



государственное автономное учреждение
Калининградской области
профессиональная образовательная организация
«КОЛЛЕДЖ ПРЕДПРИНИМАТЕЛЬСТВА»

РАБОЧАЯ ПРОГРАММА ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

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

**Специальность 10.02.05 Обеспечение информационной безопасности
автоматизированных систем**

СОГЛАСОВАНО

Генеральный директор
ООО АУТСОРС

Рекушин С.Г.

«30» июня 2022г.



УТВЕРЖДАЮ:

государственное автономное учреждение Калининградской области
профессиональная образовательная организация "Колледж
предпринимательства"

Директор

Л.Н. Копцева



РАЗРАБОТЧИКИ:

государственное автономное учреждение Калининградской области
профессиональная образовательная организация "Колледж
предпринимательства"

Заведующий отделением

М.В. Зверев

1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

1.1. Область применения программы

Программа производственной практики является компонентом образовательной программы по специальности **10.02.05 Обеспечение информационной безопасности автоматизированных систем** базовой подготовки в составе профессионального модуля **02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами**, реализуемая в рамках практической подготовки студентов по программе ППСЗ.

1.2. Цели и задачи

С целью овладения указанным видом профессиональной деятельности и соответствующими профессиональными компетенциями обучающийся в ходе освоения производственной практики должен выполнить следующие задачи.

Задачи практики:

формирование практического опыта:

- 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.

профессиональных компетенций:

- ✓ Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.
- ✓ Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.
- ✓ Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.
- ✓ Осуществлять обработку, хранение и передачу информации ограниченного доступа.

✓ Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.

✓ 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.

Продолжительность производственной практики 4 недели.

Объем производственной практики 144 часов.

2. ПРОГРАММА ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

№ п/п	ОК. ПК	Практический опыт	Вид работ	Количество часов
1			Анализ принципов построения систем информационной защиты производственных подразделений.	6
2			Анализ принципов построения систем информационной защиты производственных подразделений.	6
3			Анализ принципов построения систем информационной защиты производственных подразделений.	6
4			Анализ принципов построения систем информационной защиты производственных подразделений.	6
5			Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы.	6
6			Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы.	6
7			Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы.	6
8			Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы.	6
9			Участие в диагностировании, устранении отказов и обеспечении работоспособности программно-аппаратных средств обеспечения информационной безопасности;	6

10			Участие в диагностировании, устранении отказов и обеспечении работоспособности программно-аппаратных средств обеспечения информационной безопасности;	6
11			Участие в диагностировании, устранении отказов и обеспечении работоспособности программно-аппаратных средств обеспечения информационной безопасности;	6
12			Участие в диагностировании, устранении отказов и обеспечении работоспособности программно-аппаратных средств обеспечения информационной безопасности;	6
13			Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении	6
14			Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении	6
15			Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении	6
16			Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной	6

			безопасности в структурном подразделении	
17			Участие в обеспечении учета, обработки, хранения и передачи конфиденциальной информации	6
18			Участие в обеспечении учета, обработки, хранения и передачи конфиденциальной информации	6
19			Участие в обеспечении учета, обработки, хранения и передачи конфиденциальной информации	6
20			Участие в обеспечении учета, обработки, хранения и передачи конфиденциальной информации	6
21			Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами при выполнении задач практики.	6
22			Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами при выполнении задач практики.	6
23			Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами при выполнении задач практики.	6
24			Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной	6

			безопасности программно-аппаратными средствами при выполнении задач практики.	
Дифференцированный зачет				

3. МЕСТО И УСЛОВИЯ ПРОВЕДЕНИЯ ПРАКТИКИ

Производственная практика проводится в профильных организациях на основе договоров, заключаемых между образовательным учреждением и организациями по месту прохождения производственной практики.

Освоение производственной практики ПП.02 в рамках профессионального модуля является обязательным условием допуска к преддипломной практике по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Реализация рабочей программы производственной практики требует наличия производственно-технической инфраструктуры предприятия.

Оснащенность рабочих мест для проведения практики должна предусматривать возможность освоения в полном объеме вида профессиональной деятельности. При прохождении практики все обучающиеся должны быть обеспечены рабочими местами, на которых имеется:

- персональный компьютер (клиент и сервер) с подключением к системе телекоммуникаций (электронная почта, Интернет);
- аппаратное и программное обеспечение для работы обучающихся в рамках практики;
- информационная система на основе локальной вычислительной сети.

Все объекты должны соответствовать действующим санитарным и противопожарным нормам, а также требованиям техники безопасности при проведении производственных работ.

4. ПРОВЕРКА РЕЗУЛЬТАТОВ ПРАКТИКИ

Промежуточная аттестация практики проводится в форме дифференцированного зачета в последний день практики на основании аттестационного листа, дневника и отчета по практике, оформленных в соответствии с требованиями фонда оценочных средств по практике.