очная**

Москва, 2022 г.

**Разработчик(и):**

Доцент, к.т.н., доцент  /И.В. Калуцкий/

**Согласовано:**

И.о. заведующего кафедрой «Информационная безопасность»,  А.Ю. Гневшев

Руководитель образовательной программы
Доцент. к.т.н.  /С.А. Кесель/

# Содержание

## 1 Цели, задачи и планируемые результаты прохождении практики

Цель практики закрепление и углубление теоретических знаний, полученных студентами при изучении дисциплин, относящихся к профессиональному циклу и дисциплин специализации при реализации и внедрении системы информационной безопасности на предприятии, а также приобретение и развитие необходимых практических навыков и умений при реализации и внедрении системы информационной безопасности в соответствии с требованиями к уровню подготовки выпускников.

Задачи практики:

- получение практических навыков при реализации и внедрении средств защиты информационно-технологических ресурсов автоматизированной системы на предприятии;
- получение практических навыков эксплуатации средств защиты информационно-технологических ресурсов автоматизированной системы на предприятии;
- овладение методов и средств, связанных с реализацией частных политик информационной безопасности автоматизированной системы,
- осуществление мониторинга и аудита безопасности автоматизированной системы на предприятии.

Планируемые результаты обучения должны соотноситься с установленными в ОПОП ВО индикаторами достижения компетенций.

Программа составлена в соответствии с требованиями ФГОС ВО с учетом рекомендаций и ООП ВО по направлению подготовки 10.04.01 «Информационная безопасность».

Компетенции обучающегося, формируемые в результате прохождения «производственной практики (проектно-технологической)»:

| Код и наименование компетенций | Индикаторы достижения компетенции |
|---|---|
| УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий | ИУК-1.1. Анализирует проблемную ситуацию как систему, осуществляет её декомпозицию и определяет связи между ее составляющими.<br>ИУК-1.2. Определяет противоречивость и пробелы в информации, необходимой для решения проблемной ситуации, а также критически оценивает релевантность используемых информационных источников. |

| | |
|---|---|
| | ИУК-1.3. Разрабатывает и содержательно аргументирует стратегию решения проблемной ситуации на основе системного и междисциплинарного подходов с учетом оценки существующих рисков и возможностей их минимизации. |
| УК-2. Способен управлять проектом на всех этапах его жизненного цикла | ИУК-2.1. Разрабатывает концепцию управления проектом на всех этапах его жизненного цикла в рамках обозначенной проблемы: формулирует цель и пути достижения, задачи и способы их решения, обосновывает актуальность, значимость, ожидаемые результаты и возможные сферы их применения.<br>ИУК-2.2. Разрабатывает план реализации проекта в соответствии с существующими условиями, необходимыми ресурсами, возможными рисками и распределением зон ответственности участников проекта.<br>ИУК-2.3. Осуществляет мониторинг реализации проекта на всех этапах его жизненного цикла, вносит необходимые изменения в план реализации проекта с учетом количественных и качественных параметров достигнутых промежуточных результатов |
| УК-3. Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели | ИУК-3.1. Демонстрирует управленческую компетентность, необходимую для формирования команды и руководства ее работой на основе разработанной стратегии сотрудничества.<br>ИУК-3.2. Планирует, организует, мотивирует, оценивает и корректирует совместную деятельность по достижению поставленной цели с учетом интересов, особенностей поведения и мнений ее членов.<br>ИУК-3.3. Применяет способы, методы и стратегии оптимизации социально-психологического климата в коллективе, предупреждения и разрешения конфликтов, технологии обучения и развития профессиональной |

| | |
|---|---|
| | и коммуникативной компетентности членов команды |
| ПК-1. Способен анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты | ИПК-1.1. Применяет знания направлений развития информационных технологий, основных видов политик безопасности объектов защиты;<br>ИПК-1.2. Умеет прогнозировать эффективность функционирования, оценивать затраты и риски объектов защиты;<br>ИПК-1.3. Владеет навыками формирования политики безопасности объектов защиты |
| ПК-2. Способен разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности | ИПК-2.1. Знает методы концептуального проектирования технологий обеспечения информационной безопасности;<br>ИПК-2.2. Умеет применять методы разработки систем, комплексов, средств и технологий обеспечения информационной безопасности;<br>ИПК-2.3. Владеет навыками разработки систем, комплексов, средств и технологий обеспечения информационной безопасности; |
| ПК-3. Способен проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов | ИПК-3.1. Знает:<br>отечественные и международные стандарты информационной безопасности; основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; основные методы и средства обеспечения безопасности операционных систем; основные методы и средства обеспечения сетевой безопасности; основные методы и средства обеспечения безопасности в системах управления базами данных.<br>ИПК-3.2. Умеет:<br>обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности объекта защиты;<br>осуществлять выбор функциональной структуры системы обеспечения информационной безопасности. |

| | |
|---|---|
| | ИПК-3.3. Владеет:<br>навыками применения отечественных и международных стандартов информационной безопасности для обоснования состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты;<br>-навыками настройки подсистем защиты основных операционных систем. |
| ПК-4. Способен разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности | ИПК-4.1. Знает: программы и методики испытаний средств и систем обеспечения информационной безопасности в соответствии с нормативными актами.<br>ИПК-4.2. Умеет: разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности<br>ИПК-4.3. Владеет: навыками проведения испытаний средств и систем обеспечения информационной безопасности |
| ПК-15. Способен организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности | ИПК-15.1. Знает методы ввода в эксплуатацию систем и средства обеспечения информационной безопасности.<br>ИПК-15.2. Умеет: организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности.<br>ИПК-15.3. Владеет методами организации выполнения работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности |

## 2 Место практики в структуре образовательной программы

Производственная (проектно-технологическая) практика относится к числу обязательных

практик учебного плана по направлению подготовки 10.04.01 «Информационная безопасность» профиля «Системы управления информационной безопасностью».

Производственная (проектно-технологическая) практика базируется на знаниях и компетенциях, полученных в магистратуре при изучении дисциплин «Защита информации в

системах обработки данных» (Б1.1.2), «Организационное и правовое обеспечение информационной безопасности» (Б1.1.3), «Управление информационной безопасностью» (Б1.1.5), «Проектирование организационно-распорядительных документов по обеспечению информационной безопасности» (Б1.1.6), «Научно-исследовательская и проектная деятельность» (Б1.2.5), «Аудит систем управления информационной безопасностью» (Б1.2.3), «Стратегии управления информационной безопасностью» (Б1.2.4), «Программно-аппаратные средства защиты информации» (Б1.2.ЭД.1.1), «Методы и средства криптографической защиты информации» (Б1.2.ЭД.1.2), «Защита информации в автоматизированных системах управления технологическими процессами» (Б1.2.ЭД.2.1), «Защита информации от утечки по техническим каналам» (Б1.2.ЭД.2.2).

Компетенции, полученные при прохождении производственной (проектно-технологической) практики, являются необходимыми при прохождении производственной эксплуатационной практики (Б2.1.1), производственной практики (научно-исследовательской работы) (Б2.1.2), подготовке и защите Выпускной квалификационной работы (ВКР) (Б3.1).

## 3 Характеристика практики

Тип и вид практики – производственная, проектно-технологическая

## 4 Структура и содержание практики

4.1 Общая трудоемкость практики составляет 6 зачетных(е) единиц(ы) (____ недель).

| **№ п/п** | **Разделы (этапы) практики** | **Виды работ на практике, включая самостоятельную работу студентов и трудоемкость (в зачетных единицах, часах)** | | | **Формы текущего контроля** |
|---|---|---|---|---|---|
| | | Виды работ | ЗЕТ | час | |
| 1 | Установка и настройка средств защиты информации в автоматизированной системе | Эксплуатационная документация на систему защиты информации автоматизированной системы, руководство администратора и пользователя средств защиты информации. | 1 | 36 | Раздел отчета. Установка и настройка средств защиты информации |
| 2 | Разработка документов, определяющих мероприятия, | Перечень лиц, имеющих доступ к объектам защиты информационной системы, и их права (привилегии) доступа к этим объектам, а также | 1 | 36 | Раздел отчета. Документы, определяющ |

| | | | | | |
|---|---|---|---|---|---|
| | проводимые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации | перечень лиц, имеющих доступ в помещения, в которых расположены технические средства обработки информации.<br>Состав организационных мер и порядок их реализации.<br>Порядок учета, хранения и использования съемных машинных носителей информации.<br>Порядок вывода информации на внешние носители информации.<br>Правила и порядок генерации, смены и восстановления паролей пользователей, заведения и удаления учетных записей пользователей.<br>Порядок выявления инцидентов, связанных с нарушениями требований о защите информации, и реагирования на эти инциденты.<br>Порядок обслуживания системы защиты информации обслуживающим персоналом. | | | их мероприятия, проводимые оператором. |
| 3 | Внедрение организационных мер в информационной системе. | Реализация в соответствии с организационно-распорядительными документами по защите информации правил, регламентирующих права доступа субъектов доступа к объектам доступа (далее - правила разграничения доступа), и введение ограничений на действия пользователей и обслуживающего персонала, а так же на изменение условий эксплуатации, состава и конфигурации технических средств обработки информации и программного обеспечения. Проверка полноты и детальности описания в организационно-распорядительных документах по защите информации действий пользователей и администраторов информационной системы по реализации организационных мер.<br>Отработка действий должностных лиц и подразделений, | 1 | 36 | Раздел отчета. Документы по организационным мерам. |

| | | | | | |
|---|---|---|---|---|---|
| | | ответственных за реализацию организационных мер. | | | |
| 4 | Предварительные испытания системы защиты информации информационной системы | Проверка работоспособности системы защиты информации информационной системы, а также принятие решения о возможности опытной эксплуатации системы защиты информации информационной системы. | 1 | 36 | Раздел отчета. Предварительные испытания системы защиты информации информационной системы. |
| 5 | Опытная эксплуатация системы защиты информации информационной системы.<br>Анализ уязвимостей информационной системы | Проверка функционирования системы защиты информации информационной системы, в том числе реализованных мер по защите информации, а также готовность пользователей и администраторов к эксплуатации системы защиты информации информационной системы. Оценка возможности преодоления нарушителем системы защиты информации информационной системы и предотвращения реализации угроз безопасности информации.<br>Средства контроля (анализа) защищенности информации.<br>Анализ уязвимостей средств защиты информации, технических средств обработки информации и программного обеспечения информационной системы.<br>Правильность установки и настройки средств защиты информации, технических средств обработки информации и программного обеспечения, а также корректность работы средств защиты информации при их взаимодействии с техническими средствами обработки информации и программным обеспечением.<br>Уточнение модели угроз безопасности информации и при | 1 | 36 | Раздел отчета. Опытная эксплуатация системы защиты информации информационной системы. |

| | | | | | |
|---|---|---|---|---|---|
| | | необходимости принимаются дополнительные меры по защите информации с целью устранения выявленных уязвимостей. | | | |
| 6 | Администрирование системы защиты информации информационной системы. | Заведение и удаление учетных записей пользователей, управление полномочиями пользователей информационной системы и поддержание правил разграничения доступа в информационной системе.<br>Управление средствами защиты информации в информационной системе, включая восстановление их работоспособности, генерацию, смену и восстановление паролей.<br>Централизованное управление системой защиты информации автоматизированной системы (в случае технической возможности).<br>Внесение изменений в организационно-распорядительные документы по защите информации (при необходимости).<br>Информирование пользователей о правилах эксплуатации системы защиты информации автоматизированной системы и отдельных средств защиты информации и их обучение. | 1 | 36 | Раздел отчета. Администрирование системы защиты информации информационной системы. |

4.2 Очная форма обучения

| № п/п | Вид учебной работы | Количество часов | Семестры | |
|---|---|---|---|---|
| | | | Семестр | Количество недель |
| **1** | **Аудиторные занятия** | 504 | | |
| | В том числе: | | | |
| 1.1 | Лекции | 72 | | |
| 1.2 | Семинарские/практические занятия | - | | |
| 1.3 | Лабораторные занятия | 432 | | |
| **2** | **Самостоятельная работа** | **504** | 2 | |
| **3** | **Промежуточная аттестация** | | 2 | |

| | | | | |
|---|---|---|---|---|
| | Дифференцированный зачет | | | |
| | Итого: | **504** | | |

### 4.3 Содержание практики

1. Получение индивидуального задания в рамках программы практики и в соответствии с направлением научных исследований по тематике магистерской диссертации.
2. Проведение производственного вводного инструктажа по технике безопасности и охране труда на месте проведения практики.
3. Ознакомление с предприятием, правилами внутреннего трудового распорядка.
4. Знакомство с информационно-методической базой учебной практики.
5. Определение объекта научного исследования.
6. Провести обзор по библиографическим источникам с целью изучения и применения пакетов программ для научных исследований, средств автоматизации проведения научных исследований в соответствии с индивидуальным заданием
7. Подготовить аналитический отчет по результатам обзора пакетов программ для научных исследований, средств автоматизации проведения научных исследований в соответствии с индивидуальным заданием.
8. Выбрать и обосновать пакеты программ для научных исследований и средства автоматизации проведения научных исследований, наиболее эффективные для подготовки магистерской диссертации.
9. Написание отчета по учебной практике, составление библиографии по теме магистерской диссертации.
10. Оформление отчета о практике, формирование портфолио обучающегося, приложений.
11. Защита отчета по практике.

## 5 Учебно-методическое и информационное обеспечение

### 5.1 Нормативные документы и ГОСТы

1 Федеральный государственный образовательный стандарт высшего профессионального образования по направлению подготовки 10.04.01 «Информационная безопасность», уровень – магистратура, утвержденный приказом от 19 сентября 2017 г. № 918;

2 Образовательной программой «Интеллектуальные системы» направления подготовки 10.04.01 «Информационная безопасность»;

3 Учебным планом университета по направлению подготовки 10.04.01 «Информационная безопасность».

4 ГОСТ 7.32-2001 (Отчет о научно-исследовательской работе);

5 ГОСТ Р 7.05-2008 (Библиографическая ссылка);

6 ГОСТ 7.1-2003 (Библиографическая запись. Библиографическое описание. Общие требования и правила составления).

### 5.2 Основная литература

1 Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Приказ ФСТЭК России от 11 февраля 2013 г. N 17.

2 Филиппович Ю.Н. Лингвистическое обеспечение информационных систем. Часть 1. Компьютерная лингвистика. Начало (посл.четв.XX в.). — М.: МГУП имени Ивана Федорова, 2013. — 452 с. – Режим доступа: URL: http://itclaim.ru/Library/Articles/publications_Philippovich_Yuriy/books_Philippovich_Yuriy.html

3 Ю.Н. Караулов, Ю.Н. Филиппович. Лингвокультурное сознание русской языковой личности. Моделирование состояния и функционирования.– М., 2009: Издательский центр «Азбуковник». – 336 с. – Режим доступа: URL: http://itclaim.ru/Library/Articles/publications_Philippovich_Yuriy/books_Philippovich_Yuriy.html

4 Шунейко, А. А. Квантитативная лингвистика и новые информационные технологии: учебник для вузов / А. А. Шунейко, И. А. Авдеенко. — Москва: Издательство Юрайт, 2022. — 347 с. — (Высшее образование). — ISBN 978-5-534-15446-7. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/507476Дополнительная литература

### 5.3 Дополнительная литература

1 Филиппович Ю.Н. Метафоры информационных технологий: анализ статей компьютерных журналов. / Серия «Компьютерная лингвистика». Вступ. Статья Ю.Н.Караулова. М.: МГУП, 2002.- книга в комплекте с CD ROM. – Режим доступа: URL:http://itclaim.ru/Library/Articles/publications_Philippovich_Yuriy/books_Philippovich_Yuriy.html

2 Филиппович Ю.Н., Прохоров А.В. Семантика информационных технологий: опыты словарно-тезаурусного описания. / Серия «Компьютерная лингвистика». Вступ. Статья А.И.Новикова. М.: МГУП, 2002.- книга в комплекте с CD ROM. – Режим доступа: URL:http://itclaim.ru/Library/Articles/publications_Philippovich_Yuriy/books_Philippovich_Yuriy. htm l

3 Филиппович Ю.Н., Черкасова Г.А., Д.Дельфт. Ассоциации информационных технологий: эксперимент на русском и французском языках. / Серия «Компьютерная лингвистика». Вступ. Статья Н.В.Уфимцевой. М.: МГУП, 2002.- книга в комплекте с CD ROM. – Режим доступа: URL: http://itclaim.ru/Library/Articles/publications_Philippovich_Yuriy/books_Philippovich_Yuriy. html

4 Филиппович А.Ю., Коршунов С. В., Дербенев Е.В., Филиппович Ю.Н. Проектирование основных и дополнительных образовательных программ в сфере ИКТ // Под ред. А.Ю. Филипповича. – М.: Лаборатория проблем технического образования МГТУ им. Н.Э. Баумана, 2010. – 134 с. Режим доступа: URL:http://itclaim.ru/Library/Articles/publications_Philippovich_Yuriy/books_Philippovich_Yuriy.html

5 Переходько, И. В. Компьютерные технологии в переводе : учебное пособие / И. В. Переходько. — Оренбург : ОГУ, 2018. — 110 с. — ISBN 978-5-7410-2208-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/159856

### 5.4 Электронные образовательные ресурсы

1. Научно-образовательный кластер CLAIM (it-claim.ru.)
2. ЭБС Лань (lanbook.com)
3. Образовательная платформа Юрайт. Для вузов и ссузов. (urait.ru)

### 5.5 Лицензионное и свободно распространяемое программное обеспечение

При прохождении практики может использоваться только лицензионное программное обеспечение и свободно распространяемые Интернет-ресурсы. Основной Интернет ресурс – Научно-образовательный кластер CLAIM — it-claim.ru.

### 5.6 Современные профессиональные базы данных и информационные справочные системы

1. http://www.philippovich.ru Научно-образовательный кластер CLAIM
2. http://www.raai.org/ Российская ассоциация искусственного интеллекта
3. http://fuzzy.raai.org/ Российская ассоциация нечетких систем
4. http://aihandbook.intsys.org.ru/index.php/resources/orgs/242-org-p12 Ассоциация нейроинформатики/RNNS
5. www.aaai.org Американская ассоциация искусственного интеллекта American Association for Artificial Intelligence (AAAI)
6. http://aifuture.chat.ru/ Искусственный интеллект ("Взгляд в будущее").
7. http://aicommunity.narod.ru/ Материалы об искусственном интеллект.
8. Онлайн курс «Машинное обучение» - https://www.coursera.org/learn/machinelearning
9. Онлайн курс «Нейронные сети и компьютерное зрение» - https://stepik.org/course/50352
10. Онлайн курс ШАД «Машинное обучение» - https://yandexdataschool.ru/eduprocess/courses/machine-learning
11. Информационный ресурс www.machinelearning.ru

## 6 Материально-техническое обеспечение

В качестве материально-технического обеспечения практики следует использовать: материалы по практике, представленные в цифровом виде. При необходимости, обучающимся предоставляются учебно-вычислительные лаборатории с доступом в интернет, вместительностью не менее 30 человек, с наличием соответствующего числа персональных компьютеров, с наличием интерактивной доски/проектора с экраном для реализации возможности подключения персонального компьютера преподавателя.

Всю необходимую информацию по прохождению учебной (проектно-технологической) практики необходимо извлекать из специальных методических указаний, утверждённых на выпускающей кафедре.

# 7 Методические рекомендации

## 7.1 Методические рекомендации для руководителя по организации практики

Процесс прохождения учебной (проектно-технологической) практики осуществляется в рамках рабочего учебного плана по направлению подготовки 10.04.01 «Информационная безопасность», в соответствии с образовательной программой «Интеллектуальные системы».

Структура и последовательность прохождения этапов учебной (проектнотехнологической) практики представлена в п. 3 настоящей рабочей программы.

Промежуточная аттестация магистрантов в форме дифференцированного зачёта проводится по результатам выполнения всех видов учебной работы, предусмотренных учебным планом по учебной (проектно-технологической) практике. Оценка степени достижения обучающимися планируемых результатов обучения по учебной (проектнотехнологической) практике проводится преподавателем, являющимся руководителем магистранта методом экспертной оценки. По итогам промежуточной аттестации по учебной (проектно-технологической) практике выставляется оценка по пятибалльной системе.

К промежуточной аттестации допускаются только студенты, выполнившие все виды учебной работы, предусмотренные рабочей программой по учебной (проектнотехнологической) практике.

Перечень литературы и информационных ресурсов, необходимой в ходе прохождения практики, приведен в п.4 настоящей рабочей программы.

Всю необходимую информацию по прохождению учебной (проектно-технологической) практики необходимо извлекать из специальных методических указаний, утверждённых на выпускающей кафедре.

## 7.2 Методические указания для обучающихся по освоению дисциплины

При подготовке к защите практики следует получить необходимую литературу и наглядные пособия по указанию преподавателя. Материал лекции целесообразно записывать на одной стороне тетради, для того чтобы пополнить материал на самостоятельной подготовке из рекомендуемых источников. Материалы лекций по пройденным занятиям целесообразно повторять перед защитой.

В процессе прохождения практики магистранты приобретают умения использовать методы, средства и технологии решения конкретных задач профессиональной деятельности с применением ЭВМ, получают практические навыки разработки программ и осваивают

приемы работы в телекоммуникационных сетях. Производственная практика направлена на изучение средств сбора и регистрации данных и организации их обработки в конкретных системах. Производственная практика предусматривает самостоятельную разработку магистрантами программ с заданной функциональностью. В рамках этих занятий преподаватель проводит анализ типовых ошибок, допущенных при решении поставленных задач, организует рассмотрение наиболее удачных вариантов решений. Магистранты привлекаются к разбору и сравнительному анализу предлагаемых вариантов программных реализаций решаемых задач.

Всю необходимую информацию по прохождению учебной (проектно-технологической) практики необходимо извлекать из специальных методических указаний, утверждённых на выпускающей кафедре.

# 8 Фонд оценочных средств

## 8.1 Методы контроля и оценивания результатов прохождения практики

В качестве основной формы отчетности является письменный отчет. Форма контроля прохождения практики - дифференцированный зачет.

По окончании практики студент-практикант составляет письменный отчет и в порядке, установленном кафедрой, сдает его и другие отчетные материалы, предусмотренные методическими указаниями кафедры к прохождению практики, подписанные руководителем практики от организации.

Отчет должен содержать сведения о конкретно выполненной студентом работе в период прохождения практики.

При оценке итогов работы студента принимается во внимание характеристика, данная ему руководителем практики от предприятия.

## 8.2 Шкала и критерии оценивания результатов прохождения практики

Отчеты оцениваются в процентах степени выполнения следующих критериев и для выставления оценки суммируются проценты за каждый из четырех критериев:

1. Полнота выполнения практического задания (30%): соответствует ли функциональность заданным требованиям и целям, насколько точно и без ошибок код выполняет поставленные задачи, насколько эффективно задание отвечает требованиям целевой аудитории и обеспечивает приятное восприятие.

2. Качество и структура кода (10%): качество, читаемость и организация кода, рациональность выполнения задания, последовательность именования и соблюдение лучших практик.
3. Творчество и инновации (10%): творческий подход студентов к выполнению заданий, насколько студенты вышли за рамки основных требований и реализовали дополнительные возможности или использовали уникальные решения.
4. Ответы на вопросы по коду студента и теории (50%):

Дает краткий ответ, содержащий ошибки или неточности. На наводящие вопросы отвечает неправильно (10% из 50%)

Дает развернутый ответ, содержащий ошибки или неточности. На наводящие вопросы отвечает неверно (20% из 50%)

Дает развернутый ответ, содержащий ошибки или неточности. На наводящие вопросы отвечает правильно (30% из 50%)

Дает правильные и развернутые ответы на вопросы (50% из 50%).

### 8.3 Оценочные средства

8.3.1 Текущий контроль

1. Установка и настройка средств защиты информации в автоматизированной системы.
2. Разработка документов, определяющих мероприятия, проводимые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации.
3. Внедрение организационных мер в информационной системе.
4. Предварительные испытания системы защиты информации информационной системы.
5. Опытная эксплуатация системы защиты информации информационной системы.
6. Анализ уязвимостей информационной системы.
7. Приемочные испытания системы защиты информации информационной системы
8. Обеспечение безопасности среды эксплуатации информационной системы
9. Администрирование системы защиты информации информационной системы.
10. Реагирование на инциденты, связанные с нарушением требований о защите информации.
11. Управление конфигурацией системы защиты информации автоматизированной системы
12. Управление защитой информации в информационной системе
13. Методические материалы, используемые в образовательной деятельности.

8.3.2 Промежуточная аттестация

1. Эксплуатационная документация на систему защиты информации автоматизированной системы.
2. Руководство администратора и пользователя средств защиты информации.
3. Состав организационных мер и порядок их реализации.
4. Порядок учета, хранения и использования съемных машинных носителей информации.
5. Порядок вывода информации на внешние носители информации.
6. Правила и порядок генерации, смены и восстановления паролей пользователей, заведения и удаления учетных записей пользователей.
7. Порядок выявления инцидентов, связанных с нарушениями требований о защите информации, и реагирования на эти инциденты.
8. Порядок обслуживания системы защиты информации обслуживающим персоналом.
9. Реализация в соответствии с организационно-распорядительными документами по защите информации правил, регламентирующих права доступа субъектов доступа к объектам доступа (далее - правила разграничения доступа).
10. Введение ограничений на действия пользователей и обслуживающего персонала, а так же на изменение условий эксплуатации, состава и конфигурации технических средств обработки информации и программного обеспечения.
11. Проверка полноты и детальности описания в организационно-распорядительных документах по защите информации действий пользователей и администраторов информационной системы по реализации организационных мер.
12. Отработка действий должностных лиц и подразделений, ответственных за реализацию организационных мер.
13. Проверка работоспособности системы защиты информации информационной системы.
14. Принятие решения о возможности опытной эксплуатации системы защиты информации информационной системы.
15. Опытная эксплуатация системы защиты информации информационной системы
16. Проверка функционирования системы защиты информации информационной системы, в том числе реализованных мер по защите информации, а также готовность пользователей и администраторов к эксплуатации системы защиты информации информационной системы.

17. Оценка возможности преодоления нарушителем системы защиты информации информационной системы и предотвращения реализации угроз безопасности информации.
18. Средства контроля (анализа) защищенности информации.
19. Анализ уязвимостей средств защиты информации, технических средств обработки информации и программного обеспечения информационной системы.
20. Правильность установки и настройки средств защиты информации, технических средств обработки информации и программного обеспечения, а также корректность работы средств защиты информации при их взаимодействии с техническими средствами обработки информации и программным обеспечением.
21. Уточнение модели угроз безопасности информации и при необходимости принимаются дополнительные меры по защите информации с целью устранения выявленных уязвимостей.
22. Проверка выполнения требований к системе защиты информации информационной системы в соответствии с техническим заданием на ее создание.
23. Организация контролируемой зоны, в пределах которой размещаются стационарные технические средства, обрабатывающие информацию конфиденциального характера.
24. Средства защиты информации, а также средства, обеспечивающие функционирование информационной системы.
25. Контроль и управление доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены.
26. Защита технических средств, средств защиты информации и средств обеспечения функционирования.
27. Заведение и удаление учетных записей пользователей, управление полномочиями пользователей информационной системы и поддержание правил разграничения доступа в информационной системе.
28. Управление средствами защиты информации в информационной системе, включая восстановление их работоспособности, генерацию, смену и восстановление паролей.
29. Централизованное управление системой защиты информации автоматизированной системы (в случае технической возможности).
30. Информирование пользователей о правилах эксплуатации системы защиты информации автоматизированной системы и отдельных средств защиты информации и их обучение.

31. Выявление инцидентов, связанных с нарушением требований о защите информации, включая выявление сбоев в работе технических средств, программного обеспечения и средств защиты информации.
32. Выявление внедрения вредоносных компьютерных программ (вирусов), неправомерных действий пользователей и иных событий, связанных с нарушением свойств безопасности информации (конфиденциальности, целостности, доступности).
33. Выявление причин возникновения инцидентов, связанных с нарушением требований о защите информации.
34. Планирование и принятие мер по предупреждению и устранению инцидентов, в том числе по восстановлению информационной системы и ее сегментов после сбоев, выявлению и устранению последствий внедрения вредоносных компьютерных программ (вирусов), неправомерных действий пользователей и иных событий, связанных с нарушением свойств безопасности информации (конфиденциальности, целостности, доступности).
35. Обеспечение целостности системы защиты информации информационной системы, включая резервирование средств защиты информации.
36. Установка обновлений программного обеспечения, включая программное обеспечение средств защиты информации, выпускаемых их разработчиками.
37. Управление параметрами настройки средств защиты информации, составом и конфигурацией технических средств и программного обеспечения, а также контроль за несанкционированными подключениями технических средств и установкой программного обеспечения
38. Выполнение организационных мер по защите информации.
39. Контроль состояния защиты информации в информационной системе, включая контроль за событиями и действиями пользователей информационной системы.
40. Анализ и оценка функционирования системы защиты информации информационной системы, включая выявление и устранение недостатков в функционировании системы защиты информации информационной системы.
41. Периодический анализ уязвимостей информационной системы и оперативное принятие первоочередных мер по устранению вновь выявленных уязвимостей, приводящих к возникновению актуальных угроз безопасности.
42. Периодический анализ изменения угроз безопасности информации в информационной системе, возникающих в ходе ее эксплуатации, и принятие мер по защите информации в случае возникновения новых угроз безопасности информации.

43. Анализ влияния на систему защиты информации информационной системы планируемых изменений в информационной системе.

44. Доработка (модернизация) системы защиты информации информационной системы и ее переаттестация при изменении класса защищенности информационной системы, состава актуальных угроз безопасности информации или проектных решений по системе защиты информации информационной системы (в том числе состава используемых средств защиты информации).

45. Сопровождение системы защиты информации информационной системы в ходе ее эксплуатации, включая корректировку эксплуатационной документации на нее.