Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Григорьев Сергей Сергеевич
Должность: Заместитель директора по информатизации и цифровизации
Дата подписания: 10.03.2025 07:14:23
Уникальный программный ключ:
33b52346aed603d1e29801db513455d4dfc35e27

ГПОУ «ЯКУТСКИЙ КОЛЛЕДЖ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ»

УТВЕРЖДЕНО
ученым педагогическим советом
(протокол №06-23 от «26» июня 2023 г.)
Председатель педагогического совета
Директор _____ Л.Н. Цой

Программа производственбной практики
ПП.02.01 ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ

ППССЗ по специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Объем практики – 144 часа

Якутск, 2023

Разработчики рабочей программы:	НПОУ «ЯКИТ»	Преподаватель	И.И. Михайлов
	(место работы)	(должность)	(инициалы, фамилия)

Обсуждено на заседании отделения «19» июня 2022 г. протокол №9/1

Председатель отделения Зав. отделения _____ И.В. Пронин

Рассмотрено на заседании научно-методической комиссии «20» июня 2023 г. протокол №6

Председатель НМК Заместитель директора по учебно-методической работе _____ «26» июня 2023 г.

Заместитель директора по учебно-производственной работе _____ И.П. Каштанов «26» июня 2023 г.

№ п/п	Прилагаемый к Рабочей программе документ, содержащий текст обновления	Решение отделения		Подпись заведующего отделения	Фамилия И.О. заведующего отделения
		дата	Протокол №		
1.	Приложение № 1				
2.	Приложение № 2				
3.	Приложение № 3				
4.	Приложение № 4				
5.	Приложение № 5				

1. Цели и задачи практики:

Целями прохождения практики ПП.02.01 являются: углубление студентом первоначального профессионального опыта, развитие общих и профессиональных компетенций, проверку его готовности к самостоятельной трудовой деятельности в организациях различных организационно правовых форм.

2. Место практики в структуре ППССЗ: ПП.02.01 входит в профессиональный модуль ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами. ПП.02.01 реализуется в 4-м семестре.

3. Требования к результатам прохождения практики:

Процесс прохождения практики направлен на формирование ряда профессиональных и компетенций.

Профессиональные компетенции:

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.

ДПК 5.1. Подготовка (организация поверки) контрольно-измерительного оборудования для проведения контроля функционирования инфокоммуникационной системы.

ДПК 5.2. Документирование результатов контроля, включая подготовку протоколов или ввод данных в автоматизированные информационные системы**.**

Планируемые результаты обучения по практике:

Знать:

- особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;
- 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.

Уметь:

- 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.

Владеть (иметь опыт):

- 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.

4. Объем практики

Объем практики (в з. ед)	144
Продолжительность (в неделях)	4
Семестр	4
Форма промежуточной аттестации	Дифф. зачет

5. Содержание практики

1. Применение программных и программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах
2. Диагностика, устранение отказов и обеспечение работоспособности программно-аппаратных средств обеспечения информационной безопасности
3. Оценка эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности
4. Составление документации по учету, обработке, хранению и передаче конфиденциальной информации
5. Использование программного обеспечения для обработки, хранения и передачи конфиденциальной информации

6. Составление маршрута и состава проведения различных видов контрольных проверок при аттестации объектов, помещений, программ, алгоритмов.

7. Устранение замечаний по результатам проверки

8. Анализ и составление нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами, с учетом нормативных правовых актов.

9. Применение математических методов для оценки качества и выбора наилучшего программного средства

10. Использование типовых криптографических средств и методов защиты информации, в том числе и электронной подписи.

6. Оценочные средства для текущего контроля и промежуточной аттестации по итогам прохождения практики

Текущий контроль прохождения практики осуществляется преподавателем. Форма отчетности по учебной практике устанавливается преподавателем. Методами контроля и оценки является интерпретация результатов наблюдений за деятельностью обучающегося в процессе выполнения заданий практики.

7. Учебно-методическое и информационное обеспечение практики:

Основные источники:

1. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2022. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/491249

2. Запечников, С. В. Криптографические методы защиты информации : учебник для вузов / С. В. Запечников, О. В. Казарин, А. А. Тарасов. — Москва : Издательство Юрайт, 2022. — 309 с. — (Высшее образование). — ISBN 978-5-534-02574-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/489487

3. Системы управления технологическими процессами и информационные технологии : учебное пособие для среднего профессионального образования / В. В. Троценко, В. К. Федоров, А. И. Забудский, В. В. Комендантов. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2022. — 136 с. — (Профессиональное образование). — ISBN 978-5-534-09939-3. — Текст : электронный // Образовательная

платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/493021

4. Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2022. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/493262

5. Гутгарц, Р. Д. Проектирование автоматизированных систем обработки информации и управления : учебное пособие для вузов / Р. Д. Гутгарц. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 351 с. — (Высшее образование). — ISBN 978-5-534-15761-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/509638

Дополнительные источники:

1. Лобанова, Н. М. Эффективность информационных технологий : учебник и практикум для вузов / Н. М. Лобанова, Н. Ф. Алтухова. — Москва : Издательство Юрайт, 2022. — 237 с. — (Высшее образование). — ISBN 978-5-534-00222-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/489364

2. Проектирование информационных систем : учебник и практикум для вузов / под общей редакцией Д. В. Чистова. — Москва : Издательство Юрайт, 2022. — 258 с. — (Высшее образование). — ISBN 978-5-534-00492-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/489307

8. Материально-техническое обеспечение практики

Реализация программы учебной практики требует наличия лаборатории системного и прикладного программирования.

Оборудование лаборатории и рабочих мест лаборатории:

- компьютерные столы;
- рабочее место преподавателя;
- шкафы для учебных пособий;

Технические средства обучения:

- медиапроектор;
- интерактивная доска;
- компьютеры, объединенные локальной сетью с лицензионным программным обеспечением:

- Microsoft Office;
- Microsoft Visual Studio.

Специальные условия для получения среднего профессионального образования обучающимися с ОВЗ.

Для лиц с нарушениями слуха:

- индукционная система,
- сенсорный информационный киоск.

Для лиц с нарушениями зрения:

- сенсорные моноблоки,
- электронный видеоувеличитель,
- мультимедийная система,
- документ-камера,
- сенсорный информационный киоск.

Для лиц с нарушениями опорно-двигательного аппарата:

- сенсорные моноблоки.