

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Пашнанов Эрдне Лиджиевич
Должность: И.о. директора филиала
Дата подписания: 01.08.2024 13:54:40
Уникальный программный ключ:
f29e48b9891aa9797b1ae9fac0693fa267ac161d

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное
учреждение инклюзивного высшего образования

**«Российский государственный
университет социальных технологий»**

КАЛМЫЦКИЙ ФИЛИАЛ ФГБОУ ИВО «РГУ СоцТех»

УТВЕРЖДАЮ

И.о. директора филиала

Э.Л Пашнанов


«__» _____ 2024 г.

**РАБОЧАЯ ПРОГРАММА
ПРАКТИЧЕСКОЙ ПОДГОТОВКИ
(ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ)
ПМ 02 ПРИМЕНЕНИЕ ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ
ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В
АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ
по специальности
10.02.05 Обеспечение информационной безопасности
автоматизированных систем
квалификация – техник по защите информации**


г. Элиста, 2024 г.

ОДОБРЕНА
Предметно-цикловой комиссией
цифровых технологий и
кибербезопасности

Разработана на основе Федерального
государственного образовательного
стандарта среднего
профессионального
образования по специальности
10.02.05 Обеспечение
информационной безопасности
автоматизированных систем

протокол № 8
от « 13 » 03 2024 г.
председатель предметно-цикловой
комиссии
Ц.Ю. Катрикова /  /
подпись

Одобрена научно-методическим советом

Протокол № 5
от « 20 » 03 2024 г.
Заместитель директора по
учебно-методической работе  /Н.С.Бамбушева/

составитель:

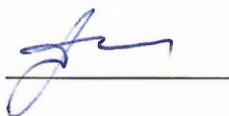


В.В. Пипенко, высшая квалификационная категория,
преподаватель Калмыцкого филиала ФГБОУ ИВО
«Российский государственный университет социальных
технологий»



О.Н. Вепрева, высшая квалификационная категория,
преподаватель Калмыцкого филиала ФГБОУ ИВО
«Российский государственный университет социальных
технологий»

рецензенты:



К.Б. Дундуев, высшая квалификационная категория,
преподаватель Калмыцкого филиала ФГБОУ ИВО
«Российский государственный университет социальных
технологий»



Агеев С.С., заместитель начальника отдела программного
обеспечения и защиты информации Министерства финансов
Республики Калмыкия

РЕЦЕНЗИЯ

на рабочую программу по производственной практике (по профилю специальности) по профессиональному модулю ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами для специальности СПО 10.02.05 Обеспечение информационной безопасности автоматизированных систем, разработанную преподавателем Калмыцкого филиала ФГБОУ ИВО «Российский государственный университет социальных технологий» Пипенко В.В.

Представленная рабочая программа производственной практики (по профилю специальности) по профессиональному модулю ПМ. 02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами разработана с учетом требований Федерального государственного образовательного стандарта по специальности среднего профессионального образования 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Структура рабочей программы соответствует структуре примерных программ профессиональных модулей среднего профессионального образования.

В общей характеристике рабочей программы сформулированы цели и планируемые результаты освоения производственной практики (по профилю специальности), виды работ, обеспечивающих формирование профессиональных компетенций, количество часов, коды формируемых компетенций, формы и методы контроля.

Объем производственной практики (по профилю специальности) и виды работ, предусмотренные ФГОС СПО и учебным планом по специальности, соответствуют тематическому содержанию производственной практики (по профилю специальности).

Содержание программы направлено на приобретение обучающимися знаний, умений, общих и профессиональных компетенций, определенных ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем и соответствует объему часов, указанному в рабочем учебном плане.

Материально-техническое обеспечение включает наличие рабочего места, оснащенного оборудованием и техническими средствами обучения.

Информационное обеспечение обучения содержит современный перечень основных печатных источников, дополнительных печатных источников и электронных источников.

Контроль и оценка результатов освоения производственной практики (по профилю специальности) содержит результаты (освоенный практический опыт) и методы оценки результатов обучения и осуществляется преподавателем в процессе проведения различных видов работ.

Рабочая программа позволит студентам в достаточной мере освоить виды работ, овладеть общими и профессиональными компетенциями, необходимых для качественного освоения программы подготовки специалистов среднего звена.

Рабочая программа производственной практики (по профилю специальности) рекомендуется к применению в учебном процессе Калмыцкого филиала ФГБОУ ИВО «Российский государственный университет социальных технологий».

Рецензент



С.С. Агеев, заместитель начальника отдела программного обеспечения и защиты информации Министерства финансов Республики Калмыкия

РЕЦЕНЗИЯ

на рабочую программу по производственной практике (по профилю специальности) по профессиональному модулю ПМ. 02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами для специальности СПО 10.02.05 Обеспечение информационной безопасности автоматизированных систем, разработанную преподавателем Калмыцкого филиала ФГБОУ ИВО «Российский государственный университет социальных технологий» Пипенко В.В.

Представленная рабочая программа производственной практики (по профилю специальности) по профессиональному модулю ПМ. 02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами разработана с учетом требований Федерального государственного образовательного стандарта по специальности среднего профессионального образования 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Структура рабочей программы соответствует структуре примерных программ профессиональных модулей среднего профессионального образования.

В общей характеристике рабочей программы сформулированы цели и планируемые результаты освоения производственной практики (по профилю специальности), виды работ, обеспечивающих формирование профессиональных компетенций, количество часов, коды формируемых компетенций, формы и методы контроля.

Объем производственной практики (по профилю специальности) и виды работ, предусмотренные ФГОС СПО и учебным планом по специальности, соответствуют тематическому содержанию производственной практики (по профилю специальности).

Содержание программы направлено на приобретение обучающимися знаний, умений, общих и профессиональных компетенций, определенных ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем и соответствует объему часов, указанному в рабочем учебном плане.

Материально-техническое обеспечение включает наличие рабочего места, оснащенного оборудованием и техническими средствами обучения.

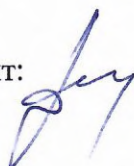
Информационное обеспечение обучения содержит современный перечень основных печатных источников, дополнительных печатных источников и электронных источников.

Контроль и оценка результатов освоения производственной практики (по профилю специальности) содержит Результаты (освоенный практический опыт) и Методы оценки результатов обучения и осуществляется преподавателем в процессе проведения различных видов работ.

Рабочая программа позволит студентам в достаточной мере освоить виды работ, овладеть общими и профессиональными компетенциями, необходимых для качественного освоения программы подготовки специалистов среднего звена.

Рабочая программа производственной практики (по профилю специальности) рекомендуется к применению в учебном процессе Калмыцкого филиала ФГБОУ ИВО «Российский государственный университет социальных технологий».

Рецензент:



К. Б. Дундуев высшая квалификационная категория, преподаватель Калмыцкого филиала ФГБОУ ИВО «Российский государственный университет социальных технологий»

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ
ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПО ПРОФИЛЮ
СПЕЦИАЛЬНОСТИ)
2. СТРУКТУРА И СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ
ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПО ПРОФИЛЮ
СПЕЦИАЛЬНОСТИ)
3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ
ПРАКТИКИ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ)
4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ
ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПО ПРОФИЛЮ
СПЕЦИАЛЬНОСТИ)

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ)

1.1. Цель и планируемые результаты освоения профессионального модуля

1.1.1. В результате изучения профессионального модуля студент должен освоить вид деятельности Защита информации в автоматизированных системах программными и программно-аппаратными средствами и соответствующие ему профессиональные компетенции:

Код	Наименование видов деятельности и профессиональных компетенций
ВД 2	Защита информации в автоматизированных системах программными и программно-аппаратными средствами
ПК 2.1.	Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.
ПК 2.2.	Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.
ПК 2.3.	Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.
ПК 2.4.	Осуществлять обработку, хранение и передачу информации ограниченного доступа.
ПК 2.5.	Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.
ПК 2.6.	Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

1.1.2. Общие компетенции

Код	Наименование видов деятельности и профессиональных компетенций
ОК 01.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 02.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 03.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 04.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 05.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 06.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.
ОК 07.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 08.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.
ОК 09.	Использовать информационные технологии в профессиональной деятельности.
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языках.

ОК 11.	Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере.
--------	---

1.1.3. В результате освоения профессионального модуля студент должен:

Иметь практический опыт	<ul style="list-style-type: none"> – установки, настройки программных средств защиты информации в автоматизированной системе; – обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами; – тестирования функций, диагностика, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации; – решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации; – применения электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных; – учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности; – работы с подсистемами регистрации событий; – выявления событий и инцидентов безопасности в автоматизированной системе.
уметь	<ul style="list-style-type: none"> – устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; – устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; – диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации; – применять программные и программно-аппаратные средства для защиты информации в базах данных; – проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; – применять математический аппарат для выполнения криптографических преобразований; – использовать типовые программные криптографические средства, в том числе электронную подпись; – применять средства гарантированного уничтожения информации; – устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; – осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак
знать	<ul style="list-style-type: none"> – особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;

	<ul style="list-style-type: none"> – методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации; – типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации; – основные понятия криптографии и типовых криптографических методов и средств защиты информации; – особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации; – типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа.
--	--

1.1.4. Базы производственной практики (по профилю специальности):

- Министерство финансов Республики Калмыкии
- ФКУ «Главное бюро медико-социальной экспертизы по Республике Калмыкия» Министерство труда и социальной защиты Российской Федерации
- Отдел по вопросам миграции Управления МВД
- ПАО Ростелеком
- Автономное учреждение РК «Многофункциональный центр предоставления государственных и муниципальных услуг»
- КУ РК «Центр учета и отчетности в организациях государственного сектора»
- МКУ «Дирекция единого заказчика»
- МКУ «Центр занятости населения», с.Троицкое
- Бюджетное учреждение РК «Республиканская больница им. П.П. Жемчуева»
- Отделение - Национальный Банк по РК Южного главного управления ЦБ РФ
- ООО «Юг-Сельхоз» (Зеленая точка)
- ООО «Зерновая компания»
- Управление Федеральной службы государственной регистрации, кадастра и картографии по РК
- ООО «Интерстрой»
- ООО «Золотая жемчужина» г. Москва с последующим трудоустройством
- ООО «Движение»
- БТИ

Прохождение практики осуществляется в соответствии с учебным планом и утвержденной программой практики и завершается составлением отчета о практике. Formой промежуточной аттестации по производственной практики (по профилю специальности) является дифференцированный зачет.

1.2. Цель и задачи производственной практики (по профилю специальности) по профессиональному модулю 02 Защита информации в

автоматизированных системах программными и программно-аппаратными средствами.

Целями производственной практики (по профилю специальности) по профессиональному модулю 02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами являются:

- закрепление теоретических знаний, полученных при изучении профессионального модуля;
- формирование у обучающихся умений, приобретение практического опыта в рамках профессионального модуля 02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами.

Задачами производственной практики (по профилю специальности) по профессиональному модулю 02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами являются:

- формирование и закрепление навыков профессиональной деятельности специалиста в области Применение инженерно-технических средств обеспечения информационной безопасности;
- развитие коммуникативных, организационных, деловых качеств у обучающихся.

1.3. Рекомендуемое количество часов на освоение рабочей программы производственной практики (по профилю специальности) по профессиональному модулю 02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами.

Бюджет времени на производственную практику (по профилю специальности) по профессиональному модулю 02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами для получения профессиональных умений и навыков определен в объеме 144 часа.

2. СТРУКТУРА И СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ)

2.1. Тематический план и содержание производственной практики (по профилю специальности) по профессиональному модулю 01 Эксплуатация подсистем безопасности автоматизированных систем

№	Наименование профессиональных компетенций	Виды работ, обеспечивающих формирование ПК	Кол-во часов	Коды формируемых компетенций	Формы и методы контроля
1.	Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.	Выполнение задач по управлению различной информацией; Делать правильный выбор в методах защиты информации; Выполнять задачи по обнаружению основных уязвимостей операционных систем; Выполнение настройки аппаратной части для безопасной работы в сети.	24	ОК 01 - 11 ПК 2.1	Оценка руководителя практики Защита отчета по производственной практике (по профилю специальности).
2.	Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.	Выполнение различных настроек для защиты системы; Выполнение настройки идентификации и аутентификации пользователей; Правильно охарактеризовать каналы утечки информации; Использование различных способов доступа; Выявление способности организовать защиту данных в сети; Своевременное реагирование на возможные атаки; Выполнение технического контроля эффективности защиты	24	ОК 01 - 11 ПК 2.2	Оценка руководителя практики Защита отчета по производственной практике (по профилю специальности).

		информации.				
3.	Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.	Выполнение оценки эффективности применения средств обеспечения информационной безопасности; Оценка концептуальной модели информационной безопасности; Осуществление защиты передаваемой информации; Планирование защиты информации от несанкционированного доступа.	24	ОК 01 - 11	ПК 2.3	Оценка руководителя практики Защита отчета по производственной практике (по профилю специальности).
4.	Осуществлять обработку, хранение и передачу информации ограниченного доступа.	Соблюдение правил ведения обеспечения учета, документации установленного образца; Проведение анализа опасных факторов; Применение безопасных приемов обеспечения учета конфиденциальной информации; Обработка и хранение конфиденциальной информации; Выполнение задач по защищенной передаче конфиденциальной информации.	24	ОК 01 - 11	ПК 2.4	Оценка руководителя практики Защита отчета по производственной практике (по профилю специальности).
5.	Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.	Выполнение передачи данных различными способами; Правильность обслуживания различных типов локальных сетей; Выполнение плановых и внеплановых проверок объектов; Построение локальной компьютерной сети; Решение технических проблем при эксплуатации систем.	36	ОК 01-11	ПК 2.5	Оценка руководителя практики Защита отчета по производственной практике (по профилю специальности).
6.	Осуществлять регистрацию основных событий в автоматизированных (информационных)	Осуществление организационного и правового обеспечения информационной безопасности систем в	36	ОК 01 - 11	ПК 2.6	Оценка руководителя практики Защита отчета по

	<p>системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.</p>	<p>рамках должностных обязанностей по защите информации; Применение нормативных, правовых актов и нормативных методических документов в области защиты информации; Выявление каналов утечки информации на объекте защиты; Организация осуществления контроля над соблюдением персоналом требований режима защиты информации; Правильность оформления документации по регламентации мероприятий и оказанию услуг в области защиты информации.</p>				<p>производственной практике(по профилю специальности).</p>
ИТОГО			144			

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ)

3.1. Требования к минимальному материально-техническому обеспечению и организации производственной практики (по профилю специальности) по профессиональному модулю 02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами.

Реализация производственной практики (по профилю специальности) по профессиональному модулю 02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами осуществляется в соответствии с заключенным договором сотрудничества с базовыми предприятиями, имеющими отделы информационной безопасности.

Необходимое оборудование и техническое оснащение рабочих мест на базах практик для проведения производственной практики (по профилю специальности):

- Положение о практике обучающихся филиала федерального государственного бюджетного образовательного учреждения инклюзивного высшего образования «Российский государственный университет социальных технологий»;

- Рабочая программа производственной практики (по профилю специальности) по профессиональному модулю 02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами;

- комплект образцов документов;
- специализированное программное обеспечение
- автоматизированные рабочие места студентов-практикантов.

3.2. Информационное обеспечение обучения

3.2.1. Основные печатные источники

1. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2018. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8.

3.2.2. Дополнительные печатные источники:

1. Васильков А.В., Васильков И.А. Безопасность и управление доступом в информационных системах: учебное пособие/ А.В.Васильков, И.А.Васильков.- М.: ФОРУМ,2010.- 368с.- (Профессиональное образование)
2. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. —

- Москва : Издательство Юрайт, 2019. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/431080> (дата обращения: 16.12.2019).
3. Введение в криптографию/под.ред.В.В.Яценко/СПб.:Питер,2001.-288с.
 4. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
 5. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
 6. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
 7. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
 8. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».
 9. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
 10. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
 11. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».
 12. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.
 13. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.
 14. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
 15. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 83.
 16. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 84.
 17. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России

- от 30 августа 2002 г. № 282.
18. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
 19. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489.
 20. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.
 21. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.
 22. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 2. Программное обеспечение базовых систем ввода-вывода персональных электронно-вычислительных машин. Классификация по уровню контроля отсутствия недеklarированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.
 23. Приказ ФАПСИ при Президенте Российской Федерации от 13 июня 2001 г. № 152 «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».
 24. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».
 25. ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий
 26. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий
 27. ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер
 28. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети
 29. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью
 30. ГОСТ Р ИСО/МЭК 15408-1-2008 Информационная технология. Методы и

- средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель
- 31.ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности
 - 32.ГОСТ Р ИСО/МЭК 15408-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности
 - 33.ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"
 - 34.Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.
 - 35.Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.
 - 36.ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
 - 37.ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
 - 38.Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 20ми02.
 - 39.Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
 - 40.Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
 - 41.Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.
 - а) программное обеспечение: специализированное программное обеспечение для проверки защищенности помещений от утечки информации по акустическому и виброакустическому каналам, специальных исследований средств вычислительной техники;
 - б) базы данных, информационно-справочные и поисковые системы: www.fstec.ru; www.gost.ru/wps/portal/tk362.
 - 42.Хорев П. Б. Методы и средства защиты информации в компьютерных системах. - М.: Академия, 2016.
 - 43.Голицына О.Л., Максимов Н.В., Попов И.И. «Базы данных» - Форум-

Инфра-М, 2019 г.

44. Нечаев В. И. Элементы криптографии. Основы теории защиты информации. - М.: Высшая школа, 2019.
45. В.Г. Жельников Криптография от папируса до компьютера. - М.: АБФ, 2016.
46. Гринберг А.С. Защита информационных ресурсов государственного управления: учебное пособие для ВУЗов - М: ЮНИТИ-Дата, 2018.
47. Галатенко В.А. Стандарты информационной безопасности - М: ИНТУИТ.РУ, 2019.
48. Кулагин В.М. Международная безопасность: учебное пособие - М: Аспект-Пресс, 2016.
49. Гришина Н.В. Организация комплексной защиты информации - М: Гелиос АРВ, 2017

3.2.3. Электронные источники:

1. <http://wm-help.net/books-online/book/98618/98618-7.html> - принципы защиты операционных систем
 2. <http://rudocs.exdat.com/docs/index-56877.html> - принципы построения операционных систем
 3. <http://www.winblog.ru/2006/08/21/21080608.html> - система парольной защиты
 4. <http://emanual.ru/download/6661.html> - средства безопасности для защиты сервисов
 5. <http://www.supermegayo.ru/vlomprogr/3.html> - Атаки на программное обеспечение.
 6. http://www.ab-solutions.ru/artides/information_security/ - Методы обеспечения информационной безопасности предприятия.
 7. <http://www.xnets.ru/plugins/content/content.php?content.113.3> - Сите безопасности Windows
 8. http://mitilan.blogspot.ru/2010/03/solaris-10_15.html - Реализация базовых функций по обеспечению безопасности Solaris.
 9. <http://asher.ru/security/book/its/08> - приемы обеспечения безопасности информационных систем.
 10. <http://itteach.ru/bazi-dannich/sozдание-zaprosov-v-bd/vse-stranitsi> - Запросы. Виды запросов. Создание запросов.
 11. <http://bd.gvm5cheb.ru/p18aa1.html> - Запрос на выборку. Групповые операции.
 12. <http://www.bnti.ru/showart.asp?aid=660&lvl=03.03>. - Технические каналы утечки информации при передаче ее по каналам связи.
- <http://www.bnti.ru/showart.asp?aid=957&lvl=03>. - Технические каналы утечки речевой информации.

3.3. Общие требования к организации производственной практики (по профилю специальности) по профессиональному модулю 01 Эксплуатация подсистем безопасности автоматизированных систем

Реализация производственной практики (по профилю специальности) по профессиональному модулю 02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами предполагает проведение производственной практики после освоения всего модуля на базовых предприятиях Калмыцкого филиала РГУ СоцТех концентрировано по окончании освоения теоретического курса обучения.

Производственная практика (по профилю специальности) по профессиональному модулю 02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами завершается дифференцированным зачетом.

По результатам производственной практики (по профилю специальности) по профессиональному модулю 02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами руководителями от организации и Филиала формируется аттестационный лист, содержащий сведения об уровне освоения обучающимся профессиональных компетенций.

По результатам производственной практики (по профилю специальности) по профессиональному модулю 02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами обучающимся составляется дневник-отчет, который утверждается организацией (учреждением).

Дневник-отчет оформляется в рукописном или печатном виде, формата А4, шрифт 14 Times New Roman, 1,0 интервал. Поля: верхнее, нижнее, левое – 20 мм, правое – 10 мм. Все страницы дневника-отчета нумеруются арабскими цифрами по порядку. Номер страницы проставляется в центре нижней части листа без точки (Приложение 2). Титульный лист является первой страницей дневника-отчета и не нумеруется (Приложение 1).

Дневник-отчет о прохождении производственной практики (по профилю специальности) подписывает руководитель практики от организации (учреждения).

3.4. Особенности обучения инвалидов и лиц с ограниченными возможностями здоровья

Учебные занятия инвалидов и лиц с ограниченными возможностями здоровья организуются совместно с другими обучающимися в учебных группах, а также индивидуально, в соответствии с графиком индивидуальных занятий.

При этом необходимо учитывать несколько аспектов:

- особенности нозологии обучающихся инвалидов и лиц с ограниченными возможностями здоровья;

- психоэмоциональное состояние обучающихся;
- психологический климат, который сложился в студенческой группе;
- настрой отдельных обучающихся и группы в целом на процесс обучения.

При организации учебных занятий в учебных группах используются социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений, создания комфортного психологического климата в группе.

В образовательной деятельности применяются материально-техническое оснащение, специализированные технические средства приема-передачи учебной информации в доступных формах для обучающихся с различными особенностями здоровья, электронные образовательные ресурсы в адаптированных формах.

Специфика обучения инвалидов и обучающихся с ограниченными возможностями здоровья предполагает использование игрового, практико-ориентированного, занимательного материала, который необходим для получения знаний и формирования необходимых компетенций. Подготовка обучающимися заданий для учебных занятий должна сочетать устные и письменные формы в соответствии с их особенностями здоровья.

Для того чтобы предотвращать наступление у обучающихся с инвалидностью и обучающихся, имеющих ограниченные возможности здоровья, быстрого утомления можно использовать следующие методы работы:

- чередование умственной и практической деятельности;
- преподнесение материала с использованием средств наглядности;
- использование технических средств обучения, чередование предъявляемой на слух информации с наглядно-демонстрационным материалом.

При освоении дисциплин инвалидами и лицами с ограниченными возможностями здоровья большое значение должно отводиться проведению с ними индивидуальной работы со стороны преподавателей. В индивидуальную работу включается:

- индивидуальная учебная работа (консультации), то есть дополнительное разъяснение учебного материала и углубленное изучение материала с теми обучающимися, которые в этом заинтересованы;
- индивидуальная воспитательная работа.

Особенности обучения обучающихся с нарушениями опорно-двигательного аппарата.

Для обучающегося, имеющего нарушения опорно-двигательного аппарата, необходимо посоветовать использовать вспомогательные средства для усвоения программы, например, диктофон и другие электронные носители информации.

При проведении аудиторных занятий с обучающимися, имеющими осложнения с моторикой рук, возможно использование следующих вариантов работы:

- обеспечение обучающихся электронными текстами лекций и заданий к учебным занятиям;
- использование технических средств фиксации текста (диктофоны) с последующим составлением тезисов лекции в ходе самостоятельной работы обучающегося, которые они впоследствии могут использовать при подготовке и ответах на учебных занятиях.

Одним из видов работы для обучающихся, испытывающих трудности в письме может быть подготовка к учебным занятиям таких заданий, которые не требуют от них написания длинных текстов ответов. Наиболее оптимальным вариантом такого задания, выполняемого в письменной форме, может служить тестовое задание. Использование тестирования обучающихся необходимо совмещать с обсуждением вариантов ответов.

Контроль знаний можно вести как в устном, так и в письменном виде.

Особенности обучения обучающихся с нарушением слуха.

При организации образовательного процесса со слабослышащей аудиторией рекомендуется использовать следующие педагогические принципы:

- наглядности преподаваемого материала;
- индивидуального подхода к каждому обучающемуся;
- использования информационных технологий;
- использования учебных пособий, адаптированных для восприятия обучающимися с нарушением слуха.

Обучающемуся с нарушением слуха следует предложить занять место на передних партах аудитории, а преподавателю больше времени находиться рядом с рабочим местом этого обучающегося. Учитывая, что такие обучающиеся лучше понимают по губам, желательно располагаться к ним лицом, говорить громко и четко.

Для повышения уровня восприятия учебной информации обучающимися рассматриваемой группы, рекомендуется применение звукоусиливающей аппаратуры, мультимедийных и других средств. Сложные для понимания темы следует снабжать как можно большим количеством наглядного материала. Особую роль в обучении лиц с нарушенным слухом, играют видеоматериалы. По возможности, предъявляемая видеoinформация может сопровождаться текстовой бегущей строкой или сурдологическим переводом.

Контроль знаний обучающихся указанной нозологии может вестись преимущественно в письменном виде, но для развития устной речи, рекомендуется предложить обучающемуся рассказать ответ на задание в тезисах.

Особенности обучения обучающихся с нарушением зрения.

Специфика обучения слабовидящих обучающихся заключается в следующем:

- необходимо дозировать учебную нагрузку;

- применять специальные формы и методы обучения, технические средства, позволяющие воспринимать информацию, а также оптические и тифлопедагогические устройства, расширяющие познавательные возможности обучающихся;

- увеличивать искусственную освещенность помещений, в которых занимаются обучающиеся с пониженным зрением.

При зрительной работе у слабовидящих обучающихся быстро наступает утомление, что снижает их работоспособность, поэтому необходимо проводить небольшие перерывы или переключение рабочей активности.

При чтении лекций, слабовидящим обучающимся следует разрешить использовать звукозаписывающие устройства и компьютеры, как способ конспектирования, во время занятий. Необходимо комментировать свои жесты и надписи на доске и передавать словами то, что часто выражается мимикой и жестами.

При работе на компьютере следует использовать принцип максимального снижения зрительных нагрузок, дозирование и чередование зрительных нагрузок с другими видами деятельности. Кроме того необходимо использовать специальные программные средства для увеличения изображения на экране или для озвучивания информации.

При проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья обеспечивается выполнение следующих дополнительных требований в зависимости от индивидуальных особенностей обучающихся:

1. информация по порядку проведения процедуры оценивания предоставляется в доступной форме (устно, в письменной форме, на электронном носителе, в печатной форме увеличенным шрифтом и т.п.);

2. доступная форма предоставления заданий оценочных средств (в печатной форме, в печатной форме увеличенным шрифтом, в форме электронного документа);

3. доступная форма предоставления ответов на задания (письменно на бумаге, набор ответов на компьютере, устно и др.).

При необходимости для обучающихся с инвалидностью и обучающихся с ограниченными возможностями здоровья процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов, а также может быть предоставлено дополнительное время для подготовки ответа на зачете или экзамене.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ)

№	Результаты (освоенный практический опыт)	Формы и методы контроля и оценки
1.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	<ul style="list-style-type: none"> - обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; - адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач
2.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	- использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач
3.	Планировать и реализовывать собственное профессиональное и личностное развитие.	<ul style="list-style-type: none"> - демонстрация ответственности за принятые решения - обоснованность самоанализа и коррекция результатов собственной работы;
4.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	<ul style="list-style-type: none"> - взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; - обоснованность анализа работы членов команды (подчиненных)
5.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	<ul style="list-style-type: none"> - грамотность устной и письменной речи, - ясность формулирования и изложения мыслей
6.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.	- соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик,
7.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	<ul style="list-style-type: none"> - эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик; - знание и использование ресурсосберегающих технологий в области телекоммуникаций
8.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.	- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик;

9.	Использовать информационные технологии в профессиональной деятельности.	- эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту;
10.	Пользоваться профессиональной документацией на государственном и иностранном языках.	- эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке.
11.	Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.	Демонстрировать умения и практические навыки в установке и настройке отдельных программных, программно-аппаратных средств защиты информации
12.	Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.	Демонстрировать знания и умения в обеспечении защиты информации в автоматизированных системах отдельными программными, программно-аппаратными средствами
13.	Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.	Выполнение перечня работ по тестированию функций отдельных программных и программно-аппаратных средств защиты информации
14.	Осуществлять обработку, хранение и передачу информации ограниченного доступа.	Проявлять знания, навыки и умения в обработке, хранении и передаче информации ограниченного доступа
15.	Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.	Демонстрация алгоритма проведения работ по уничтожению информации и носителей информации с использованием программных и программно-аппаратных средств. Проявлять знания и умения в защите автоматизированных (информационных) систем с использованием программных и программноаппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак

Критерии оценки

Оценка	Критерии
Отлично	глубокое и полное овладение содержанием заданий по видам работ, свободное ориентирование в них, уверенное владение технической терминологией, знание содержания правовых норм, грамотное логичное изложение ответа, грамотное использование междисциплинарных связей, свободное ориентирование в имеющемся на рынке, специализированном оборудовании, умение увязывать теоретические знания с практической деятельностью, умение осуществлять профессиональное толкование технических вопросов при принятии решений по практическим ситуациям, полная аргументация принятого решения по профессиональной задаче, отсутствуют затруднения в ответах на дополнительные или уточняющие вопросы.
Хорошо	полное овладение содержанием заданий по видам работ, ориентирование в них, владение технической терминологией, знание содержания правовых норм, грамотное изложение заданий по видам работ, но их содержание и форма имеют отдельные неточности, использование междисциплинарных связей, незначительные затруднения в умении увязывать теорию с практикой, несущественные ошибки при профессиональном толковании технических вопросов в принятии решений по конкретным ситуациям, аргументация принятого решения по профессиональной задаче, на большинство дополнительных или уточняющих вопросов дан правильный ответ.
Удовлетворительно	знание и понимание содержания основных заданий по видам работ, но неполное, непоследовательное их изложение, допуск неточностей в определении понятий, слабое владение технической терминологией, существенные затруднения в умении увязывать теорию с практикой, ошибки при профессиональном толковании технических вопросов в принятии решений по конкретным ситуациям, аргументация решения по профессиональной задаче отсутствует, затруднения в ответах на дополнительные или уточняющие вопросы.
Неудовлетворительно	не освоена значительная часть заданий по видам работ, неумение выделять главное и второстепенное, искажение смысла понятийного аппарата и технической терминологии, беспорядочное изложение заданий по видам работ с существенными ошибками, невладение междисциплинарными связями, неумение увязывать теорию с практикой, невладение навыками профессионального толкования технических вопросов

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное
учреждение инклюзивного высшего образования

**«Российский государственный
университет социальных технологий»**

КАЛМЫЦКИЙ ФИЛИАЛ ФГБОУ ИВО «РГУ СоцТех»

ДНЕВНИК-ОТЧЕТ

по производственной практике (по профилю специальности)

Студента(ки) _____ курса _____ группы

ПМ. 02 Защита информации в автоматизированных системах программными и
программно-аппаратными средствами

Оценка результатов практики руководителя от КФ РГУ СоцТех

(дифференцированная оценка)

II. КАЛЕНДАРНО–ТЕМАТИЧЕСКИЙ ПЛАН ПРОХОЖДЕНИЯ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

Дата выполнения работы	Этапы выполняемых работ и заданий по программе практики	Срок выполнения		Подпись руководителя о выполнении задания
		начало	окончание	
1	2	4	5	6

Содержание и объем выполненных работ подтверждаю.

Руководитель практики от организации _____ (_____)
подпись Ф.И.О.
 М.П.

III. ПЕРЕЧЕНЬ РАБОТ ВЫПОЛНЕННЫХ РАБОТ ВО ВРЕМЯ ПРОХОЖДЕНИЯ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ НА ПРЕДПРИЯТИИ

Дата	Структурное подразделение, рабочее место, должность	Краткое содержание работы, выполненной в течение дня	Подпись руководителя практики от организации
1	2	3	4

Подпись практиканта _____

Содержание и объем выполненных работ подтверждаю.

Руководитель практики от организации _____ (_____)
подпись Ф.И.О.
 М.П.

