Министерство образования Иркутской области
Государственное бюджетное профессиональное
образовательное учреждение Иркутской области
«Иркутский авиационный техникум»

Методические указания по выполнению самостоятельной работы по дисциплине

ОП.16 Безопасность информационных систем

специальности

09.02.07 Информационные системы и программирование

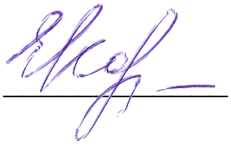
Иркутск, 2025

РАССМОТРЕНЫ

Председатель ЦК

_____ / /

УТВЕРЖДАЮ
Зам. директора


_____ Е.А. Коробкова

№	Разработчик ФИО
1	Бодоев Даниил Александрович

Пояснительная записка

Дисциплина ОП.16 Безопасность информационных систем входит в Общепрофессиональный цикл. Самостоятельная работа является одним из видов учебно работы обучающегося без взаимодействия с преподавателем.

Основные цели самостоятельной работы:

- систематизация и закрепление теоретических знаний и практических умений обучающихся;
- углубление и расширение теоретических знаний, формирование умений использовать справочную документацию и дополнительную литературу;
- развитие познавательных способностей и активности обучающихся, творческой инициативы, самостоятельности, ответственности и организованности;
- формирование самостоятельного мышления;
- развитие исследовательских умений.

Рекомендации для обучающихся по выработке навыков самостоятельной работы:

- Слушать, записывать и запоминать лекцию.
- Внимательно читать план выполнения работы.
- Выбрать свой уровень подготовки задания.
- Обращать внимание на рекомендуемую литературу. Из перечня литературы выбирать ту, которая наиболее полно раскрывает вопрос задания.
- Учиться кратко излагать свои мысли.
- Использовать общие правила написания конспекта.
- Обращать внимание на достижение основной цели работы.

Тематический план

Раздел Тема	Тема занятия	Название работы	Количество часов
Раздел 3. Методы и средства защиты Тема 2. Защита на уровне ОС, сетевые экраны, антивирусное ПО	Анализ логов антивирусного ПО	Анализ логов антивирусного ПО	2

Самостоятельная работа №1

Название работы: Анализ логов антивирусного ПО.
Цель работы: Изучить методы анализа логов антивирусного программного обеспечения для выявления угроз безопасности.
Уровень СРС: реконструктивная.
Форма контроля: Текстовый документ.
Количество часов на выполнение: 2 часа.
Задание:

1. Изучить структуру логов популярного антивирусного ПО (Kaspersky, или ESET, или Dr.Web)

2. Описать основные типы записей в логах и их значение

3. Привести примеры анализа логов для выявления:

    - Вирусных атак

    - Попыток несанкционированного доступа

    - Подозрительной активности

Критерии оценки:
оценка «3» - Представлено описание структуры логов без примеров анализа
оценка «4» - Описана структура логов и приведены примеры анализа для 1-2 типов угроз
оценка «5» - Полное описание структуры логов с примерами анализа для всех основных типов угроз