МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
Декан факультета
«Информационных технологий»
_____ / Д.Г. Демидов /
«26» февраля 2026 г.

РАБОЧАЯ ПРОГРАММА
технологической практики

Направление подготовки
10.03.01 «Информационная безопасность»

Образовательная программа (профиль)
«Безопасность компьютерных систем»

Квалификация выпускника
Бакалавр

Форма обучения
Очная
Год приема - 2026

Москва 2026 г.

Разработчик(и):

Доцент кафедры «Информационная безопасность»  /И.В. Калуцкий/
к.т.н., доцент

Согласовано:
Заведующий кафедрой «Информационная безопасность»  /И.В.Калуцкий/

Руководитель образовательной программы,  /А.Ю.

Гневшев/

Содержание

1. Цели, задачи и планируемые результаты прохождения практики

К **основным целям** освоения технологической практики следует отнести:

- закрепление и углубление теоретических знаний, полученных студентами при изучении дисциплин профессионального цикла и дисциплин специализации для формирования требований и разработке системы защиты информации автоматизированной системы;
- приобретение и развитие необходимых практических умений и навыков при формировании требований и разработке системы информационной безопасности на предприятии в соответствии с требованиями к уровню подготовки выпускника.

К **основным задачам** освоения технологической практики следует отнести:

- 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.

Компетенции обучающегося, формируемые в результате прохождения практики

В результате освоения технологической практики у обучающихся формируются следующие компетенции и должны быть достигнуты следующие результаты обучения как этап формирования соответствующих компетенций:

Код и наименование компетенций	Индикаторы достижения компетенции
ПК-1. Способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;	ИПК-1.1. Знает современные виды информационного взаимодействия и обслуживания, принципы и методы противодействия несанкционированному информационному воздействию на вычислительные сети и системы передачи информации, основные задачи и понятия криптографии, требования к шифрам и основные характеристики шифров, модели шифров и математические методы их исследования, принципы построения криптографических алгоритмов; ИПК-1.2. Умеет использовать и настраивать программно-аппаратные средства защиты информации, проводить анализ показателей качества сетей и систем связи ИПК-1.3. Владеет навыками по установке, настройке и обслуживанию программных, программно-аппаратных и технических средств защиты информации
ОПК-7. Способен использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности	ИОПК-7.1. Знает современные средства разработки и анализа программного обеспечения на языках высокого уровня, методы программирования и разработки эффективных алгоритмов решения прикладных задач, базовые структуры данных, основные алгоритмы сортировки и поиска и способы их эффективной реализации, основы администрирования операционных систем и вычислительных сетей, эталонную модель взаимодействия открытых систем, методы

	коммутации и маршрутизации, сетевые протоколы; ИОПК-7.2. Умеет выбирать необходимые инструментальные средства для разработки программ в различных операционных системах и средах, составлять, тестировать, отлаживать и оформлять программы на языках высокого уровня, включая объектно-ориентированные, формализовать поставленную задачу, выбирать необходимые инструментальные средства для разработки программ в различных операционных системах и средах, устанавливать и осуществлять первичную настройку одной из операционных систем; ИОПК-7.3. Владеет навыками разработки программ на языке программирования высокого уровня, способами оценки сложности работы алгоритмов, основными подходами к организации процесса разработки программного обеспечения.
ОПК-1.2. Способен администрировать средства защиты информации в компьютерных системах и сетях	ИОПК-1.2.1.Знает принципы организации информационных систем в соответствии с требованиями по защите информации, криптографические стандарты и как их использовать в информационных системах; ИОПК-1.2.2.Умеет развертывать, конфигурировать и настраивать вычислительные сети, формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе, применять отечественные и зарубежные стандарты в области криптографических методов компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем; ИОПК-1.2.3.Владеет навыками использования типовых криптографических алгоритмов
ОПК-1.1. Способен разрабатывать и реализовывать политики управления доступом в компьютерных системах	ИОПК-1.1.1. Знает формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах; ИОПК-1.1.2. Умеет применять формальные модели для разработки политик безопасности, политик управления доступом; ИОПК-1.1.3. Владеет навыками создания формальных моделей управления доступом.
ОПК-2. Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности	ИОПК-2.1 Знает информационно-коммуникационные технологии, программные средства системного и прикладного назначения; ИОПК-2.2. Умеет применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности ИОПК-2.3.Владеет навыками применения информационно-коммуникационных технологий, программными средствами системного и прикладного назначения, в том числе отечественного производства, для решения задач.
ПК-3. Способен принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	ИПК-3.1. Знает методы и средства контроля эффективности технической защиты информации; ИПК-3.2. Умеет контролировать эффективность принятых мер по реализации частных политик информационной безопасности информационных

	систем; ИПК-3.3. Владеет навыками выбора и обоснования критериев эффективности функционирования защищенных информационных систем, навыками участия в экспертизе состояния защищенности информации на объекте защиты.
ПК-4. Способен оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	ИПК-4.1. Знает свойства, функции и признаки документа, в том числе как объекта нападения и защиты; основы документационного обеспечения управления, задачи органов защиты информации на предприятиях, порядок организации работы и нормативные правовые акты по сертификации средств защиты информации; ИПК-4.2. Умеет квалифицированно исследовать состав документации предприятия (организации), разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации; владеет методами формирования требований по защите информации.

2. Место практики в структуре образовательной программы

Технологическая практика относится к блоку 2 «Практики» части, формируемой участниками образовательных отношений (Б2.2.1), основной образовательной программы (Б2.2.1.3).

Практика базируется на дисциплинах базовой и вариативной части учебного плана.

Данная практика является предшествующей для выполнения выпускной квалификационной работы.

3. Характеристика практики

Тип и вид практики – производственная, стационарная.

Способ и форма проведения практики – непрерывно.

Практика проводится в сторонних учреждениях, организациях и предприятиях любых организационно-правовых форм, основная деятельность которых предопределяет наличие объектов и видов профессиональной деятельности выпускников по данной специальности (специализации) или на кафедрах и в лабораториях вуза, обладающих необходимым кадровым и научно-техническим потенциалом.

Практика проводится в 8 семестре на базе предприятий требуемого профиля.

4. Структура и содержание практики

Общая трудоемкость практики составляет 10 зачетных единиц, 288 часов.

№ п/п	Разделы (этапы) практики	Виды работ на практике, включая самостоятельную работу студентов и трудоемкость (в зачетных единицах, часах)			Формы текущего контроля
		Виды работ	ЗЕ	час	

1	Определение актуальных угроз безопасности информации и разработку на их основе модели угроз	Оценка возможностей и потенциала нарушителей (внешних, внутренних), анализа возможных уязвимостей информационной системы, возможных последствий от реализации угроз безопасности информации для нарушения свойств безопасности информации (конфиденциальности, целостности, доступности), а также с учетом структурно-функциональных характеристик информационной системы, включающих структуру и состав информационной системы, физические, функциональные и технологические взаимосвязи между сегментами (составными частями) информационной системы и взаимосвязи с иными информационными системами, режимы обработки информации в информационной системе в целом и в ее отдельных сегментах. Модель угроз безопасности информации.	1	36	Модель угроз
2	Классификация информационной системы	Определение значимости обрабатываемой информации конфиденциального характера и масштаба информационной системы. Класс защищенности.	1	36	Класс защищенности
3	Определение требований к системе защиты информации информационной системы	Цель и задачи обеспечения защиты информации в информационной системе. Перечень нормативных правовых актов, методических документов и национальных стандартов, требованиям которых должна соответствовать информационная система. Перечень типов объектов защиты информационной системы. Требования к мерам и средствам защиты информации, применяемым в информационной системе.	1	36	Требования к мерам и средствам защиты информации
4	Разработка проектных решений по системе защиты информации информационной системы	Субъекты доступа (пользователи, процессы и иные субъекты доступа) и объекты доступа (устройства, объекты файловой системы, запускаемые и исполняемые модули, объекты системы управления базами данных, объекты, создаваемые прикладным программным обеспечением, иные объекты доступа). Состав мер по защите информации, обеспечивающих блокирование (нейтрализацию) актуальных угроз безопасности информации, и их содержание в соответствии с установленным классом защищенности информационной системы. Организационные меры, виды и типы средств защиты информации. Логическая структура, состав (количество) и места размещения элементов системы защиты информации автоматизированной системы. Средства защиты информации с учетом их совместимости с информационными технологиями и техническими средствами обработки информации, функций безопасности этих средств и особенностей	1	36	Проектные решения по системе защиты информации информационной системы

		их реализации, а также класса защищенности информационной системы. Параметры настройки средств защиты информации, обеспечивающие реализацию мер по защите информации и блокирование (нейтрализацию) актуальных угроз безопасности информации, в том числе путем устранения возможных уязвимостей информационной системы.			
5	Эксплуатационная документация на систему защиты информации информационной системы	Организационная структура системы защиты информации информационной системы. Состав, номенклатуру, места установки и параметры настройки средств защиты информации, программного обеспечения и технических средств обработки информации. Порядок создания, удаления в информационной системе учетных записей пользователей и установления полномочий пользователей и администраторов информационной системы. Порядок контроля за событиями и действиями пользователей в информационной системе. Порядок обновления программного обеспечения, включая программное обеспечение средств защиты информации, в информационной системе. Порядок выявления и устранения недостатков в системе защиты информации информационной системы, а также порядок внесения изменений в эксплуатационную документацию на систему защиты информации информационной системы. Порядок контроля целостности системы защиты информации информационной системы и ее тестирования. Правила эксплуатации системы защиты информации информационной системы, порядок ее настройки и восстановления работоспособности в случае нарушения функционирования системы защиты информации информационной системы. Порядок управления параметрами настройки средств защиты информации, составом и конфигурацией технических средств обработки информации и программного обеспечения, а также контроля за несанкционированными подключениями технических средств обработки информации и установкой программного обеспечения. Порядок архивирования информации конфиденциального характера, содержащейся в информационной системе, и стирания (уничтожения) данных и остаточной информации с машинных носителей информации и (или) уничтожения машинных носителей информации.	1	35	Эксплуатационная документация на систему защиты
6	Тестирование системы защиты информации	Проверка работоспособности и совместимости средств защиты	1	18	Проверка выполнения

	информационной системы	информации с информационными технологиями и техническими средствами обработки информации. Проверка выполнения средствами защиты информации требований к системе защиты информации информационной системы. Корректировка документации на систему защиты информации информационной системы (при необходимости).			средствами защиты информации требований к системе защиты информации информационной системы.
7	Обеспечение безопасности среды эксплуатации информационной системы	Организация контролируемой зоны, в пределах которой размещаются стационарные технические средства, обрабатывающие информацию конфиденциального характера, и средства защиты информации, а также средства, обеспечивающие функционирование информационной системы. Контроль и управление доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены. Защита технических средств, средств защиты информации и средств обеспечения функционирования.	1	18	Раздел отчета. Защита технических средств, средств защиты информации и средств обеспечения функционирования.
8	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. Управление средствами защиты информации в информационной системе, включая восстановление их работоспособности, генерацию, смену и восстановление паролей. Централизованное управление системой защиты информации автоматизированной системы (в случае технической возможности). Внесение изменений в организационно-распорядительные документы по защите информации (при необходимости). Информирование пользователей о правилах эксплуатации системы защиты информации автоматизированной системы и отдельных средств защиты информации и их обучение.	1	18	Раздел отчета. Администрирование системы защиты информации информационной системы.
9	Реагирование на инциденты, связанные с нарушением требований о защите информации.	Выявление инцидентов, связанных с нарушением требований о защите информации, включая выявление сбоев в работе технических средств, программного обеспечения и средств защиты информации, выявление внедрения вредоносных компьютерных программ (вирусов), неправомерных действий пользователей и иных событий, связанных с нарушением свойств безопасности информации (конфиденциальности, целостности, доступности). Своевременное информирование структурного подразделения или должностного лица, ответственных за	1	18	Раздел отчета. Реагирование на инциденты, связанные с нарушением требований о защите информации

		защиту информации, пользователями информационной системы об инцидентах, связанных с нарушением требований о защите информации. Выявление причин возникновения инцидентов, связанных с нарушением требований о защите информации, 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).			
10	Управление конфигурацией системы защиты информации автоматизированной системы	Обеспечение целостности системы защиты информации информационной системы, включая резервирование средств защиты информации. Установка обновлений программного обеспечения, включая программное обеспечение средств защиты информации, выпускаемых их разработчиками. 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	0,5	18	Раздел отчета. Управление конфигурацией системы защиты информации автоматизированной системы
11	Управление защитой информации в информационной системе	Выполнение организационных мер по защите информации. Контроль состояния защиты информации в информационной системе, включая контроль за событиями и действиями пользователей информационной системы. Анализ и оценка функционирования системы защиты информации информационной системы, включая выявление и устранение недостатков в функционировании системы защиты информации информационной системы. Периодический анализ уязвимостей информационной системы и оперативное принятие первоочередных мер по устранению вновь выявленных уязвимостей, приводящих к возникновению актуальных угроз безопасности. 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. Анализ влияния на систему защиты информации информационной системы планируемых изменений в	0,5	18	Раздел отчета. Управление защитой информации в информационной системе

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

5. Учебно-методическое и информационное обеспечение

5.1 Нормативные документы и ГОСТы

- 06.032 Специалист по безопасности компьютерных систем и сетей
- 06.033 Специалист по защите информации в автоматизированных системах

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. Рацеев, С. М. Программирование на языке Си / С. М. Рацеев. — 2-е изд., стер. — Санкт-Петербург : Лань, 2023. — 332 с. — ISBN 978-5-507- 47236-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/351863 .

3. Тутубалин, П. И. Программирование на языках высокого уровня : учебное пособие / П. И. Тутубалин. — Казань : КНИТУ-КАИ, 2021. — 346 с. — ISBN 978-5-7579-2579-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/264911

4. Павловская, Т. А. Программирование на языке высокого уровня C# : учебное пособие / Т. А. Павловская. — 2-е изд. — Москва : ИНТУИТ, 2016. — 245 с. — Текст : электронный // Лань : электронно- библиотечная система. — URL: https://e.lanbook.com/book/100413

5.3 Дополнительная литература

– Мартишин, С.А. Базы данных. Практическое применение СУБД SQL- и NoSQL-типа для проектирования информационных систем: учеб.пособие / С.А. Мартишин, В.Л. Симонов, М.В. Храпченко. — М.: Форум, 2018. — 368 с. — (Среднее профессиональное образование).

– Мартишин, С.А. Проектирование и реализация баз данных в СУБД MySQL с использованием MySQL Workbench. Методы и средства проектирования

информационных систем и технологий. Инструментальные средства информационных систем: учеб. пособие / С.А. Мартишин, В.Л. Симонов, М.В. Храпченко. — М.:Форум, 2018. — 160 с.— (Среднее профессиональное образование).

- Мюллер, Р.Дж. Проектирование баз данных и UML / Р.Дж. Мюллер; перев. Е. Молодцова. — М.: Лори, 2018. — 420 с.
- Стасышин, В.М. Базы данных: технологии доступа: учеб. пособие / В.М. Стасышин, Т.Л. Стасышина. — М.: Юрайт, 2017. — 178 с. — (Университеты России).

5.4 Электронные образовательные ресурсы

Определяется предприятием

5.5 Лицензионное и свободно распространяемое программное обеспечение

Для заданий по практике необходимо следующее программное обеспечение.

1. Microsoft windows 8-10 или Astra Linux.
2. notepad++.
3. Chrome.
4. Microsoft Word или Libre office.

5.6 Современные профессиональные базы данных и информационные справочные системы

Определяется предприятием

6. Материально-техническое обеспечение

Материально-техническое обеспечение практики определяется предприятием.

Программа составлена в соответствии с требованиями ФГОС ВО с учетом рекомендаций и ООП ВО по направлению подготовки 10.03.01 «Информационная безопасность».

7. Методические рекомендации

7.1 Учебно-методическое обеспечение самостоятельной работы студентов на практике

Контрольные вопросы и задания для проведения аттестации по итогам практики

1. Оценка возможностей и потенциала нарушителей (внешних, внутренних).
2. Анализ возможных уязвимостей информационной системы.
3. Возможные последствия от реализации угроз безопасности информации для нарушения свойств безопасности информации (конфиденциальности, целостности, доступности).
4. Физические, функциональные и технологические взаимосвязи между сегментами (составными частями) информационной системы и взаимосвязи с иными информационными системами,
5. Режимы обработки информации в информационной системе в целом и в ее отдельных сегментах.
6. Модель угроз безопасности информации.
7. Определение значимости обрабатываемой информации конфиденциального характера.

8. Масштаб информационной системы.
9. Класс защищенности.
10. Цель и задачи обеспечения защиты информации в информационной системе.
11. Перечень нормативных правовых актов, методических документов и национальных стандартов, требованиям которых должна соответствовать информационная система.
12. Перечень типов объектов защиты информационной системы.
13. Требования к мерам и средствам защиты информации, применяемым в информационной системе.
14. Субъекты доступа (пользователи, процессы и иные субъекты доступа) и объекты доступа (устройства, объекты файловой системы, запускаемые и исполняемые модули, объекты системы управления базами данных, объекты, создаваемые прикладным программным обеспечением, иные объекты доступа).
15. Состав мер по защите информации, обеспечивающих блокирование (нейтрализацию) актуальных угроз безопасности информации.
16. Содержание состава мер по защите информации в соответствии с установленным классом защищенности информационной системы.
17. Организационные меры, виды и типы средств защиты информации.
18. Логическая структура, состав (количество) и места размещения элементов системы защиты информации автоматизированной системы.
19. Средства защиты информации с учетом их совместимости с информационными технологиями и техническими средствами обработки информации, функций безопасности этих средств и особенностей их реализации, а также класса защищенности информационной системы.
20. Параметры настройки средств защиты информации, обеспечивающие реализацию мер по защите информации и блокирование (нейтрализацию) актуальных угроз безопасности информации, в том числе путем устранения возможных уязвимостей информационной системы.
21. Организационная структура системы защиты информации информационной системы.
22. Состав, номенклатуру, места установки и параметры настройки средств защиты информации, программного обеспечения и технических средств обработки информации.
23. Порядок создания, удаления в информационной системе учетных записей пользователей и установления полномочий пользователей и администраторов информационной системы.
24. Порядок контроля за событиями и действиями пользователей в информационной системе.
25. Порядок обновления программного обеспечения, включая программное обеспечение средств защиты информации, в информационной системе.
26. Порядок выявления и устранения недостатков в системе защиты информации информационной системы, а также порядок внесения изменений в эксплуатационную документацию на систему защиты информации информационной системы.
27. Порядок контроля целостности системы защиты информации информационной системы и ее тестирования.
28. Правила эксплуатации системы защиты информации информационной системы, порядок ее настройки и восстановления работоспособности в случае нарушения функционирования системы защиты информации информационной системы.
29. Порядок управления параметрами настройки средств защиты информации, составом и конфигурацией технических средств обработки информации и программного обеспечения, а также контроля за несанкционированными подключениями технических средств обработки информации и установкой программного обеспечения.
30. Порядок архивирования информации конфиденциального характера, содержащейся в информационной системе, и стирания (уничтожения) данных и остаточной информации с машинных носителей информации и (или) уничтожения машинных носителей информации.

31. Проверка работоспособности и совместимости средств защиты информации с информационными технологиями и техническими средствами обработки информации.
32. Проверка выполнения средствами защиты информации требований к системе защиты информации информационной системы.
33. Организация контролируемой зоны, в пределах которой размещаются стационарные технические средства, обрабатывающие информацию конфиденциального характера.
34. Средства защиты информации, а также средства, обеспечивающие функционирование информационной системы.
35. Контроль и управление доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены.
36. Защита технических средств, средств защиты информации и средств обеспечения функционирования.
37. Заведение и удаление учетных записей пользователей, управление полномочиями пользователей информационной системы и поддержание правил разграничения доступа в информационной системе.
38. Управление средствами защиты информации в информационной системе, включая восстановление их работоспособности, генерацию, смену и восстановление паролей.
39. Централизованное управление системой защиты информации автоматизированной системы (в случае технической возможности).
40. Информирование пользователей о правилах эксплуатации системы защиты информации автоматизированной системы и отдельных средств защиты информации и их обучение.
41. Выявление инцидентов, связанных с нарушением требований о защите информации, включая выявление сбоев в работе технических средств, программного обеспечения и средств защиты информации.
42. Выявление внедрения вредоносных компьютерных программ (вирусов), неправомерных действий пользователей и иных событий, связанных с нарушением свойств безопасности информации (конфиденциальности, целостности, доступности).
43. Выявление причин возникновения инцидентов, связанных с нарушением требований о защите информации.
44. 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).
45. Обеспечение целостности системы защиты информации информационной системы, включая резервирование средств защиты информации.
46. Установка обновлений программного обеспечения, включая программное обеспечение средств защиты информации, выпускаемых их разработчиками.
47. 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
48. Выполнение организационных мер по защите информации.
49. Контроль состояния защиты информации в информационной системе, включая контроль за событиями и действиями пользователей информационной системы.
50. Анализ и оценка функционирования системы защиты информации информационной системы, включая выявление и устранение недостатков в функционировании системы защиты информации информационной системы.

51. Периодический анализ уязвимостей информационной системы и оперативное принятие первоочередных мер по устранению вновь выявленных уязвимостей, приводящих к возникновению актуальных угроз безопасности.
52. 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.
53. Анализ влияния на систему защиты информации информационной системы планируемых изменений в информационной системе.
54. 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).
55. Сопровождение системы защиты информации информационной системы в ходе ее эксплуатации, включая корректировку эксплуатационной документации на нее.

7.2 Методические указания для обучающихся по освоению дисциплины

Самостоятельная работа проводится в соответствии с содержанием настоящей рабочей программы и представляют собой выполнение индивидуальных заданий от руководителей практики в соответствие с регламентом выполнения работ в организации, где проводится практика.

Посещение рабочего места (или организации, предоставляющей место практики) является обязательным. Обучающийся обязан соблюдать график работы, определенный нормативными документами организации, предоставляющей место практики. Обучающийся обязан соблюдать правила техники безопасности и другие нормативные документы, принятые в организации, для безопасного выполнения соответствующих работ.

Регулярная проработка материала по практике «Производственная (проектно-технологическая) практика» является одним из важнейших видов самостоятельной работы обучающегося в течение семестра, необходимой для качественной подготовки к семестровой и промежуточной аттестации по практике.

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.

8.2 Шкала и критерии оценивания результатов прохождения практики

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.

8.3 Оценочные средства

8.3.1 Текущий контроль

Отчет по практике

Отчет о практике должен содержать:

1. Определение актуальных угроз безопасности информации и разработку на их основе модели угроз.
2. Классификация информационной системы.
3. Определение требований к системе защиты информации информационной системы.
4. Разработка проектных решений по системе защиты информации информационной системы.
5. Эксплуатационная документация на систему защиты информации информационной системы.
6. Тестирование системы защиты информации информационной системы.
7. Обеспечение безопасности среды эксплуатации информационной системы
8. Администрирование системы защиты информации информационной системы.
9. Реагирование на инциденты, связанные с нарушением требований о защите информации.
10. Управление конфигурацией системы защиты информации автоматизированной системы
11. Управление защитой информации в информационной системе

8.3.2 Промежуточная аттестация

Дифференцированный зачет

Вопросы для дифференцированного зачета

1. Оценка возможностей и потенциала нарушителей (внешних, внутренних).
2. Анализ возможных уязвимостей информационной системы.
3. Возможные последствия от реализации угроз безопасности информации для нарушения свойств безопасности информации (конфиденциальности, целостности, доступности).
4. Физические, функциональные и технологические взаимосвязи между сегментами (составными частями) информационной системы и взаимосвязи с иными информационными системами,
5. Режимы обработки информации в информационной системе в целом и в ее отдельных сегментах.
6. Модель угроз безопасности информации.
7. Определение значимости обрабатываемой информации конфиденциального характера.
8. Масштаб информационной системы.
9. Класс защищенности.
10. Цель и задачи обеспечения защиты информации в информационной системе.
11. Организация контролируемой зоны, в пределах которой размещаются стационарные технические средства, обрабатывающие информацию конфиденциального характера.
12. Средства защиты информации, а также средства, обеспечивающие функционирование информационной системы.
13. Контроль и управление доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены.

14. Защита технических средств, средств защиты информации и средств обеспечения функционирования.
15. Заведение и удаление учетных записей пользователей, управление полномочиями пользователей информационной системы и поддержание правил разграничения доступа в информационной системе.
16. Управление средствами защиты информации в информационной системе, включая восстановление их работоспособности, генерацию, смену и восстановление паролей.
17. Централизованное управление системой защиты информации автоматизированной системы (в случае технической возможности).
18. Информирование пользователей о правилах эксплуатации системы защиты информации автоматизированной системы и отдельных средств защиты информации и их обучение.
19. Выявление инцидентов, связанных с нарушением требований о защите информации, включая выявление сбоев в работе технических средств, программного обеспечения и средств защиты информации.
20. Выявление внедрения вредоносных компьютерных программ (вирусов), неправомерных действий пользователей и иных событий, связанных с нарушением свойств безопасности информации (конфиденциальности, целостности, доступности).
21. Выявление причин возникновения инцидентов, связанных с нарушением требований о защите информации.
22. 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).
23. Обеспечение целостности системы защиты информации информационной системы, включая резервирование средств защиты информации.
24. Установка обновлений программного обеспечения, включая программное обеспечение средств защиты информации, выпускаемых их разработчиками.
25. 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
26. Выполнение организационных мер по защите информации.
27. Контроль состояния защиты информации в информационной системе, включая контроль за событиями и действиями пользователей информационной системы.
28. Анализ и оценка функционирования системы защиты информации информационной системы, включая выявление и устранение недостатков в функционировании системы защиты информации информационной системы.
29. Периодический анализ уязвимостей информационной системы и оперативное принятие первоочередных мер по устранению вновь выявленных уязвимостей, приводящих к возникновению актуальных угроз безопасности.
30. 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.

31. Анализ влияния на систему защиты информации информационной системы планируемых изменений в информационной системе.
32. 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).
33. Сопровождение системы защиты информации информационной системы в ходе ее эксплуатации, включая корректировку эксплуатационной документации на нее.
34. Перечень нормативных правовых актов, методических документов и национальных стандартов, требованиям которых должна соответствовать информационная система.
35. Перечень типов объектов защиты информационной системы.
36. Требования к мерам и средствам защиты информации, применяемым в информационной системе.
37. Субъекты доступа (пользователи, процессы и иные субъекты доступа) и объекты доступа (устройства, объекты файловой системы, запускаемые и исполняемые модули, объекты системы управления базами данных, объекты, создаваемые прикладным программным обеспечением, иные объекты доступа).
38. Состав мер по защите информации, обеспечивающих блокирование (нейтрализацию) актуальных угроз безопасности информации.
39. Содержание состава мер по защите информации в соответствии с установленным классом защищенности информационной системы.
40. Организационные меры, виды и типы средств защиты информации.
41. Логическая структура, состав (количество) и места размещения элементов системы защиты информации автоматизированной системы.
42. Средства защиты информации с учетом их совместимости с информационными технологиями и техническими средствами обработки информации, функций безопасности этих средств и особенностей их реализации, а также класса защищенности информационной системы.
43. Параметры настройки средств защиты информации, обеспечивающие реализацию мер по защите информации и блокирование (нейтрализацию) актуальных угроз безопасности информации, в том числе путем устранения возможных уязвимостей информационной системы.
44. Организационная структура системы защиты информации информационной системы.
45. Состав, номенклатуру, места установки и параметры настройки средств защиты информации, программного обеспечения и технических средств обработки информации.
46. Порядок создания, удаления в информационной системе учетных записей пользователей и установления полномочий пользователей и администраторов информационной системы.
47. Порядок контроля за событиями и действиями пользователей в информационной системе.
48. Порядок обновления программного обеспечения, включая программное обеспечение средств защиты информации, в информационной системе.
49. Порядок выявления и устранения недостатков в системе защиты информации информационной системы, а также порядок внесения изменений в эксплуатационную документацию на систему защиты информации информационной системы.

50. Порядок контроля целостности системы защиты информации информационной системы и ее тестирования.
51. Правила эксплуатации системы защиты информации информационной системы, порядок ее настройки и восстановления работоспособности в случае нарушения функционирования системы защиты информации информационной системы.
52. Порядок управления параметрами настройки средств защиты информации, составом и конфигурацией технических средств обработки информации и программного обеспечения, а также контроля за несанкционированными подключениями технических средств обработки информации и установкой программного обеспечения.
53. Порядок архивирования информации конфиденциального характера, содержащейся в информационной системе, и стирания (уничтожения) данных и остаточной информации с машинных носителей информации и (или) уничтожения машинных носителей информации.
54. Проверка работоспособности и совместимости средств защиты информации с информационными технологиями и техническими средствами обработки информации.
55. Проверка выполнения средствами защиты информации требований к системе защиты информации информационной системы.

Приложение 1

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

ОТЧЕТ О ПРОХОЖДЕНИИ ПРОИЗВОДСТВЕННОЙ (ПРОЕКТНО-ТЕХНОЛОГИЧЕСКАЯ) ПРАКТИКИ

Студент группы _____ _____
Номер группы подпись ФИО

Руководитель практики от Вуза: _____
подпись ФИО

Организация (место прохождения практики): _____

Даты прохождения практики: с " " 20 г по " " 20 г

Руководитель практики от организации: _____
подпись ФИО

Москва, 20__

Приложение 2
Пример оформления задания на практику

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение
высшего образования
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
ЗАДАНИЕ НА ПРОИЗВОДСТВЕНУЮ ПРАКТИКУ (ПРОЕКТНО-ТЕХНОЛОГИЧЕСКУЮ)
по направлению 10.03.01 «Информационная безопасность»
Образовательная программа (профиль)
«Безопасность компьютерных систем»

Кафедра «Информационная безопасность»
Студент: Иванов Иван Иванович группа: ХХХ-ХХХ

ТЕМА	Личный кабинет студента ФГАОУ ВО «Московский Политех»
ПРАКТИЧЕСКИЙ РЕЗУЛЬТАТ	
Назначение	автоматизация процесса коммуникации внутри организации Заказчика.
Основные функции	авторизация пользователя в системе; построение аналитических отчетов о существующих записях работников и студентов университета на мероприятия, образовательные программы; организация внутреннего мессенджера в системе; организация системы уведомлений внутренним структурным единицам университета о запросах студентов и работников университета – заказ справки, получение выписки и т.д.; организация механизма записи на учебные и внеучебные мероприятия.
Используемые технологии и платформы	1С предприятие и «Директум» система
ВЫПОЛНЕНИЕ РАБОТЫ	
Решаемые задачи	разработка прототипа; разработка макетов дизайна; проектирование API; разработка документации
Состав технической документации	Пояснительная записка
Состав графической части	Презентация

Преподаватель: / /
подпись ФИО, уч. звание и степень

Студент: _____ /Иванов Иван Иванович группа: XXX-XXX/

подпись ФИО, группа

Приложение 3
Пример оформления титульного листа Отчета о прохождении практики

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

ОТЧЕТ О ПРОХОЖДЕНИИ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПРОЕКТНО-ТЕХНОЛОГИЧЕСКАЯ)

по направлению 10.03.01 «Информационная безопасность»
Образовательная программа (профиль)
«Безопасность компьютерных систем»

Студент группы _____ _____ _____
Номер группы ФИО подпись

Руководитель практики от Вуза: _____ _____
ФИО подпись

Организация (место прохождения практики): _____

Даты прохождения практики: с "__" _____ 20 __ по "__" _____ 20__

Руководитель практики от организации: _____ _____
ФИО подпись

Москва, 2026

Приложение 4
Пример оформления дневника практики

Дневник учебной практики

Даты проведения: _____

Студент: _____ Группа:_____

Место прохождения практики: _____

Руководитель практики от образовательной организации: _____

Руководитель практики от профильной организации: _____

Инструктаж по технике безопасности провел

_____ _____ _____
ФИО дата подпись

Инструктаж по технике безопасности провел

_____ _____ _____
ФИО дата подпись

С техникой безопасности ознакомлен

_____ _____ _____
ФИО дата подпись

Даты	Виды и основное содержание работы	Отметка о выполнении работы руководителем

Руководитель практики от образовательной организации:

_____ _____ _____
ФИО дата подпись

Руководитель практики от профильной организации:

_____ _____ _____
ФИО дата подпись

Утверждаю

_____
(ФИО)

_____
(подпись)

Приложение 5
Инструкция по ТБиОТ

Инструкция по технике безопасности и охране труда (Информационная безопасность)

Москва, 2026 г.

1 ОБЩИЕ ТРЕБОВАНИЯ ОХРАНЫ ТРУДА

К выполнению заданий в компьютерном классе допускаются участники образовательного процесса:

- прошедшие инструктаж по охране труда и технике безопасности;
- ознакомленные с инструкцией по охране труда;
- не имеющие противопоказаний к занятиям на компьютере по состоянию здоровья.

В процессе выполнения аудиторных заданий и нахождения на территории и в помещениях места проведения занятий, учащийся обязан четко соблюдать:

- инструкции по охране труда и технике безопасности;
- соблюдать личную гигиену;
- принимать пищу в строго отведенных местах.

При работе в аудитории на обучающегося могутвоздействовать следующие вредные и (или) опасные факторы:

Физические:

- повышенные уровни электромагнитного излучения;
- повышенный или пониженный уровень освещенности;
- повышенный уровень прямой и отраженной блесткости;
- неравномерность распределения яркости в поле зрения;
- повышенная яркость светового изображения;
- повышенный уровень пульсации светового потока;
- повышенное значение напряжения в электрической цепи, замыкание которой может произойти через тело человека.

Психологические:

- напряжение зрения и внимания;
- интеллектуальные и эмоциональные нагрузки;
- длительные статические нагрузки;
- монотонность труда.

При несчастном случае пострадавший или очевидец несчастного случая обязан немедленно сообщить о случившемся преподавателю.

В помещении находится аптечка первой помощи, укомплектованная изделиями медицинского назначения, ее необходимо использовать для оказания первой помощи, самопомощи в случаях получения травмы.

Несоблюдение обучающимся норм и правил ОТ и ТБ ведет к не допуску к занятию в аудитории.

2 ТРЕБОВАНИЯ ОХРАНЫ ТРУДА ПЕРЕД НАЧАЛОМ РАБОТЫ

Перед началом работы обучающийся должны выполнить следующее:

2.1. Ознакомиться с инструкцией по технике безопасности, с планами эвакуации при возникновении пожара, местами расположения санитарно- бытовых помещений, медицинскими кабинетами.

По окончании ознакомительного периода, обучающиеся подтверждают свое ознакомление со всеми процессами, подписав лист прохождения инструктажа по работе на оборудовании по форме, определенной в приложении А.

2.2. Подготовить рабочее место:

- убрать все посторонние предметы, которые могут отвлекать внимание и затруднять работу;
- проверить правильность установки стола, стула и, при необходимости, провести регулировку;
- отрегулировать освещенность, убедиться в достаточной освещенности, отсутствии отражений на экране, отсутствии встречного светового потока;

2.3. Подготовить оборудование:

Таблица 1 – Правила подготовки оборудования

Наименование оборудования	Правила подготовки
Персональный компьютер (мониторы, системный блок, клавиатура, мышь)	Проверить правильность подключения оборудования к электросети (кабели электропитания, удлинители, сетевые фильтры должны находиться с тыльной стороны рабочего места);

Монитор	Расположить на расстоянии не менее 50 см от глаз (оптимально 60-70 см).
Клавиатура	Расположить на поверхности стола на расстоянии 100-300 мм от края, обращенного к пользователю.

2.4. О замеченных недостатках и неисправностях немедленно сообщить преподавателю и до устранения неполадок к работе за компьютером не приступать.

3 ТРЕБОВАНИЯ ОХРАНЫ ТРУДА ВО ВРЕМЯ РАБОТЫ

3.1. При работе обучающегося в аудитории, необходимо соблюдать требования безопасности при работе на персональном компьютере:

Таблица 2 – Требования безопасности

Наименование оборудования	Требования безопасности
Системный блок, монитор	Держать открытыми все вентиляционные отверстия устройств. При необходимости прекращения работы на некоторое время корректно закрыть все активные задачи. Запрещается: – касаться одновременно экрана монитора и клавиатуры; – прикасаться к задней панели системного блока при включенном питании; – переключение разъемов интерфейсных кабелей периферийных – устройств при включенном питании; – производить отключение питания во время выполнения активной задачи; – производить частые переключения питания; – допускать попадание влаги на поверхность системного блока, монитора, рабочую поверхность клавиатуры, дисковода, принтера и др. устройств; – производить самостоятельное вскрытие и ремонт оборудования;

3.2. Суммарное время непосредственной работы с персональным компьютером и другой оргтехникой в течение дня должно быть не более 6 часов.

Продолжительность непрерывной работы с персональным компьютером и другой оргтехникой без регламентированного перерыва не должна превышать 2-х часов. Через каждые 2 часа работы следует делать регламентированный перерыв продолжительностью 15 мин.

3.3. При работе за компьютером:

- необходимо быть внимательным, не отвлекаться посторонними разговорами и делами, не отвлекать других учащихся;
- соблюдать настоящую инструкцию;
- соблюдать правила эксплуатации оборудования;
- поддерживать порядок и чистоту на рабочем месте;
- работать только на исправном оборудовании.

4 ТРЕБОВАНИЯ ОХРАНЫ ТРУДА В АВАРИЙНЫХ СИТУАЦИЯХ

4.1. При обнаружении неисправности в работе электрических устройств, находящихся под напряжением (повышенном их нагреве, появления искрения, запаха гари, задымления и т.д.), обучающемуся следует немедленно отключить питание и сообщить о случившемся преподавателю. Работу продолжить только после устранения возникшей неисправности.

4.2. В случае возникновения у обучающего плохого самочувствия или получения травмы сообщить об этом преподавателю.

4.3. При поражении обучающегося электрическим током немедленно отключить электросеть, оказать первую помощь (самопомощь) пострадавшему, сообщить преподавателю, при необходимости обратиться к врачу.

4.4. При несчастном случае или внезапном заболевании необходимо в первую очередь отключить питание электрооборудования, сообщить о случившемся преподавателю, который должен принять мероприятия по оказанию первой помощи пострадавшим, вызвать скорую медицинскую помощь, при необходимости отправить пострадавшего в ближайшее лечебное учреждение.

4.5. При возникновении пожара необходимо немедленно оповестить преподавателя. При последующем развитии событий следует руководствоваться указаниями преподавателя. Приложить усилия для исключения состояния страха и паники.

При обнаружении очага возгорания в аудитории необходимо любым возможным способом постараться загасить пламя с обязательным соблюдением мер личной безопасности.

При возгорании одежды попытаться сбросить ее. Если это сделать не удается, упасть на пол и, перекатываясь, сбить пламя; необходимо накрыть горящую одежду куском плотной ткани, облиться водой, запрещается бежать

– бег только усилит интенсивность горения.

В загоревшемся помещении не следует дожидаться, пока приблизится пламя. Основная опасность пожара для человека – дым. При наступлении признаков удушья лечь на пол и как можно быстрее ползти в сторону эвакуационного выхода.

4.6. При обнаружении взрывоопасного или подозрительного предмета не подходите близко к нему, предупредите о возможной опасности преподавателя и окружающих людей.

При происшествии взрыва необходимо спокойно уточнить обстановку и действовать по указанию преподавателя, при необходимости эвакуации возьмите с собой документы и предметы первой необходимости, при передвижении соблюдайте осторожность, не трогайте поврежденные конструкции, оголившиеся электрические провода. В разрушенном или поврежденном помещении не следует пользоваться открытым огнем (спичками, зажигалками и т.п.).

5 ТРЕБОВАНИЕ ОХРАНЫ ТРУДА ПО ОКОНЧАНИИ РАБОТ

После окончания занятий каждый обучающийся обязан:

5.1 Привести в порядок рабочее место.

5.2 Произвести закрытие всех активных задач

5.3 Сообщить преподавателю о выявленных во время работы неполадках и неисправностях оборудования и инструмента, и других факторах, влияющих на безопасность занятий.

Приложение 6
Комплекс упражнений для производственной гимнастики

Комплекс упражнении производственной гимнастики

Внимание! Данные комплекс упражнений не учитывает всех особенностей индивидуального физического развития и наличие хронических заболеваний. Перед применением проконсультируйтесь со специалистом.

Комплекс упражнений для глаз № 1

- периодически (раз в 60-120 минут) переключать зрение с близкого на дальнее – просто смотреть вдаль в течение 5-7 минут;
- максимально зажмурить, затем широко открыть глаза; повторить 10 раз;
- делать движения глазами вверх/вниз, влево/вправо, вращать ими по часовой стрелке и против нее; каждое движение повторить по 10 раз;
- свести глаза к носу (попытаться посмотреть на собственную переносицу), расслабить глаза; повторить 10 раз.

Комплекс упражнений для глаз № 2

Перед выполнением упражнений сядьте удобно, выпрямите спину и расслабьтесь. Поморгайте глазами быстро, затем медленно. Упражнения выполняются тщательно и медленно.

Глаза вверх, вниз – 2 раза. Поморгали глазами.

Глаза вправо, влево – 2 раза. Поморгали глазами.

Рисуем глазами квадрат – 2 раза по часовой стрелке. Поморгали глазами.

Рисуем глазами квадрат - 2 раза против часовой стрелки. Поморгали глазами.

Рисуем глазами круг по часовой стрелке – 2 раза. Поморгали глазами.

Рисуем глазами круг против часовой стрелки – 2 раза. Поморгали глазами.

Рисуем глазами волнистую змейку в правую сторону, а затем в левую. Поморгали глазами.

Теперь несильно потрите глаза кулачками. Разогрейте ладони, потирая их друг о друга и приложите их к глазам так, чтобы не проникал свет, и повторите все вышеперечисленные упражнения по три раза.

Не снимая ладони с глаз, расслабьтесь, представьте себя в лесу или на берегу моря, подумайте о чем-нибудь хорошем. Можно помедитировать.

Затем, часто моргая, откройте глаза. Резко не вставайте. Для того, чтобы не просто снять напряжение с глаз, но и улучшить зрение, выполняйте упражнения 2-3 раза в день, до еды, чтобы глаза омывала голодная кровь.

Для работников умственного труда

1. потягивание, руки подняты над головой, кисти сцеплены "в замок" - вдох, руки опускают - выдох.
2. ногу отставляют в сторону на носок, руки за голову - вдох, опуская руки и приставляя ногу - выдох.
3. руки вытянуты вперед, кисти расслаблены и опущены вниз. Приседая, руки вниз - выдох, выпрямляясь, руки назад, поднимаются на носки - вдох.
4. прыжки на месте на носках, руки на поясе.
5. руки в стороны, повороты туловища и головы попеременно вправо и влево.
6. поднимая руки вверх, прогибаются назад - вдох, зачем наклоняются впе-ред, держа руки на поясе - выдох.

7. -ноги расставлены на ширину плеч, руки перед грудью. Попеременно отво-дя то правую, то левую руку в сторону, делают вдох, опуская руки - выдох.

Каждое упражнение повторяют 6-12 раз. Перед началом и в конце занятия" спокойная ходьба, после 4-5 упражнений для людей, более физически подготов-ленных, - ускоренная ходьба или бег 1-3 мин.

Для работников офиса

1. голова поочередно наклоняется во все стороны (в правую, левую, назад и вперед), а затем медленно вращается по часовой, а затем против часовой стрелки;
2. аналогичное вращение кистей рук (сначала одной, потом другой, затем обеими – также со сменой направления);
3. повороты корпуса в одну и другую сторону с одновременным выбрасыванием в сторону поворота руки (правой – при повороте влево, и наоборот);
4. расслабление и напряжение мышц живота (можно выполнять, даже не вставая со стула);
5. также сидя на стуле, немного приподнять вытянутые ноги и опустить их на место, повторив упражнение несколько раз;
6. повторить упражнение для кистей рук, но уже применительно к щиколоткам (повороты и вращения в обе стороны);
7. 10-15 раз поочередно приподняться на носках, а затем на пятках;
8. сделать несколько легких прыжков на месте;
9. поставив ноги на уровне ширины плеч и руки на пояс, наклониться вперед, назад, влево и вправо;
10. сделать несколько вращений бедрами (по часовой стрелке и против нее);
11. походить на месте;

12. сделать несколько махов руками;
13. поприседать (количество раз – в зависимости от готовности, возраста и конституции тела);
14. наклониться, постаравшись дотянуться кончиками пальцев до пола;
15. сев на стул, закрыть глаза и расслабленно посидеть около 30 секунд;
16. поочередно 10-15 раз зажмуриваться и широко распахивать глаза;
17. поводить взглядом по кругу (в одну, а затем в другую сторону);
18. сосредоточиться взглядом на каких-либо далеких предметах.

В комплекс физкультурной паузы следует включать такие упражнения, которые влияли бы иначе, чем трудовые движения, воздействовали на другие мышечные группы и части тела, так как принцип активного отдыха наиболее эффективно реализуется при переключении с одного вида деятельности на другой.

Для 1-й группы профессий: вводную гимнастику - перед началом работы; через 2,5 - 3 ч. - физкультурную паузу, затем в середине 2-й половины рабочего дня - вторую физкультурную паузу (с меньшей интенсивностью);

Для 2-й группы профессий: перед работой - вводную гимнастику; через 2 ч. работы - физкультурную паузу; вторую физкультурную паузу - во 2-й половине дня и (по необходимости) физкультминутки;

Для 3-й группы профессий: через 1,5 - 2 ч. работы физкультурную паузу, физкультминутки (по мере необходимости) и пассивный отдых в сочетании с активным;

Для 4-й группы профессий: сначала вводная гимнастика, через 3-3,5 ч.

- физкультурная пауза; во 2-й половине дня - физкультпауза и физкультминутки (по мере необходимости).

Вводная гимнастики, в данном случае, это утренняя гимнастика, перед началом трудового дня.

Особенностью занятий является прежде всего то, что они проводятся непосредственно после работы или до нее, в цехе (отделе, заводской лаборатории и др.), в обычных рабочих костюмах, со всем составом рабочих или служащих (мужчины, женщины) самого различного возраста, состояния здоровья и физической подготовленности.

Занятия гимнастикой в режиме труда немыслимы без тщательного врачебного контроля, который осуществляет врач медицинской части или заводской поликлиники, а также методист или общественный инструктор. Улучшение здоровья, физического развития рабочих и служащих, уменьшение заболеваемости и производственного травматизма — самый важный итог занятий производственной гимнастикой.