МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Смоленский казачий институт промышленных технологий и бизнеса (филиал) федерального государственного бюджетного образовательного учреждения «Московский государственный университет технологий и управления имени К.Г. Разумовского (Первый казачий университет)»

Смоленский казачий институт промышленных технологий и бизнеса (филиал)

УТВЕРЖДАЮ
Директор СКИПТБ (филиал) ФГБОУ ВО
«МГУТУ им. К.Г. Разумовского (ПКУ)
_____ Н.С. Коржикова
«21» апреля 2026 г.

Рабочая программа дисциплины (модуля)

Б1.О.04.10 ОБЩЕПРОФЕССИОНАЛЬНЫЙ МОДУЛЬ Информационная безопасность

Кафедра:	Системной автоматизации и информационных технологий
Направление подготовки:	15.03.04 Автоматизация технологических процессов и производств
Направленность (профиль):	Проектирование автоматизированных систем
Квалификация выпускника:	Бакалавр
Форма обучения:	заочная
Год набора:	2026
Общая трудоемкость:	216 часов/6 з.е.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 00F5 665F CCDB 5046 05DD 6E08 EBCB D00A DC
Действителен: с 21 октября 2025 г. по 14 января 2027 г.
Владелец: Коржикова Надежда Сергеевна
Должность: Директор

Вязьма, 2026 г.

Программу составил(и):
Старший преподаватель Долотовский Алексей Игоревич

Рабочая программа дисциплины (модуля)
"Информационная безопасность"
разработана на основании учебного плана, утвержденного ученым советом 26 марта 2026 г. протокол № 9 в соответствии с ФГОС ВО Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 15.03.04 Автоматизация технологических процессов и производств (приказ Минобрнауки России от 09.08.2021 г. № 730),

Руководитель ОПОП
канд. пед. наук, доцент Кузьмин К.А._____

Рабочая программа обсуждена на заседании обеспечивающей кафедры
Системной автоматизации и информационных технологий
Протокол от 10 апреля 2026 г. № 9
Зав. кафедрой Кузьмин Константин Анатольевич_____

СОДЕРЖАНИЕ

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОСНОВНОЙ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ И ОБЪЕМ С РАСПРЕДЕЛЕНИЕМ ПО СЕМЕСТРАМ

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫЕ С РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОСНОВНОЙ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОРГАНИЗАЦИИ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

6. ОЦЕНОЧНЫЕ И МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

9. ОРГАНИЗАЦИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

1.1. Цели:

Дисциплина информационная безопасность направлена на обеспечение надежной защиты информации и информационных систем от различных угроз и атак.

1.2. Задачи:

- изучение основных положений государственной политики в области обеспечения информационной безопасности Российской Федерации, основных понятий в области защиты информации и методологических принципов создания систем защиты информации;
- изучение видов защищаемой информации, угроз информационной безопасности, сущности и разновидностей информационного оружия, методов и средств ведения информационных
- изучение методов и средств обеспечения информационной безопасности компьютерных систем, механизмов защиты информации, формальных моделей безопасности, критериев оценки защищенности и обеспечения безопасности автоматизированных систем;
- приобретение умений в подборе и анализе показателей качества и критериев оценки систем безопасности, отдельных методов и средств защиты информации, использовании современной научно-технической литературой для решения задач по вопросам защиты информации;
- приобретение навыков анализа информационной инфраструктуры государства с точки зрения информационной безопасности, подбора нормативных и методических материалов по вопросам защиты информации.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ И ОБЪЕМ С РАСПРЕДЕЛЕНИЕМ ПО КУРСАМ

Цикл (раздел) ОП: "Информационная безопасность"

Дисциплина относится к обязательной части ОПОП и обязательна для освоения.

Связь с предшествующими дисциплинами (модулями), практиками

№ п/п	Наименование	Курс	Шифр компетенции
1	Электротехника и электроника	3	ОПК-4.1, ОПК-4.2, ОПК-4.3
2	Основы информационных технологий	1	УК-1.1, УК-1.2, УК-1.3, ОПК-4.1, ОПК-4.2, ОПК-4.3
3	Пакеты прикладных программ для профессиональной деятельности	1	ОПК-2.1, ОПК-2.2, ОПК-2.3, ОПК-4.1, ОПК-4.2, ОПК-4.3
4	Основы алгоритмизации и программирования	1	ОПК-14.1, ОПК-14.2, ОПК-14.3
5	Разработка программных приложений	1	ОПК-14.1, ОПК-14.2, ОПК-14.3

Распределение часов дисциплины

Курс	4		Итого	
Вид занятий	УП	РП		
Лекции	4	4	4	4
Лабораторные	6	6	6	6
Практические	4	4	4	4
В том числе в форме практ.подготовки	2	2	2	2
Итого ауд.	14	14	14	14
Контактная работа	14	14	14	14
Сам. работа	189	189	189	189
Часы на контроль	13	13	13	13
Итого	216	216	216	216

Вид промежуточной аттестации:

Экзамен 4 курс

Зачёт 4 курс

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫЕ С РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОСНОВНОЙ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс изучения дисциплины (модуля) направлен на формирование следующих компетенций и индикаторов их

ОПК-14:Способен разрабатывать алгоритмы и компьютерные программы, пригодные для практического применения

ОПК-14.1: Знает процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов (информационные технологии); логику построения и принципы функционирования современных языков программирования и языков работы с базами данных, сред разработки информационных систем и технологий, принципы разработки алгоритмов и компьютерных программ; современные языки программирования и языки работы с базами данных, среды разработки информационных систем и технологий

ОПК-14.2: Умеет выбирать языки программирования и языки работы с базами данных, среды разработки информационных систем и технологий, исходя из имеющихся задач; применять современные языки программирования для разработки оригинальных алгоритмов и компьютерных программ, пригодных для практического применения, вести базы данных и информационные хранилища, применять современные программные среды разработки информационных систем и технологий; читать коды программных продуктов, написанных на освоенных языках программирования, и вносить требуемые изменения; анализировать профессиональные задачи, разрабатывать подходящие информационные решения; самостоятельно осваивать новые для себя современные языки программирования и языки работы с базами данных, среды, разработки информационных систем и технологий

ОПК-14.3: Владеет навыками разработки оригинальных алгоритмов и компьютерных программ, пригодных для практического применения; навыками отладки и тестирования прототипов программно-технических комплексов задач

ОПК-4:Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности

ОПК-4.1: Знает процессы, методы поиска, сбора, хранения, обработки, представления, распространения информации и способы осуществления таких процессов и методов (информационные технологии); современные инструментальные среды, программно-технические платформы и программные средства, в том числе отечественного производства, используемые для решения задач профессиональной деятельности, и принципы их работы

ОПК-4.2: Умеет выбирать и использовать современные информационно-коммуникационные и интеллектуальные технологии, инструментальные среды, программно-технические платформы и программные средства, в том числе отечественного производства, для решения задач профессиональной деятельности; анализировать профессиональные задачи, выбирать и использовать подходящие информационные технологии

ОПК-4.3: Владеет навыками работы с данными с помощью информационных технологий; навыками применения современных информационно-коммуникационных и интеллектуальных технологий, инструментальных сред, программно-технических платформ и программных средств, в том числе отечественного производства, для решения задач профессиональной деятельности

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименования разделов, тем, их краткое содержание и результаты освоения /вид занятия/	Курс	Часы	Инте ракт.	Прак. подг.	Индикаторы достижения компетенции	Виды контроля
	Раздел 1.Введение в информационную безопасность						
1.1	**Тема 1. Введение в информационную безопасность Знать: Основные принципы информационной безопасности: конфиденциальность, целостность и доступность /Лек/**	4	1	0	0	ОПК-4.1	Устный опрос
1.2	**Тема 2. Основы криптографии Знать: Основные алгоритмы шифрования /Лек/**	4	1	0	0	ОПК-14.1	Устный опрос
1.3	**Установка и настройка основных инструментов безопасности Уметь: настраивать брандмауэр для контроля сетевого трафика и защиты от несанкционированного доступа к системе Владеть: инструментами мониторинга угроз для обнаружения аномальной активности в сети или на устройстве /Пр/**	4	2	0	0	ОПК-4.2,ОПК-4.3	Отчет по практическим работам
1.4	**Анализ сетевого трафика и обнаружение Уметь: распознавать обычный сетевой трафик и выявлять аномалии, которые могут указывать на атаки или несанкционированную активность. Владеть: настройкой правил фильтрации трафика для выявления и блокирования**	4	2	0	0	ОПК-14.2,ОПК-14.3	Отчет по лабораторной работе

	потенциально вредоносной активности. /Лаб/						
1.5	**Уязвимости и атаки** **Знать: различные типы уязвимостей, таких как уязвимости веб-приложений, сетевых протоколов, операционных систем и других компонентов информационных систем** **Уметь: проводить оценку уязвимостей информационных систем с использованием специализированных инструментов и методов для выявления потенциальных уязвимостей** **Владеть: методами проактивной защиты информационных систем от уязвимостей и атак, включая регулярное обновление программного обеспечения, мониторинг сетевой активности и применение мер безопасности /Ср/**	4	64	0	0	ОПК-4.1,ОПК-4.2,ОПК-4.3,ОПК-14.1,ОПК-14.2,ОПК-14.3	Вопросы для самоподготовки
1.6	**Зачет** **ОПК-4.1: Знает процессы, методы поиска, сбора, хранения, обработки, представления, распространения информации и способы осуществления таких процессов и методов (информационные технологии); современные инструментальные среды, программно-технические платформы и программные средства, в том числе отечественного производства, используемые для решения задач профессиональной деятельности, и принципы их работы** **ОПК-4.2: Умеет выбирать и использовать современные информационно-коммуникационные и интеллектуальные технологии, инструментальные среды, программно-технические платформы и программные средства, в том числе отечественного производства, для решения задач профессиональной деятельности; анализировать профессиональные задачи, выбирать и использовать подходящие информационные технологии** **ОПК-4.3: Владеет навыками работы с данными с помощью информационных технологий; навыками применения современных информационно-коммуникационных и интеллектуальных технологий, инструментальных сред, программно-технических платформ и программных средств, в том числе отечественного производства, для решения задач профессиональной деятельности** **ОПК-14.1: Знает процессы, методы**	4	4	0	0	ОПК-4.1,ОПК-4.2,ОПК-4.3,ОПК-14.1,ОПК-14.2,ОПК-14.3	Вопросы к зачету, итоговое тестирование

	поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов (информационные технологии); логику построения и принципы функционирования современных языков программирования и языков работы с базами данных, сред разработки информационных систем и технологий, принципы разработки алгоритмов и компьютерных программ; современные языки программирования и языки работы с базами данных, среды разработки информационных систем и технологий **ОПК-14.2: Умеет выбирать языки программирования и языки работы с базами данных, среды разработки информационных систем и технологий, исходя из имеющихся задач; применять современные языки программирования для разработки оригинальных алгоритмов и компьютерных программ, пригодных для практического применения, вести базы данных и информационные хранилища, применять современные программные среды разработки информационных систем и технологий; читать коды программных продуктов, написанных на освоенных языках программирования, и вносить требуемые изменения; анализировать профессиональные задачи, разрабатывать подходящие информационные решения; самостоятельно осваивать новые для себя современные языки программирования и языки работы с базами данных, среды, разработки информационных систем и технологий** **ОПК-14.3: Владеет навыками разработки оригинальных алгоритмов и компьютерных программ, пригодных для практического применения; навыками отладки и тестирования прототипов программно-технических комплексов задач /Зачёт/**						
	Раздел 2.Защита при разработке приложений						
2.1	**Тема 3. Защита баз данных** **Знать: методы управления доступом к базе данных через аутентификацию и авторизацию пользователей /Лек/**	4	1	0	0	ОПК-14.1	Устный опрос
2.2	**Тема 4. Защита веб-приложений** **Знать: методы идентификации потенциальных уязвимостей в веб-**	4	1	0	0	ОПК-14.1	Устный опрос

	приложениях, такие как инъекции SQL, межсайтовый скриптинг (XSS), межсайтовая подделка запросов (CSRF) и другие /Лек/						
2.3	**Защита операционных систем Уметь: настраивать политики безопасности операционной системы для управления доступом пользователей, паролей, шифрования данных и других аспектов безопасности Владеть: настройкой механизмов контроля доступа, таких как ACL (управление списками контроля доступа) или права доступа к файлам и папкам. /Пр/**	4	1	0	1	ОПК-14.2,ОПК-14.3	Отчет по практическим работам
2.4	**Перехват и анализ безопасности мобильных приложений Уметь: проводить реверс-инжиниринг мобильных приложений для анализа их структуры, работы с сервером и обработки данных Владеть: методами разработки мобильных приложений с учетом принципов безопасности, включая защиту данных, обработку аутентификации и обеспечение целостности приложения. /Пр/**	4	1	0	1	ОПК-14.2,ОПК-14.3	Отчет по практическим работам
2.5	**Разработка стратегии безопасности Уметь: проводить анализ угроз и уязвимостей информационной системы для определения потенциальных рисков безопасности. Владеть: методами управления безопасностью информации, включая защиту конфиденциальности, целостности и доступности данных. /Лаб/**	4	2	0	0	ОПК-14.2,ОПК-14.3	Отчет по лабораторной работе
2.6	**Защита информации и криптография Уметь: идентифицировать потенциальные уязвимости в системах защиты информации и критически оценивать их Владеть: методологией разработки криптографических систем с учетом современных стандартов безопасности для защиты информации от несанкционированного доступа /Лаб/**	4	2	0	0	ОПК-4.2,ОПК-4.3,ОПК-14.2,ОПК-14.3	Отчет по лабораторной работе
2.7	**Защита компьютерных сетей Знать: основные сетевые протоколы, таких как TCP/IP, DNS, DHCP, HTTP, HTTPS, FTP и другие, их функциональности и уязвимостей Уметь: правильно настраивать сетевое оборудование, такое как маршрутизаторы, коммутаторы, брандмауэры, для обеспечения безопасности и эффективности сети Владеть: разработкой и реализацией политики безопасности сети, включая установку правил доступа,**	4	62	0	0	ОПК-4.1,ОПК-4.2,ОПК-4.3,ОПК-14.1,ОПК-14.2,ОПК-14.3	Вопросы для самоподготовки

	шифрование трафика, аутентификацию пользователей и другие меры безопасности /Ср/						
2.8	**Защита операционных систем** **Знать: основных типов уязвимостей операционных систем, таких как уязвимости ядра, отказ в обслуживании, переполнение буфера, а также способы их эксплуатации** **Уметь: устанавливать и настраивать антивирусное программное обеспечение, брандмауэры, программы для обнаружения вторжений и другие инструменты защиты операционных систем** **Владеть: методами обеспечения безопасности при работе с внешними устройствами, такими как USB-накопители, внешние жесткие диски и прочее, включая сканирование на вирусы и контроль доступа /Ср/**	4	63	0	0	ОПК-4.1,ОПК-4.2,ОПК-4.3,ОПК-14.1,ОПК-14.2,ОПК-14.3	Вопросы для самоподготовки
2.9	**Экзамен** **ОПК-4.1: Знает процессы, методы поиска, сбора, хранения, обработки, представления, распространения информации и способы осуществления таких процессов и методов (информационные технологии); современные инструментальные среды, программно-технические платформы и программные средства, в том числе отечественного производства, используемые для решения задач профессиональной деятельности, и принципы их работы** **ОПК-4.2: Умеет выбирать и использовать современные информационно-коммуникационные и интеллектуальные технологии, инструментальные среды, программно-технические платформы и программные средства, в том числе отечественного производства, для решения задач профессиональной деятельности; анализировать профессиональные задачи, выбирать и использовать подходящие информационные технологии** **ОПК-4.3: Владеет навыками работы с данными с помощью информационных технологий; навыками применения современных информационно-коммуникационных и интеллектуальных технологий, инструментальных сред, программно-технических платформ и программных средств, в том числе отечественного производства, для решения задач**	4	9	0	0	ОПК-4.1,ОПК-4.2,ОПК-4.3,ОПК-14.1,ОПК-14.2,ОПК-14.3	Вопросы к экзамену, итоговое тестирование

	профессиональной деятельности ОПК-14.1: Знает процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов (информационные технологии); логику построения и принципы функционирования современных языков программирования и языков работы с базами данных, сред разработки информационных систем и технологий, принципы разработки алгоритмов и компьютерных программ; современные языки программирования и языки работы с базами данных, среды разработки информационных систем и технологий ОПК-14.2: Умеет выбирать языки программирования и языки работы с базами данных, среды разработки информационных систем и технологий, исходя из имеющихся задач; применять современные языки программирования для разработки оригинальных алгоритмов и компьютерных программ, пригодных для практического применения, вести базы данных и информационные хранилища, применять современные программные среды разработки информационных систем и технологий; читать коды программных продуктов, написанных на освоенных языках программирования, и вносить требуемые изменения; анализировать профессиональные задачи, разрабатывать подходящие информационные решения; самостоятельно осваивать новые для себя современные языки программирования и языки работы с базами данных, среды, разработки информационных систем и технологий ОПК-14.3: Владеет навыками разработки оригинальных алгоритмов и компьютерных программ, пригодных для практического применения; навыками отладки и тестирования прототипов программно-технических комплексов задач /Экзамен/						

Перечень применяемых активных и интерактивных образовательных технологий:

Информационные технологии

Личностно ориентированная технология, способ организации самостоятельной деятельности учащихся, направленный на решение задачи учебного проекта

Проектная технология

Стандартизированный метод оценки знаний, умений, навыков учащихся, который помогает выявить и сформировать индивидуальный темп обучения, пробелы в текущей итоговой подготовке

Технология организации самостоятельной работы

Организации самостоятельной работы учащихся на более высоком уровне может способствовать применение технологии проектного и проблемного обучения. Методы самостоятельного приобретения знаний основаны на использовании проблемного обучения

Технология поиска информации (Информационная технология)

Информационная технология неотделима от субьектов образовательной деятельности, она является определяющим фактором технологии работы с информацией, применяемой в образовательной практике

Технология проектного обучения (метод проектов)

Это совокупность приѐмов, действий учащихся в их определѐнной последовательности для достижения поставленной задачи – решения определенной проблемы, значимой для учащихся и оформленной в виде некоего конечного продукта. Основная цель проектного обучения состоит в предоставлении учащимся возможности самостоятельного приобретения знаний в процессе решения практических задач или проблем, требующего интеграции знаний из различных предметных областей. Эта технология предполагает совокупность исследовательских, поисковых, проблемных методов, творческих по своей сути. В ходе самостоятельной работы учащихся над проектом формируются следующие интеллектуальные умения: - обстоятельно анализировать (определять и уяснять цели и задачи предстоящей работы);
выбирать и планировать формы и методы деятельности; организовать свою самостоятельную работу; учитывать результаты и корректировать дальнейшие действия; осуществлять контроль и самоконтроль;
проводить рефлексию итогов процесса самостоятельной работы и себя в нем

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОРГАНИЗАЦИИ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Самостоятельная (внеаудиторная) работа обучающегося (далее - СРС) – это планируемая учебная, практическая, учебно-исследовательская, научно-исследовательская работа студентов, выполняемая во внеаудиторное время (свободное от аудиторных учебных занятий) по заданию и при методическом руководстве научно-педагогического работника (далее – преподаватель) и (или) лиц, привлекаемых к реализации основных профессиональных образовательных программ на иных условиях, но без их непосредственного участия.
СРС по заданию и при методическом руководстве преподавателя и (или) лиц, привлекаемых к реализации основных профессиональных образовательных программ на иных условиях, реализуется во время групповых консультаций и (или) индивидуальной работы обучающихся с преподавателями Университета и (или) лиц, привлекаемых к реализации образовательных программ на иных условиях (в том числе индивидуальных консультаций), а также во время текущего контроля выполнения заданий, отнесенных к самостоятельной работе обучающихся.
Целью СРС является овладение формирование компетенций через овладение знаниями, умениями и навыками профессиональной деятельности по направлению подготовки (специальности). Самостоятельная работа является обязательной для каждого обучающегося.
Формы самостоятельной работы обучающихся определяются преподавателями кафедр Университета при разработке рабочих программ дисциплин (модулей), рабочих программ практик, программ государственной итоговой (итоговой) аттестации, методических указаний по выполнению практических, лабораторных работ, написанию курсовых работ/проектов и ВКР в соответствии с их содержанием.
В Университете оборудованы специальные помещения для самостоятельной работы обучающихся. Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к информационно -телекоммуникационной сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду Университета.

6. ОЦЕНОЧНЫЕ И МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ

6.1. Перечень компетенций с указанием уровней их сформированности

ОПК-14:Способен разрабатывать алгоритмы и компьютерные программы, пригодные для практического применения

Недостаточный уровень:

Не знает процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов (информационные технологии); логику построения и принципы функционирования современных языков программирования и языков работы с базами данных, сред разработки информационных систем и технологий, принципы разработки алгоритмов и компьютерных программ; современные языки программирования и языки работы с базами данных, среды разработки информационных систем и технологий

Не умеет выбирать языки программирования и языки работы с базами данных, среды разработки информационных систем и технологий, исходя из имеющихся задач; применять современные языки программирования для разработки оригинальных алгоритмов и компьютерных программ, пригодных для практического применения, вести базы данных и информационные хранилища, применять современные программные среды разработки информационных систем и технологий; читать коды программных продуктов, написанных на освоенных языках программирования, и вносить требуемые изменения; анализировать профессиональные задачи, разрабатывать подходящие информационные решения; самостоятельно осваивать новые для себя современные языки программирования и языки работы с базами данных, среды, разработки информационных систем и технологий

Не владеет навыками разработки оригинальных алгоритмов и компьютерных программ, пригодных для практического применения; навыками отладки и тестирования прототипов программно-технических комплексов задач

Пороговый уровень:

Знает процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов (информационные технологии); логику построения и принципы

функционирования современных языков программирования и языков работы с базами данных, сред разработки информационных систем и технологий, принципы разработки алгоритмов и компьютерных программ; современные языки программирования и языки работы с базами данных, среды разработки информационных систем и технологий

Умеет выбирать языки программирования и языки работы с базами данных, среды разработки информационных систем и технологий, исходя из имеющихся задач; применять современные языки программирования для разработки оригинальных алгоритмов и компьютерных программ, пригодных для практического применения, вести базы данных и информационные хранилища, применять современные программные среды разработки информационных систем и технологий; читать коды программных продуктов, написанных на освоенных языках программирования, и вносить требуемые изменения; анализировать профессиональные задачи, разрабатывать подходящие информационные решения; самостоятельно осваивать новые для себя современные языки программирования и языки работы с базами данных, среды, разработки информационных систем и технологий

Владеет навыками разработки оригинальных алгоритмов и компьютерных программ, пригодных для практического применения; навыками отладки и тестирования прототипов программно-технических комплексов задач

Продвинутый уровень:

На высоком уровне знает процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов (информационные технологии); логику построения и принципы функционирования современных языков программирования и языков работы с базами данных, сред разработки информационных систем и технологий, принципы разработки алгоритмов и компьютерных программ; современные языки программирования и языки работы с базами данных, среды разработки информационных систем и технологий

На высоком уровне умеет выбирать языки программирования и языки работы с базами данных, среды разработки информационных систем и технологий, исходя из имеющихся задач; применять современные языки программирования для разработки оригинальных алгоритмов и компьютерных программ, пригодных для практического применения, вести базы данных и информационные хранилища, применять современные программные среды разработки информационных систем и технологий; читать коды программных продуктов, написанных на освоенных языках программирования, и вносить требуемые изменения; анализировать профессиональные задачи, разрабатывать подходящие информационные решения; самостоятельно осваивать новые для себя современные языки программирования и языки работы с базами данных, среды, разработки информационных систем и технологий

На высоком уровне владеет навыками разработки оригинальных алгоритмов и компьютерных программ, пригодных для практического применения; навыками отладки и тестирования прототипов программно-технических комплексов задач

Высокий уровень:

В полном объеме знает процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов (информационные технологии); логику построения и принципы функционирования современных языков программирования и языков работы с базами данных, сред разработки информационных систем и технологий, принципы разработки алгоритмов и компьютерных программ; современные языки программирования и языки работы с базами данных, среды разработки информационных систем и технологий

В полном объеме умеет выбирать языки программирования и языки работы с базами данных, среды разработки информационных систем и технологий, исходя из имеющихся задач; применять современные языки программирования для разработки оригинальных алгоритмов и компьютерных программ, пригодных для практического применения, вести базы данных и информационные хранилища, применять современные программные среды разработки информационных систем и технологий; читать коды программных продуктов, написанных на освоенных языках программирования, и вносить требуемые изменения; анализировать профессиональные задачи, разрабатывать подходящие информационные решения; самостоятельно осваивать новые для себя современные языки программирования и языки работы с базами данных, среды, разработки информационных систем и технологий

В полном объеме владеет навыками разработки оригинальных алгоритмов и компьютерных программ, пригодных для практического применения; навыками отладки и тестирования прототипов программно-технических комплексов задач

ОПК-4:Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности

Недостаточный уровень:

Не знает процессы, методы поиска, сбора, хранения, обработки, представления, распространения информации и способы осуществления таких процессов и методов (информационные технологии); современные инструментальные среды, программно-технические платформы и программные средства, в том числе отечественного производства, используемые для решения задач профессиональной деятельности, и принципы их работы

Не умеет выбирать и использовать современные информационно-коммуникационные и интеллектуальные технологии, инструментальные среды, программно-технические платформы и программные средства, в том числе отечественного производства, для решения задач профессиональной деятельности; анализировать профессиональные задачи, выбирать и использовать подходящие информационные технологии

Не владеет навыками работы с данными с помощью информационных технологий; навыками применения современных информационно-коммуникационных и интеллектуальных технологий, инструментальных сред, программно-технических платформ и программных средств, в том числе отечественного производства, для решения задач профессиональной деятельности

Пороговый уровень:

Знает процессы, методы поиска, сбора, хранения, обработки, представления, распространения информации и способы

осуществления таких процессов и методов (информационные технологии); современные инструментальные среды, программно-технические платформы и программные средства, в том числе отечественного производства, используемые для решения задач профессиональной деятельности, и принципы их работы

Умеет выбирать и использовать современные информационно-коммуникационные и интеллектуальные технологии, инструментальные среды, программно-технические платформы и программные средства, в том числе отечественного производства, для решения задач профессиональной деятельности; анализировать профессиональные задачи, выбирать и использовать подходящие информационные технологии

Владеет навыками работы с данными с помощью информационных технологий; навыками применения современных информационно-коммуникационных и интеллектуальных технологий, инструментальных сред, программно-технических платформ и программных средств, в том числе отечественного производства, для решения задач профессиональной деятельности

Продвинутый уровень:

На высоком уровне знает процессы, методы поиска, сбора, хранения, обработки, представления, распространения информации и способы осуществления таких процессов и методов (информационные технологии); современные инструментальные среды, программно-технические платформы и программные средства, в том числе отечественного производства, используемые для решения задач профессиональной деятельности, и принципы их работы

На высоком уровне умеет выбирать и использовать современные информационно-коммуникационные и интеллектуальные технологии, инструментальные среды, программно-технические платформы и программные средства, в том числе отечественного производства, для решения задач профессиональной деятельности; анализировать профессиональные задачи, выбирать и использовать подходящие информационные технологии

На высоком уровне владеет навыками работы с данными с помощью информационных технологий; навыками применения современных информационно-коммуникационных и интеллектуальных технологий, инструментальных сред, программно-технических платформ и программных средств, в том числе отечественного производства, для решения задач профессиональной деятельности

Высокий уровень:

В полном объеме знает процессы, методы поиска, сбора, хранения, обработки, представления, распространения информации и способы осуществления таких процессов и методов (информационные технологии); современные инструментальные среды, программно-технические платформы и программные средства, в том числе отечественного производства, используемые для решения задач профессиональной деятельности, и принципы их работы

В полном объеме умеет выбирать и использовать современные информационно-коммуникационные и интеллектуальные технологии, инструментальные среды, программно-технические платформы и программные средства, в том числе отечественного производства, для решения задач профессиональной деятельности; анализировать профессиональные задачи, выбирать и использовать подходящие информационные технологии

В полном объеме владеет навыками работы с данными с помощью информационных технологий; навыками применения современных информационно-коммуникационных и интеллектуальных технологий, инструментальных сред, программно-технических платформ и программных средств, в том числе отечественного производства, для решения задач профессиональной деятельности

6.2. Описание критериев оценивания успеваемости

НЕДОСТАТОЧНЫЙ УРОВЕНЬ	ПОРОГОВЫЙ УРОВЕНЬ	ПРОДВИНУТЫЙ УРОВЕНЬ	ВЫСОКИЙ УРОВЕНЬ
Обучающийся демонстрирует: - существенные пробелы в знаниях учебного материала; - принципиальные ошибки при ответе на основные вопросы билета, отсутствует знание и понимание основных понятий и категорий; - непонимание сущности дополнительных вопросов в рамках заданий билета; - отсутствие умения выполнять практические задания, предусмотренные программой дисциплины (модуля); - отсутствие готовности (способности) к дискуссии и низкая степень контактности.	Обучающийся демонстрирует: - знания теоретического материала; - неполные ответы на основные вопросы, ошибки в ответе, недостаточное понимание сущности излагаемых вопросов; - неуверенные и неточные ответы на дополнительные вопросы; - недостаточное владение литературой, рекомендованной программой дисциплины (модуля); - умение без грубых ошибок решать практические задания, которые следует выполнить.	Обучающийся демонстрирует: - знание и понимание основных вопросов контролируемого объема программного материала; - твердые знания теоретического материала; - способность устанавливать и объяснять связь практики и теории, выявлять противоречия, проблемы и тенденции развития; - правильные и конкретные, без грубых ошибок ответы на поставленные вопросы; - умение решать практические задания, которые следует выполнить; - владение основной литературой, рекомендованной	Обучающийся демонстрирует: - глубокие, всесторонние и аргументированные знания программного материала; - полное понимание сущности и взаимосвязи рассматриваемых процессов и явлений, точное знание основных понятий в рамках обсуждаемых заданий; - способность устанавливать и объяснять связь практики и теории; - логически последовательные, содержательные, конкретные и исчерпывающие ответы на все задания билета, а также дополнительные вопросы экзаменатора; - умение решать

		программой дисциплины (модуля); - наличие собственной обоснованной позиции по обсуждаемым вопросам; - незначительные оговорки и неточности в раскрытии отдельных положений вопросов билета, присутствует неуверенность в ответах на дополнительные вопросы.	практические задания; - свободное использование в ответах на вопросы материалов рекомендованной основной и дополнительной литературы.
Оценка «незачет», «неудовлетворительно»	**Оценка «зачтено/удовлетворительно», «удовлетворительно»**	**Оценка «зачтено/хорошо», «хорошо»**	**Оценка «зачтено/отлично», «отлично»**

6.3. Оценочные средства текущего контроля

Вопросы для устного опроса

Тема 1.

1. Что такое информационная безопасность и почему она важна для организаций?
2. Какие основные угрозы существуют для информационной безопасности?
3. Какие типы атак на информационную безопасность вы знаете?
4. Что такое уязвимость в контексте информационной безопасности?
5. Какие методы защиты информации вы знаете?
6. Что такое аутентификация и какие методы аутентификации существуют?
7. Какие принципы безопасности информации существуют и как они применяются?
8. Что такое шифрование и как оно помогает обеспечить безопасность данных?
9. Какие роли и обязанности могут быть у специалистов по информационной безопасности?
10. Какие стандарты и законы регулируют область информационной безопасности?
11. Что такое резервное копирование и как оно связано с обеспечением информационной безопасности?
12. Какие основные принципы следует соблюдать при разработке безопасных паролей?
13. Что такое социальная инженерия и как ей можно противостоять?
14. Какие основные шаги следует предпринять для обеспечения безопасности беспроводных сетей?
15. Как важно обучение сотрудников вопросам информационной безопасности для организации?

Тема 2.

1. Что такое криптография и каков ее основной цель?
2. Какие основные типы криптографии существуют?
3. Что такое шифрование и какие методы шифрования вы знаете?
4. Какие ключевые понятия используются в криптографии, такие как открытый и закрытый ключи?
5. Что такое симметричное и асимметричное шифрование?
6. Как работает алгоритм RSA и в чем его особенности?
7. Какие атаки на криптографические системы вы знаете?
8. Что такое цифровая подпись и как она используется в криптографии?
9. Что такое хэширование и какие цели преследует этот процесс?
10. Какие основные принципы криптографической безопасности существуют?
11. Какие стандарты криптографии используются на практике?
12. Какие методы аутентификации могут быть усилены с помощью криптографии?
13. Какой принцип лежит в основе криптографических протоколов для защиты информации в сети?
14. Каким образом криптография используется для защиты данных в цифровой экономике?
15. Как важно понимание основ криптографии для обеспечения информационной безопасности в современном мире?

Тема 3.

1. Какие угрозы могут быть направлены на базы данных?
2. Какие основные принципы обеспечения безопасности баз данных существуют?
3. Что такое SQL-инъекции и как ими можно защитить базы данных?
4. Какие методы шифрования данных могут быть применены для защиты информации в базах данных?
5. Как важно обеспечение правильного управления доступом к данным в базах данных?
6. Какие методы аутентификации могут быть использованы для защиты баз данных?
7. Что такое мониторинг и аудит баз данных, и почему это важно для их безопасности?
8. Какие резервные копии данных могут помочь в защите баз данных от потерь?
9. Как важно обновление программного обеспечения баз данных для обеспечения безопасности?
10. Что такое DDoS-атаки на базы данных и как ими можно защититься?
11. Как важно обучение персонала по вопросам безопасности баз данных?
12. Какие методы мониторинга активности пользователей могут помочь в обнаружении аномалий в базах данных?
13. Как важно использование безопасных паролей для доступа к базам данных?
14. Какие методы защиты от внутренних угроз могут быть применены к базам данных?
15. Каким образом обеспечивается целостность данных в базах данных и как это связано с их защитой?

Тема 4.
1. Какие уязвимости часто встречаются в веб-приложениях?
2. Какие методы аутентификации можно применить для защиты веб-приложений?
3. Как важно обеспечить защиту от атак по переполнению буфера в веб-приложениях?
4. Что такое XSS (межсайтовый скриптинг) и как защититься от него в веб-приложениях?
5. Какие методы защиты CSRF (межсайтовой подделки запросов) могут быть применены к веб-приложениям?
6. Какие методы шифрования данных могут быть использованы для защиты конфиденциальности в веб-приложениях?
7. Как важно обеспечение правильного управления доступом к функциям и данным в веб-приложениях?
8. Что такое инъекции SQL и как защититься от них в веб-приложениях?
9. Какие методы обеспечения безопасности сессий могут быть использованы в веб-приложениях?
10. Что такое клиентская сторона веб-приложений и какие уязвимости связанные с ней могут быть обнаружены?
11. Как важно проведение тестирования на проникновение для выявления уязвимостей в веб-приложениях?
12. Каким образом можно защитить веб-приложения от атаки по перебору паролей?
13. Какие методы мониторинга активности пользователей могут помочь в обнаружении аномалий в веб-приложениях?
14. Как важно обновление программного обеспечения и библиотек веб-приложений для обеспечения их безопасности?
15. Какой подход следует использовать для обеспечения безопасности API веб-приложений?

Тема 5.
1. Какие основные угрозы могут быть направлены на мобильные устройства?
2. Какие методы аутентификации могут быть использованы для защиты мобильных устройств?
3. Как важно обеспечить защиту от вредоносного ПО на мобильных устройствах?
4. Что такое уязвимости Bluetooth и как защитить мобильные устройства от атак через Bluetooth?
5. Какие методы шифрования данных могут быть применены для защиты конфиденциальности на мобильных устройствах?
6. Как важно обеспечить правильное управление доступом к данным и функциям на мобильных устройствах?
7. Что такое удаленное управление устройствами (MDM) и как оно может помочь в защите мобильных устройств?
8. Как важно обеспечить безопасность Wi-Fi соединений на мобильных устройствах?
9. Какие методы защиты от утери мобильных устройств могут быть использованы?
10. Что такое атаки через сеть мобильной связи и как защитить устройства от них?
11. Как важно обновление операционных систем и приложений на мобильных устройствах для обеспечения безопасности?
12. Какие методы защиты от фишинга и мошенничества могут быть применены на мобильных устройствах?
13. Как важно использование безопасных паролей и методов аутентификации на мобильных устройствах?
14. Какие методы мониторинга активности и обнаружения угроз могут быть использованы на мобильных устройствах?
15. Как важно обучение пользователей по вопросам безопасности мобильных устройств и данных?

Задания к практическим и лабораторным работам см. Приложение № 1.

Вопросы для самоподготовки
Тема 1
1. Какие основные типы уязвимостей существуют в информационной безопасности?
2. Что такое атака по переполнению буфера и каковы её последствия?
3. Какие уязвимости чаще всего используются в атаках на веб-приложения?
4. Что такое SQL инъекции и как они могут быть предотвращены?
5. Какие методы аутентификации подвержены наибольшему риску и как защититься от атак на аутентификацию?
6. Что такое межсайтовый скриптинг (XSS) и как его предотвратить?
7. Какие меры безопасности следует принять для защиты от атак межсайтовой подделки запросов (CSRF)?
8. Как уязвимости в сетевой инфраструктуре могут быть использованы для проведения атак?
9. Что такое атаки социальной инженерии и какие методы могут быть использованы для их предотвращения?
10. Какие методы шифрования могут быть использованы для защиты конфиденциальной информации?
11. Какие могут быть последствия атаки DDoS (распределенного отказа в обслуживании) и как их предотвратить?
12. Что такое атаки на беспроводные сети и как защититься от них?
13. Как уязвимости в операционных системах могут быть использованы для получения несанкционированного доступа?
14. Какие атаки могут быть направлены на мобильные устройства и как защититься от них?
15. Какие методы мониторинга и обнаружения атак могут быть применены для защиты информационных систем?

Тема 2
1. Какие угрозы могут быть направлены на компьютерные сети?
2. Какие методы аутентификации можно использовать для защиты доступа к сети?
3. Что такое фильтрация пакетов и как она помогает обеспечить безопасность сети?
4. Какие меры безопасности следует принять для защиты беспроводных сетей (Wi-Fi)?
5. Как важно обновлять программное обеспечение сетевых устройств для предотвращения уязвимостей?
6. Какие методы шифрования могут быть применены для защиты передаваемых данных в сети?
7. Что такое VPN (виртуальная частная сеть) и как она помогает обеспечить безопасность связи через открытые сети?
8. Какие меры следует принять для защиты от атаки на отказ в обслуживании (DoS) и распределенный отказ в

15. Как важно регулярно проводить аудиты безопасности сети и корректировать стратегии защиты с учетом новых угроз?

Тема 3
1. Какие основные угрозы могут быть направлены на операционные системы?
2. Как важно обновлять операционную систему и почему это необходимо для безопасности?
3. Что такое многофакторная аутентификация и как она может улучшить защиту операционной системы?
4. Какие меры безопасности следует принимать при использовании административных привилегий в операционной системе?
5. Что такое антивирусное программное обеспечение и как оно помогает защитить операционную систему от вредоносных программ?
6. Какие методы шифрования файлов и дисков можно использовать для защиты конфиденциальных данных на операционной системе?
7. Какие меры безопасности следует принимать при использовании общедоступных сетей для предотвращения атак на операционную систему?
8. Что такое защита от вторжений и какие инструменты могут быть использованы для обнаружения несанкционированной активности в операционной системе?
9. Как важно регулярно анализировать журналы событий операционной системы для обнаружения аномалий и потенциальных угроз?

6.4. Оценочные средства промежуточной аттестации

Вопросы к зачёту
ОПК-4: Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности;
Индикатор Знать
1) Установите правильную последовательность развития методов шифрования:
а) Появление симметричных шифров
б) Изобретение шифра Цезаря
в) Создание шифрмашины Энигма
г) Разработка асимметричных шифров
2) Прочитайте текст и установите соответствие между терминами и их определениями:
А) Криптология
Б) Криптоанализ
В) Криптография
Г) Шифр
1. Наука о методах обеспечения конфиденциальности информации
2. Наука о методах вскрытия шифров
3. Общая наука о шифрах и методах их анализа
4. Система преобразования информации для обеспечения секретности
5. Метод аутентификации пользователей
3) Установите правильную последовательность появления шифров:
а) Шифр Виженера
б) Решетка Кардано
в) Шифр Цезаря
г) Одноразовый шифр-блокнот
4) Прочитайте текст и установите соответствие между методами и их характеристиками:
А) Симметричное шифрование
Б) Асимметричное шифрование
В) Цифровая подпись
Г) Атака “человек посередине”
1. Требует двух ключей для работы
2. Использует один ключ для шифрования и дешифрования
3. Обеспечивает аутентификацию и целостность
4. Представляет угрозу безопасности передачи данных
5. Метод стеганографии
5) Установите правильную последовательность этапов развития криптографии:
а) Появление механических шифрмашин
б) Развитие математических основ защиты
в) Изобретение электромагнитного телеграфа
г) Формирование научных методов защиты
6) Прочитайте текст и установите соответствие между терминами и их применением:
А) Сертификат
Б) УЦ (Удостоверяющий центр)
В) Ключ
Г) Протокол
1. Инструмент для шифрования данных
2. Документ, подтверждающий личность
3. Система правил для безопасной передачи данных
4. Организация, выдающая цифровые сертификаты
5. Метод криптоанализа

7) Установите правильную последовательность развития технологий:
а) Появление цифровых подписей
б) Развитие симметричных шифров
в) Создание шифрмашины Энигма
г) Внедрение асимметричных шифров
8) Прочитайте текст и установите соответствие между методами и их особенностями:
А) Шифр Цезаря
Б) Шифр Виженера
В) Решетка Кардано
Г) Одноразовый блокнот
1. Использует таблицу для шифрования
2. Основан на сдвиге букв
3. Применяет периодическую замену
4. Обеспечивает абсолютную секретность
5. Метод перестановки
9) Установите правильную последовательность появления технологий:
а) Появление сертификатов
б) Развитие УЦ
в) Внедрение цифровых подписей
г) Создание шифрмашин
10. Прочитайте текст и установите соответствие между терминами и их функциями:
А) Стеганография
Б) Криптография
В) Цифровая подпись
Г) Сертификат
1. Метод криптоанализа
2. Метод шифрования данных
3. Инструмент аутентификации
4. Документ подтверждения личности
5. Метод скрытой передачи информации
Индикатор Уметь
11) Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор:
Какой метод шифрования обеспечивает абсолютную секретность?
а) Шифр Цезаря
б) Шифр Виженера
в) Одноразовый шифр-блокнот
г) Симметричное шифрование
12) Выберите правильные ответы и запишите аргументы, обосновывающие выбор ответа:
Какие методы шифрования используют два ключа?
а) Асимметричное шифрование
б) Симметричное шифрование
в) Шифр Энигма
г) Цифровая подпись
13) Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор:
Что такое криптоанализ?
а) Наука о методах шифрования
б) Наука о методах вскрытия шифров
в) Метод стеганографии
г) Технология создания ключей
14) Выберите правильные ответы и запишите аргументы, обосновывающие выбор ответа:
Какие характеристики присущи симметричному шифрованию?
а) Использование одного ключа
б) Высокая скорость работы
в) Сложность в управлении ключами
г) Использование двух ключей
15) Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор:
Какой метод защиты информации относится к стеганографии?
а) Шифр Цезаря
б) Решетка Кардано
в) Метод скрытой передачи данных
г) Шифр Виженера
16) Выберите правильные ответы и запишите аргументы, обосновывающие выбор ответа:
Какие преимущества имеет асимметричное шифрование?
а) Высокая скорость шифрования
б) Простота в управлении ключами
в) Возможность безопасной передачи ключей
г) Использование одного ключа
17) Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор:
Что такое атака “человек посередине”?

а) Метод шифрования данных
б) Метод криптоанализа
в) Метод перехвата и изменения данных
г) Метод аутентификации
18) Выберите правильные ответы и запишите аргументы, обосновывающие выбор ответа:
Какие функции выполняет цифровая подпись?
а) Подтверждение авторства
б) Обеспечение конфиденциальности
в) Проверка целостности данных
г) Шифрование сообщений
19) Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор:
Что такое криптографический протокол?
а) Метод шифрования данных
б) Система правил для безопасной передачи данных
в) Технология создания ключей
г) Метод криптоанализа
20) Выберите правильные ответы и запишите аргументы, обосновывающие выбор ответа:
Какие характеристики присущи шифрмашине Энигма?
а) Механическое устройство
б) Использование симметричного шифрования
в) Применение асимметричного шифрования
г) Автоматическая генерация ключей

Индикатор Владеть
21) Прочитайте текст и запишите развернутый ответ: В ходе исторического исследования были обнаружены зашифрованные послания, использовавшие шифр сцитала. Объясните принцип работы этого шифра и предположите, почему он считался надежным в свое время. Какие недостатки были у этого метода шифрования?
22) Рассчитайте количество возможных вариантов ключа для шифра Цезаря, если известно, что в алфавите используется 33 символа. Объясните, почему данный шифр считается уязвимым для современных методов криптоанализа.
23) Определите, какой метод шифрования использовался в следующем сообщении: “БМЪЛЪЖЪПЪ” (исходное сообщение “АЛФАВИТ”). Опишите алгоритм расшифровки и объясните, почему этот метод считается более надежным, чем простой шифр Цезаря.
24) Вычислите длину ключевого слова для шифра Виженера, если известно, что в зашифрованном тексте длиной 100 символов обнаружено 20 повторений определенных буквенных комбинаций через равные промежутки.
25) Прочитайте текст и запишите развернутый обоснованный ответ: В 1940-х годах немецкая армия использовала шифровальную машину “Энигма”. Объясните принцип работы этой машины и почему она считалась практически неуязвимой. Какие факторы привели к ее взлому?
26) Определите, какой метод шифрования является более надежным: симметричный или асимметричный. Приведите примеры использования каждого метода в современном мире и объясните их преимущества и недостатки.
27) Рассчитайте количество возможных комбинаций ключей для симметричного алгоритма шифрования, если длина ключа составляет 128 бит. Объясните, почему такая длина считается достаточной для обеспечения безопасности данных.
28) Прочитайте текст и запишите развернутый ответ: В процессе передачи данных через незащищенный канал была обнаружена атака “человек посередине”. Опишите механизм этой атаки и предложите методы защиты от нее.
29) Определите, какие преимущества дает использование “одноразового шифрблокнота” по сравнению с другими методами шифрования. Объясните, почему этот метод считается абсолютно надежным, несмотря на свои недостатки.
30) Вычислите время, необходимое для взлома асимметричного ключа длиной 2048 бит при современных вычислительных мощностях. Объясните, почему асимметричное шифрование используется преимущественно для обмена симметричными ключами, а не для шифрования самих данных.

ОПК-14: Способен разрабатывать алгоритмы и компьютерные программы, пригодные для практического применения.
Индикатор Знать
1) Установите правильную последовательность появления криптографических методов
А) Шифр Скитала
Б) Решетка Кардано
В) Шифр Виженера
Г) Машина Энигма
2) Установите правильную последовательность этапов работы с цифровой подписью
А) Формирование хеша сообщения
Б) Шифрование хеша закрытым ключом
В) Передача подписи вместе с сообщением
Г) Проверка подписи открытым ключом
3) Установите правильную последовательность развития асимметричного шифрования
А) Создание алгоритма RSA
Б) Разработка концепции открытого ключа
В) Появление протокола Диффи-Хеллмана
Г) Использование в SSL/TLS
4) Установите правильную последовательность действий при использовании одноразового шифроблокнота
А) Генерация случайной последовательности
Б) Запись ключа в блокнот
В) Побитовое сложение с текстом
Г) Уничтожение использованного ключа

3. Требует уничтожения ключа после использования
4. Механическое устройство для перестановки символов
5. Позволяет скрывать сообщение в тексте
7) Установите соответствие между криптографическими понятиями и их определениями
А) Криптография
Б) Криптоанализ
В) Стенография
Г) Цифровая подпись
1. Наука о создании методов шифрования
2. Наука о взломе шифров
3. Метод подтверждения подлинности документа
4. Симметричный алгоритм шифрования
5. Сокрытие факта передачи сообщения
8) Установите соответствие между историческими шифровальными устройствами и их особенностями
А) Скитала
Б) Машина Энигма
В) Роторная машина Хеберна
Г) Дисковый шифратор Джефферсона
1. Использовала набор роторов для шифрования
2. Античный шифр перестановки с использованием цилиндра
3. Первая американская роторная машина
4. Портативное устройство с 36 дисками
5. Применяла рефлектор для двойного шифрования
9) Установите соответствие между типами шифрования и их свойствами
А) Симметричное шифрование
Б) Асимметричное шифрование
В) Хеш-функции
Г) Квантовое шифрование
1. Использует открытый и закрытый ключи
2. Одинаковый ключ для шифрования и дешифровки
3. Преобразование данных фиксированной длины
4. Уязвимо к атаке "человек посередине"
5. Основано на принципах квантовой физики
10) Установите соответствие между криптографическими атаками и их описанием
А) Атака "грубой силы"
Б) Атака "человек посередине"
В) Атака на основе времени
Г) Дифференциальный криптоанализ
1. Анализ времени выполнения операций
2. Перебор всех возможных ключей
3. Подмена ключей в канале связи
4. Анализ различий в шифротекстах
5. Использование социальной инженерии

Индикатор Уметь
11) Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор:
Какой шифр является примером моноалфавитной замены?
А) Шифр Виженера
Б) Шифр Цезаря
В) Одноразовый блокнот
Г) Решетка Кардано
12) Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор:
Какой метод криптоанализа использовался для взлома шифра Энигмы?
А) Атака "грубой силы"
Б) Дифференциальный криптоанализ
В) Метод "Бомбы" Тьюринга
Г) Частотный анализ
13) Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор:
Какой алгоритм относится к асимметричному шифрованию?
А) AES
Б) DES
В) RSA
Г) Blowfish
14) Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор:
Какой элемент не входит в состав цифровой подписи?
А) Хеш-функция
Б) Закрытый ключ
В) Симметричный шифр
Г) Открытый ключ

15) Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор:
Какой метод защиты информации основан на сокрытии самого факта передачи данных?
А) Криптография
Б) Стенография
В) Хеширование
Г) Шифрование
16) Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор:
Какой недостаток характерен для одноразового шифроблокнота?
А) Низкая стойкость к частотному анализу
Б) Сложность генерации истинно случайных ключей
В) Ограниченная длина ключа
Г) Возможность повторного использования ключа
17) Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор:
Какой принцип лежит в основе асимметричного шифрования?
А) Использование одного ключа для шифрования и дешифрования
Б) Математическая сложность факторизации больших чисел
В) Подстановка и перестановка символов
Г) Применение роторных механизмов
18) Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор:
Какой элемент не используется в криптографических протоколах?
А) Сертификаты
Б) Удостоверяющие центры
В) Стенографические контейнеры
Г) Хеш-функции
19) Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор:
Какой метод позволяет защититься от атаки "человек посередине"?
А) Использование симметричного шифрования
Б) Применение цифровых сертификатов
В) Увеличение длины ключа
Г) Частая смена алгоритмов шифрования
20) Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор:
Какой исторический шифр использовал цилиндр для перестановки символов?
А) Шифр Цезаря
Б) Скитала
В) Машина Энигма
Г) Дисковый шифратор Джефферсона

Индикатор Владеть
21) Вычислите контрольную сумму CRC-8 для сообщения "10100110" при использовании генераторного полинома $x^3 + x + 1$ (1011).
и запишите ответ
22) Вычислите общий секретный ключ по алгоритму Диффи-Хеллмана, если:
o Общие параметры: p = 23, g = 5
o Секретный ключ Алисы: a = 6
o Секретный ключ Боба: b = 15
и запишите ответ
23) Рассчитайте время, необходимое для полного перебора всех возможных комбинаций 8-символьного пароля, состоящего из цифр и латинских букв (верхний и нижний регистр), если скорость перебора составляет 1 миллион паролей в секунду.
и запишите ответ
24) Определите, можно ли считать безопасным соединение с сайтом, если при проверке сертификата обнаружены следующие параметры:
o Алгоритм подписи: SHA-1
o Длина ключа: 1024 бит
o Срок действия: 5 лет
Обоснуйте ответ.

25) Определите минимально необходимую длину симметричного ключа для обеспечения безопасности на 10 лет вперед, учитывая закон Мура (удвоение вычислительной мощности каждые 2 года) и текущий стандарт в 256 бит.

26) Определите, какое количество информации (в битах) утечет при компрометации одного сеансового ключа в системе, использующей:
o Протокол TLS 1.3
o Perfect Forward Secrecy
o 1000 сеансов связи

27) Определите риск компрометации системы при использовании одного мастер-пароля для 20 различных сервисов, если вероятность взлома одного пароля составляет 0,01.

28) Определите эффективность системы обнаружения вторжений (IDS) при следующих параметрах:
o Количество реальных атак: 50
o Обнаружено атак: 45

1. Входные данные не валидировались
2. Использовались учетные записи с повышенными привилегиями
3. Журналирование было отключено
Какие конкретные меры защиты нужно реализовать для предотвращения подобных инцидентов?"

30) Прочитайте текст и запишите развернутый ответ:
"Сотрудник получил письмо с требованием срочно обновить учетные данные по ссылке. При наведении курсора ссылка показывает один адрес, а в тексте письма отображается другой. Какие действия должен предпринять сотрудник и почему?"

Вопросы к экзамену
ОПК-4: Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности;
Индикатор Знать
1) Установите правильную последовательность этапов работы с персональными данными:
а) Классификация информации
б) Настройка политик безопасности
в) Применение технических средств защиты
г) Изучение нормативно-правовой базы
2) Прочитайте текст и установите соответствие между методами и их определениями:
А) Фишинг
Б) Претекстинг
В) Квид про Кво
Г) Тайпсвотинг
1. Метод получения информации через создание ложной ситуации
2. Метод социальной инженерии с использованием подменных веб-сайтов
3. Метод обмена информацией на информацию
4. Метод анализа клавиатурного почерка
5. Метод физического доступа к устройству
3) Установите правильную последовательность появления методов социальной инженерии:
а) Фишинг
б) Претекстинг
в) Квид про Кво
г) Обратная социальная инженерия
4) Прочитайте текст и установите соответствие между типами вредоносного ПО и их характеристиками:
А) Троянский конь
Б) Шпионское ПО
В) Вирус
Г) Червь
1. Самовоспроизводящееся ПО
2. ПО, маскирующееся под полезное
3. ПО для сбора информации
4. Самораспространяющееся ПО
5. ПО для майнинга криптовалюты
5) Установите правильную последовательность действий при настройке безопасности:
а) Создание политик паролей
б) Внедрение антивирусной защиты
в) Настройка файрвола
г) Регулярное резервное копирование
6) Прочитайте текст и установите соответствие между методами защиты и их применением:
А) Двухфакторная аутентификация
Б) Шифрование данных
В) Антивирусная защита
Г) Фильтрация контента
1. Защита от вредоносного ПО
2. Защита при передаче данных
3. Усиленная аутентификация
4. Контроль доступа к информации
5. Защита от DDoS-атак
7) Установите правильную последовательность действий при обнаружении утечки данных:
а) Уведомление регуляторов
б) Оценка масштаба утечки
в) Устранение причин
г) Информирование субъектов ПД
8) Прочитайте текст и установите соответствие между типами паролей и их характеристиками:
А) Простой пароль
Б) Композитный пароль
В) Фраза-пароль
Г) Биометрический пароль
1. Использование нескольких типов символов

2. Использование отпечатка пальца
3. Использование простой комбинации
4. Использование длинной фразы
5. Использование графического ключа
9) Установите правильную последовательность методов сбора информации:
а) Анализ открытых источников
б) Социальная инженерия
в) Физический доступ
г) Кибербразведка
10) Прочитайте текст и установите соответствие между методами защиты и их функциями:
А) VPN
Б) SSL-шифрование
В) Брандмауэр
Г) Антивирус
1. Защита при передаче данных
2. Контроль сетевого трафика
3. Защита от вредоносного ПО
4. Защита веб-соединений
5. Защита от DoS-атак

Индикатор Уметь
11) Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор:
Какой метод защиты информации относится к техническим средствам?
а) Классификация данных
б) Антивирусная защита
в) Политика безопасности
г) Обучение персонала
12) Выберите правильные ответы и запишите аргументы, обосновывающие выбор ответа:
Какие характеристики относятся к стойкому паролю?
а) Использование только букв
б) Длина не менее 12 символов
в) Комбинация разных типов символов
г) Простой словарный пароль
13) Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор:
Что такое фишинг?
а) Метод физического доступа к устройству
б) Метод социальной инженерии с подменными сайтами
в) Метод криптоанализа
г) Метод стеганографии
14) Выберите правильные ответы и запишите аргументы, обосновывающие выбор ответа:
Какие методы относятся к вредоносному ПО?
а) Троянский конь
б) Антивирус
в) Вирус
г) Файрвол
15) Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор:
Что такое претекстинг?
а) Метод анализа клавиатурного почерка
б) Метод получения информации через создание ложной ситуации
в) Метод обмена информацией
г) Метод фишинга
16) Выберите правильные ответы и запишите аргументы, обосновывающие выбор ответа:
Какие способы защиты от вредоносного ПО существуют?
а) Использование антивируса
б) Регулярное резервное копирование
в) Двухфакторная аутентификация
г) Обновление ПО
17) Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор:
Что такое обратная социальная инженерия?
а) Метод сбора информации из открытых источников
б) Метод, при котором жертва сама предоставляет информацию
в) Метод фишинга
г) Метод претекстинга
18) Выберите правильные ответы и запишите аргументы, обосновывающие выбор ответа:
Какие характеристики относятся к политике безопасности?
а) Правила доступа к информации
б) Методы шифрования данных
в) Порядок реагирования на инциденты
г) Технические средства защиты

19) Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор:
Что такое “дорожное яблоко”?
а) Метод фишинга
б) Метод социальной инженерии с использованием заражённых носителей
в) Метод претекстинга
г) Метод криптоанализа
20) Выберите правильные ответы и запишите аргументы, обосновывающие выбор ответа:
Какие методы относятся к классификации информации?
а) Определение уровней конфиденциальности
б) Настройка файрвола
в) Категорирование по степени важности
г) Использование VPN

Индикатор Владеть
21) Прочитайте текст и запишите развернутый ответ: В организации произошел инцидент с утечкой персональных данных. Определите, какие нормативные акты были нарушены и какие меры наказания могут последовать согласно действующему законодательству.
22) Рассчитайте минимальный срок хранения журналов регистрации событий информационной безопасности, если организация обрабатывает специальные категории персональных данных. Обоснуйте свой ответ со ссылкой на законодательство.
23) Определите категорию конфиденциальности информации, если в документе содержатся персональные данные 1000 сотрудников, включая банковские реквизиты. Объясните выбор категории с учетом возможных рисков утечки.
24) Вычислите количество возможных комбинаций для пароля, состоящего из 8 символов (буквы, цифры, спецсимволы). Оцените его стойкость к подбору и предложите рекомендации по усилению.
25) Прочитайте текст и запишите развернутый обоснованный ответ: В компанию поступил подозрительный email от “банковского сервиса”. Опишите признаки фишингового сообщения и предложите алгоритм действий сотрудника при получении подобных писем.
26) Определите, какой метод социальной инженерии использовался, если злоумышленник представился сотрудником техподдержки и запросил пароль от учетной записи. Объясните, почему этот метод эффективен и как от него защититься.
27) Рассчитайте время, необходимое для подбора пароля, состоящего из 12 случайных символов, при скорости 1 миллиард попыток в секунду. Оцените практическую стойкость такого пароля.
28) Прочитайте текст и запишите развернутый ответ: В организации обнаружены следы вредоносного ПО. Определите основные признаки заражения и предложите порядок действий по ликвидации последствий.
29) Определите, какие технические средства защиты необходимо внедрить для предотвращения утечки персональных данных через съемные носители информации. Обоснуйте выбор каждого средства.
30) Вычислите минимальный размер выборки для аудита паролей сотрудников, если в организации работает 500 человек, с доверительной вероятностью 95%. Объясните методику расчета.

ОПК-14: Способен разрабатывать алгоритмы и компьютерные программы, пригодные для практического применения.
Индикатор знать
1) Установите правильную последовательность действий при настройке защиты персональных данных в АСУ ТП:
А) Внедрение технических средств защиты
Б) Классификация и категорирование информации
В) Разработка политики безопасности
Г) Проведение аудита существующих систем
2) Установите правильную последовательность этапов криптоанализа при попытке взлома шифра:
А) Сбор статистических данных
Б) Определение типа шифра
В) Поиск уязвимостей алгоритма
Г) Построение математической модели
3) Установите правильную последовательность действий при настройке криптографической защиты в АСУ ТП:
А) Генерация ключей шифрования
Б) Выбор алгоритма шифрования
В) Настройка криптографических параметров
Г) Внедрение сертификатов безопасности
4) Установите правильную последовательность этапов защиты от фишинговых атак в промышленных системах:
А) Обучение персонала
Б) Внедрение антивирусного ПО
В) Настройка фильтров электронной почты
Г) Создание политик безопасности
5) Установите правильную последовательность действий при настройке цифровой подписи в АСУ ТП:
А) Получение сертификата от УЦ
Б) Генерация ключевой пары
В) Настройка программного обеспечения
Г) Внедрение процедуры подписания
6) Установите соответствие между методами защиты АСУ ТП и их применением в промышленных системах:
А) Шифрование каналов связи
Б) Межсетевой экран
В) Система контроля доступа
Г) Система обнаружения вторжений

2. Подмена данных в промышленном протоколе
3. Манипуляция операторами для получения доступа
4. Кража конфигурационных файлов
5. Физическое повреждение оборудования
8) Установите соответствие между криптографическими алгоритмами и их применением в АСУ ТП:
А) AES-256
Б) RSA-2048
В) SHA-256
Г) ECC
1. Генерация ключей для цифровых подписей
2. Шифрование конфигураций ПЛК
3. Проверка целостности прошивки
4. Защита каналов связи между контроллерами
5. Аутентификация датчиков
9) Установите соответствие между этапами защиты промышленных данных и их содержанием:
А) Классификация данных
Б) Категорирование систем
В) Защита каналов передачи
Г) Мониторинг событий
1. Внедрение VPN-туннелей
2. Распределение систем по уровням безопасности
3. Определение критичности производственных данных
4. Анализ журналов событий ПЛК
5. Резервное копирование конфигураций
10) Установите соответствие между типами вредоносного ПО и их действиями в АСУ ТП:
А) Промышленный вирус
Б) Троян для ПЛК
В) Шпионское ПО
Г) Рекламное ПО
1. Сбор данных о настройках оборудования
2. Изменение параметров работы контроллера
3. Распространение через USB-накопители
4. Кража учетных данных операторов
5. Нарушение работы HMI-интерфейсов

Индикатор Уметь
11) Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор:
Какой метод шифрования является наиболее надежным для защиты каналов связи в АСУ ТП?
А) DES
Б) AES-256
В) RSA-1024
Г) SHA-256
12) Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор:
Какой тип атаки представляет наибольшую угрозу для промышленных систем управления?
А) DDoS-атака
Б) Фишинговая атака
В) MITM-атака
Г) Социальная инженерия
13) Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор:
Какой алгоритм используется для создания цифровых подписей в промышленных системах?
А) RSA
Б) AES
В) ECC
Г) SHA-2
14) Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор:
Какой метод защиты от вредоносного ПО наиболее эффективен для АСУ ТП?
А) Антивирусное ПО
Б) Межсетевой экран
В) Песочница
Г) Система обнаружения вторжений
15) Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор:
Какой уровень защиты персональных данных требуется для систем АСУ ТП?
А) Базовый
Б) Повышенный
В) Высокий
Г) Максимальный
16) Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор:
Какой метод аутентификации считается наиболее надежным для промышленных контроллеров?
А) Пароль

Б) Сертификат
В) Биометрия
Г) Токен
17) Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор:
Какой протокол обеспечивает безопасную передачу данных в промышленных сетях?
А) Modbus TCP
Б) ProfiNet
В) TLS/SSL
Г) Ethernet IP
18) Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор:
Какой метод защиты используется для предотвращения replay-атак?
А) Шифрование
Б) Хеширование
В) Временные метки
Г) Цифровая подпись
19) Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор:
Какой алгоритм используется для генерации случайных чисел в криптографии АСУ ТП?
А) PRNG
Б) RNG
В) TRNG
Г) DRNG
20) Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор:
Какой метод защиты используется для предотвращения атак типа “человек посередине”?
А) SSL/TLS
Б) VPN
В) IPSec
Г) Цифровая подпись

Индикатор ВЛАДЕТЬ
21) Вычислите время, необходимое для полного перебора пароля, если известно, что пароль состоит из 8 символов, включает строчные и заглавные буквы латинского алфавита, цифры и специальные символы (!@#$%^&*). Скорость перебора - 1000 попыток в секунду.
22) Вычислите размер ключа в битах, необходимый для обеспечения защиты данных в АСУ ТП, если известно, что:
• Используемый алгоритм - AES
• Требуемый уровень защиты - высокий
• Система работает с персональными данными
23) Рассчитайте количество возможных комбинаций для генерации случайного пароля, если:
• Длина пароля - 12 символов
• Используются:
• 26 строчных букв
• 26 заглавных букв
• 10 цифр
• 10 специальных символов
24) Определите, какой тип атаки был осуществлен, если в системе обнаружены следующие признаки:
• Массовое изменение конфигураций ПЛК
• Появление неизвестных устройств в сети
• Аномальная активность в нерабочее время
• Отключение систем мониторинга
25) Определите, какие меры защиты необходимо применить для предотвращения фишинговой атаки, если в организации зафиксированы:
• Рост количества подозрительных писем
• Увеличение попыток входа в систему с неизвестных IP
• Активность в социальных сетях от имени компании
26) Определите, какой алгоритм шифрования следует использовать для защиты каналов связи между ПЛК и SCADA-системой, если:
• Требуемая скорость передачи данных - 1000 пакетов/сек
• Размер пакета - 1024 байта
• Допустимая задержка - не более 10 мс
27) Определите, какие действия необходимо предпринять при обнаружении вредоносного ПО в промышленной сети, если:
• Заражено 3 ПЛК
• Заражены 2 рабочих станции
• Обнаружены попытки выхода в интернет
28) Прочитайте текст и запишите развернутый ответ:
В системе АСУ ТП зафиксированы множественные попытки подбора паролей с различных IP-адресов. Опишите последовательность действий администратора безопасности для устранения угрозы и предотвращения повторных атак.
29) Прочитайте текст и запишите развернутый ответ:
При анализе журналов событий обнаружено, что один из операторов регулярно получает доступ к конфиденциальным данным вне своих должностных обязанностей. Опишите алгоритм расследования инцидента и необходимые меры реагирования.
30) Определите, какие технические средства защиты необходимо внедрить для обеспечения безопасности АСУ ТП, если:
• Система включает 50 ПЛК
• 20 рабочих станций

Итоговое тестирование
ОПК-4
Зачет
1. Что является основным отличием криптографии от криптоанализа?
а) Криптография занимается созданием шифров, криптоанализ - их взломом
б) Криптография использует открытые ключи, криптоанализ - закрытые
в) Криптография работает с текстом, криптоанализ - с числами
г) Криптография использует только симметричные методы
2. Какой шифр относится к методам перестановки?
а) Шифр Цезаря
б) Шифр Виженера
в) Шифр сциталя
г) Решетка Кардано
3. Что такое одноразовый шифр-блокнот?
а) Симметричный шифр
б) Асимметричный шифр
в) Абсолютно секретный шифр
г) Метод стеганографии
4. Какие преимущества имеет асимметричное шифрование?
а) Высокая скорость работы
б) Простота реализации
в) Возможность безопасной передачи ключей
г) Низкая ресурсоемкость
5. Что такое атака “человек посередине”?
а) Перехват и изменение передаваемых данных
б) Кража ключей шифрования
в) Взлом криптосистемы
г) Социальная инженерия
6. Какой метод шифрования использует таблицу Виженера?
а) Метод замены
б) Метод перестановки
в) Метод гаммирования
г) Метод стеганографии
7. Что такое цифровая подпись?
а) Электронный аналог обычной подписи
б) Метод шифрования данных
в) Способ подтверждения авторства документа
г) Метод аутентификации пользователя
8. Какие компоненты входят в систему сертификации?
а) Центр сертификации
б) Пользовательские сертификаты
в) Криптографические ключи
г) Все вышеперечисленное
9. Что такое криптографический протокол?
а) Набор правил для шифрования данных
б) Алгоритм работы криптосистемы
в) Набор правил и процедур для безопасного обмена информацией
г) Метод криптоанализа
10. Какой метод шифрования использует машину Энигма?
а) Симметричное шифрование
б) Асимметричное шифрование
в) Метод перестановки
г) Метод замены
11. Что такое стенография?
а) Метод шифрования
б) Метод скрытой передачи информации
в) Метод криптоанализа
г) Метод аутентификации
12. Какие недостатки имеет симметричное шифрование?
а) Низкая скорость работы
б) Сложность реализации
в) Проблема безопасного обмена ключами
г) Низкая стойкость
13. Что такое сертификат?
а) Документ, подтверждающий личность
б) Документ, подтверждающий права доступа
в) Документ, подтверждающий подлинность ключей
г) Документ, подтверждающий права собственности
14. Какой метод шифрования считается абсолютно надежным?

а) Шифр Цезаря
б) Одноразовый шифр-блокнот
в) Шифр Виженера
г) Асимметричное шифрование
15. Что такое ключ шифра?
а) Секретная информация для шифрования
б) Секретная информация для дешифрования
в) Секретная информация для обеих операций
г) Секретная информация для аутентификации

ОПК-14
1. Какой алгоритм шифрования используется в большинстве современных промышленных протоколов?
а) DES
б) AES
в) RSA
г) SHA-2
2. Что такое аутентификация в контексте АСУ ТП?
а) Шифрование данных
б) Подтверждение подлинности устройства
в) Управление доступом
г) Резервное копирование
3. Какой протокол обеспечивает безопасную передачу данных в промышленных сетях?
а) Modbus
б) ProfiNet
в) TLS/SSL
г) Ethernet
4. Что такое цифровая подпись в АСУ ТП?
а) Электронная метка устройства
б) Метод шифрования данных
в) Способ аутентификации
г) Метод верификации целостности данных
5. Какой метод защиты используется для предотвращения MITM-атак?
а) Шифрование данных
б) Цифровая подпись
в) Сертификат безопасности
г) Все вышеперечисленное
6. Что такое криптографический ключ?
а) Пароль пользователя
б) Секретная последовательность данных
в) IP-адрес устройства
г) MAC-адрес
7. Какой алгоритм используется для генерации случайных чисел в криптографии?
а) RSA
б) SHA-2
в) AES
г) PRNG
8. Что такое криптографическая хеш-функция?
а) Метод шифрования данных
б) Способ генерации ключей
в) Функция преобразования данных в фиксированную длину
г) Метод аутентификации
9. Какой протокол обеспечивает безопасную передачу файлов в промышленных сетях?
а) FTP
б) SFTP
в) TFTP
г) HTTP
10. Что такое криптоаналитическая атака?
а) Попытка взлома шифрования
б) Метод аутентификации
в) Способ шифрования
г) Метод генерации ключей
11. Какой алгоритм используется для симметричного шифрования?
а) RSA
б) AES
в) ECC
г) DSA
12. Что такое криптографический протокол?
а) Набор правил для безопасной передачи данных
б) Метод шифрования

в) Способ аутентификации
г) Метод генерации ключей
13. Какой метод используется для защиты от replay-атак?
а) Шифрование
б) Хеширование
в) Временные метки
г) Цифровая подпись
14. Что такое криптографический сертификат?
а) Документ, подтверждающий подлинность устройства
б) Метод шифрования
в) Способ аутентификации
г) Метод генерации ключей
15. Какой алгоритм используется для асимметричного шифрования?
а) AES
б) RSA
в) DES
г) SHA-2

Экзамен
ОПК-4
1. Какой нормативно-правовой акт регулирует защиту персональных данных в России?
а) ФЗ-152
б) ФЗ-98
в) ФЗ-242
г) ФЗ-352
2. Какие методы шифрования относятся к симметричным?
а) Шифр Цезаря
б) RSA
в) Шифр Виженера
г) Эллиптические кривые
3. Что относится к техническим средствам защиты персональных данных?
а) DLP-системы
б) Антивирусное ПО
в) Системы контроля доступа
г) Все вышеперечисленное
4. Какие признаки указывают на возможное заражение троянским ПО?
а) Замедление работы системы
б) Необычное поведение программ
в) Увеличение потребления ресурсов
г) Все вышеперечисленное
5. Какой метод социальной инженерии предполагает создание ложной ситуации?
а) Претекстинг
б) Фишинг
в) Тайпсвотинг
г) Квид про Кво
6. Что такое “дорожное яблоко”?
а) Метод социальной инженерии
б) Вид вредоносного ПО
в) Способ шифрования
г) Метод криптоанализа
7. Какие компоненты входят в систему цифровой подписи?
а) Открытый ключ
б) Закрытый ключ
в) Сертификат
г) Все вышеперечисленное
8. Что обеспечивает абсолютная секретность при правильном использовании?
а) Шифр Цезаря
б) Одноразовый шифр-блокнот
в) Шифр Виженера
г) Асимметричное шифрование
9. Какие характеристики должны быть у современного криптографического протокола?
а) Стойкость к атакам
б) Масштабируемость
в) Простота реализации
г) Все вышеперечисленное
10. Что относится к методам сбора информации из открытых источников?
а) Анализ социальных сетей
б) Изучение публичных баз данных
в) Мониторинг форумов

г) Все вышеперечисленное
11. Какие политики безопасности защищают от вредоносного ПО?
а) Запрет на съемные носители
б) Контроль доступа
в) Мониторинг активности
г) Все вышеперечисленное
12. Что такое атака “человек посередине”?
а) Перехват данных
б) Подмена ключей
в) Фишинг
г) Социальная инженерия
13. Какие методы защиты от фишинга являются наиболее эффективными?
а) Антиспам-фильтры
б) Проверка URL
в) Обучение персонала
г) Все вышеперечисленное
14. Что относится к категории конфиденциальной информации?
а) Персональные данные
б) Коммерческая тайна
в) Служебная тайна
г) Все вышеперечисленное
15. Какие требования предъявляются к стойким паролям?
а) Длина не менее 12 символов
б) Использование разных типов символов
в) Отсутствие словарных слов
г) Все вышеперечисленное

ОПК-14
1. Какой признак является наиболее надежным индикатором фишингового письма?
А) Наличие грамматических ошибок
Б) Подозрительный адрес отправителя
В) Требование немедленных действий
Г) Ссылка на поддельный сайт
2. Какой метод социальной инженерии часто используется для получения паролей?
А) Претекстинг
Б) Фишинг
В) Тайпсвотинг
Г) Квид про кво
3. Какое действие является первым шагом при обнаружении вредоносного ПО?
А) Отключение устройства от сети
Б) Запуск антивирусной проверки
В) Сохранение важных данных
Г) Обращение в службу безопасности
4. Какой тип вредоносного ПО маскируется под полезное приложение?
А) Вирус
Б) Троян
В) Червь
Г) Шпионское ПО
5. Какая комбинация символов считается наиболее надежным паролем?
А) Только цифры
Б) Только буквы
В) Буквы и цифры
Г) Буквы, цифры и специальные символы
6. Какой метод защиты от фишинга является наиболее эффективным?
А) Антивирусное ПО
Б) Двухфакторная аутентификация
В) Фильтрация почты
Г) Обучение персонала
7. Что такое “дорожное яблоко” в контексте социальной инженерии?
А) Подброшенный USB-накопитель
Б) Фальшивое электронное письмо
В) Поддельная веб-страница
Г) Социальная сеть
8. Какой метод сбора информации относится к социальной инженерии?
А) Анализ открытых источников
Б) Взлом системы
В) Установка жучков
Г) Физическое проникновение
9. Что является основным признаком заражения системы трояном?

А) Медленная работа
Б) Появление новых файлов
В) Изменение настроек
Г) Все вышеперечисленное
10. Какой метод защиты от вредоносного ПО является первичным?
А) Антивирусное ПО
Б) Межсетевой экран
В) Система обнаружения вторжений
Г) Резервное копирование
11. Что такое обратная социальная инженерия?
А) Манипуляция через доверие
Б) Манипуляция через угрозы
В) Манипуляция через подмену личности
Г) Манипуляция через обман
12. Какой признак указывает на заражение системы шпионским ПО?
А) Медленная работа
Б) Необычные системные процессы
В) Реклама в браузере
Г) Все вышеперечисленное
13. Что такое тайпсвотинг?
А) Перехват нажатий клавиш
Б) Перехват сетевого трафика
В) Перехват видео с экрана
Г) Перехват звука
14. Какой метод защиты от вредоносного ПО является вторичным?
А) Антивирусное ПО
Б) Система обнаружения вторжений
В) Межсетевой экран
Г) Резервное копирование
15. Что является основным признаком фишингового сайта?
А) Подозрительный URL
Б) Отсутствие HTTPS
В) Фальшивые контактные данные
Г) Все вышеперечисленное

6.5. Примерная тематика курсовых работ (проектов)

Учебным планом не предусмотрено

6.6. Методические указания для обучающихся по освоению дисциплины (модуля)

Методические рекомендации по подготовке к лекционным занятиям

Просмотрите конспект сразу после занятий. Пометьте материал конспекта лекций, который вызывает затруднения для понимания. Попытайтесь найти ответы на затруднительные вопросы, используя предлагаемую литературу. Если самостоятельно не удалось разобраться в материале, сформулируйте вопросы и обратитесь на текущей консультации или на ближайшей лекции за помощью к преподавателю. Каждую неделю рекомендуется отводить время для повторения пройденного материала, проверяя свои знания, умения и навыки по контрольным вопросам.
Работа с рекомендованной литературой:
При работе с основной и дополнительной литературой целесообразно придерживаться такой последовательности. Сначала прочитать весь заданный текст в быстром темпе. Цель такого чтения заключается в том, чтобы создать общее представление об изучаемом материале, понять общий смысл прочитанного. Затем прочитать вторично, более медленно, чтобы в ходе чтения понять и запомнить смысл каждой фразы, каждого положения и вопроса в целом. Чтение приносит пользу и становится продуктивным, когда сопровождается записями. Это может быть составление плана прочитанного текста, тезисы или выписки, конспектирование и др. Выбор вида записи зависит от характера изучаемого материала и целей работы с ним. Если содержание материала несложное, легко усваиваемое, можно ограничиться составлением плана. Если материал содержит новую и трудно усваиваемую информацию, целесообразно его законспектировать. План – это схема прочитанного материала, перечень вопросов, отражающих структуру и последовательность материала. Конспект – это систематизированное, логичное изложение материала источника. Различаются четыре типа конспектов: - план-конспект – это развернутый детализированный план, в котором по наиболее сложным вопросам даются подробные пояснения, - текстуальный конспект – это воспроизведение наиболее важных положений и фактов источника, - свободный конспект – это четко и кратко изложенные основные положения в результате глубокого изучения материала, могут присутствовать выписки, цитаты, тезисы; часть материала может быть представлена планом, - тематический конспект – составляется на основе изучения ряда источников и дает ответ по изучаемому вопросу. В процессе изучения материала источника и составления конспекта нужно обязательно применять различные выделения, подзаголовки, создавая блочную структуру конспекта. Это делает конспект легко воспринимаемым и удобным для работы.

Методические рекомендации по подготовке к практическим занятиям

Практические занятия представляют особую форму сочетания теории и практики. Их назначение – углубление проработки

теоретического материала предмета путем регулярной и планомерной самостоятельной работы студентов на протяжении всего курса. Процесс подготовки к практическим занятиям включает изучение нормативных документов, обязательной и дополнительной литературы по рассматриваемому вопросу. Непосредственное проведение практического занятия предполагает, например:
- индивидуальные выступления студентов с сообщениями по какому-либо вопросу изучаемой темы;
- фронтальное обсуждение рассматриваемой проблемы, обобщения и выводы;
- решение задач и упражнений по образцу;
- решение вариантных задач и упражнений;
- решение ситуационных производственных (профессиональных) задач;
- проектирование и моделирование разных видов и компонентов профессиональной деятельности;
- выполнение контрольных работ;
- работу с тестами.
При подготовке к практическим занятиям студентам рекомендуется: внимательно ознакомиться с тематикой практического занятия; прочесть конспект лекции по теме, изучить рекомендованную литературу; составить краткий план ответа на каждый вопрос практического занятия; проверить свои знания, отвечая на вопросы для самопроверки; если встретятся незнакомые термины, обязательно обратиться к словарю и зафиксировать их в тетради. Все письменные задания выполнять в рабочей тетради. Практические занятия развивают у студентов навыки самостоятельной работы по решению конкретных задач.

Методические рекомендации по подготовке к лабораторным работам

Лабораторные работы представляют одну из форм освоения теоретического материала с одновременным формированием практических навыков в изучаемой дисциплине (модуле). Их назначение – углубление проработки теоретического материала, формирование практических навыков путем регулярной и планомерной самостоятельной работы студентов на протяжении всего курса. Процесс подготовки к лабораторным работам включает изучение нормативных документов, обязательной и дополнительной литературы по рассматриваемому вопросу. Непосредственное проведение лабораторной работы предполагает:
- изучение теоретического материала по теме лабораторной работы (по вопросам изучаемой темы);
- выполнение необходимых расчетов и экспериментов;
- оформление отчета с заполнением необходимых таблиц, построением графиков, подготовкой выводов по проделанным экспериментам и теоретическим расчетам;
- по каждой лабораторной работе проводится контроль: проверяется содержание отчета, проверяется усвоение теоретического материала.
Контроль усвоения теоретического материала является индивидуальным.

Методические указания по выполнению отчёта к лабораторным работам

Основным требованием по выполнению лабораторных и практических работ является полное исчерпывающее описание всей проделанной работы, позволяющее судить о полученных результатах, степени выполнения и профессиональной подготовки студентов.
Методические указания обеспечивают комплексный подход в учебной работе студентов, единство и преемственность требований к оформлению результатов работы на разных этапах обучения. С единых позиций приведены основные требования к структуре, оформлению и содержанию отчета по лабораторным и практическим работам.
Структура отчёта:
- цель работы;
- краткие теоретические сведения;
- ход выполнения работы;
- выводы.
Дополнительные элементы:
- приложения;
- библиографический список.
Требования к содержанию отчёта:
1. Титульный лист
В верхнем поле листа указывают полное наименование учебного заведения.
В среднем поле указывается вид работы, в данном случае лабораторная или практическая работа с указанием курса, по которому она выполнена, и ниже ее название. Название работы приводится без слова "тема" и в кавычки не заключается.
Далее ближе к правому краю титульного листа указывают фамилию, инициалы и группу учащегося, выполнившего работу, а также фамилию, инициалы преподавателя, принявшего работу.
В нижнем поле листа указывается место выполнения работы и год ее написания (без слова год).
2. Цель работы должна отражать тему работы, а также конкретные задачи, поставленные студенту на период выполнения работы. По объему цель работы в зависимости от сложности и многозадачности работы составляет от нескольких строк до 0,5 страницы.
3. Краткие теоретические сведения. В этом разделе излагается краткое теоретическое описание изучаемой в работе темы. Материал раздела не должен копировать содержание методического пособия или учебника по данной теме, а ограничивается изложением основных понятий, требующихся для дальнейшей обработки полученных результатов. Объем литературного обзора не должен превышать 1/3 части всего отчета.
4. Ход выполнения работы. В данном разделе подробно излагается методика выполнения работы, процесс получения данных и способ их обработки. Если используются стандартные пакеты компьютерных программ для обработки экспериментальных результатов, то необходимо обосновать возможность и целесообразность их применения, а также

подробности обработки данных с их помощью.
5. Выводы по работе - кратко излагаются результаты работы, полученные в результате выполнения работы, а также краткий анализ полученных результатов.
Отчет по лабораторной работе оформляется на листе формата А4. Допускается оформление отчета по лабораторной работе в электронном виде средствами Microsoft Office. Текст работы должен быть напечатан через полтора интервала шрифтом Times New Roman, кегль – 12. Поля должны оставаться по всем четырем сторонам печатного листа: левое – не менее 30 мм, правое – не менее 10, нижнее – не менее 20 и верхнее – не 15 мм.
Для защиты лабораторной работы студент должен подготовить отчет, провести самостоятельную работу, иметь отметку о проверенном отчете.
Результаты определяются по пятибалльной системе оценок.

Методические рекомендации по выполнению реферата

Реферат – письменная работа объемом 8–10 страниц. Это краткое и точное изложение сущности какого-либо вопроса, темы. Тему реферата студент выбирает из предложенных преподавателем или может предложить свой вариант. В реферате нужны развернутые аргументы, рассуждения, сравнения. Содержание темы излагается объективно от имени автора. Функции реферата: информативная, поисковая, справочная, сигнальная, коммуникативная. Степень выполнения этих функций зависит от содержательных и формальных качеств реферата и для каких целей их использует. Требования к языку реферата: должен отличаться точностью, краткостью, ясностью и простотой.
Структура реферата:
1. Титульный лист
2. Оглавление (на отдельной странице). Указываются названия всех разделов (пунктов плана) реферата и номера страниц, указывающие начало этих разделов в тексте реферата.
3. Введение. Аргументируется актуальность исследования, т.е. выявляется практическое и теоретическое значение данного исследования. Далее констатируется, что сделано в данной области предшественниками, перечисляются положения, которые должны быть обоснованы. Обязательно формулируются цель и задачи реферата.
4. Основная часть. Подчиняется собственному плану, что отражается в разделении текста на главы, параграфы, пункты. План основной части может быть составлен с использованием различных методов группировки материала. В случае если используется чья-либо неординарная мысль, идея, то обязательно нужно сделать ссылку на того автора, у кого взят данный материал.
5. Заключение. Последняя часть научного текста. В краткой и сжатой форме излагаются полученные результаты, представляющие собой ответ на главный вопрос исследования.
6. Приложение. Может включать графики, таблицы, расчеты.
7. Библиография (список литературы). Указывается реально использованная для написания реферата литература. Названия книг располагаются по алфавиту с указанием их выходных данных. Общие требования к построению, содержанию и оформлению».
При проверке реферата оцениваются:
- знание фактического материала, усвоение общих представлений, понятий, идей;
- характеристика реализации цели и задач исследования;
- степень обоснованности аргументов и обобщений;
- качество и ценность полученных результатов;
- использование литературных источников;
- культура письменного изложения материала;
- культура оформления материалов работы.
Правила написания научных текстов (реферат):
Здесь приводятся рекомендации по консультированию студентов относительно данного вида самостоятельной работы. Во время консультаций руководителю следует предложить к обсуждению следующие вопросы.
• Какова истинная цель Вашего научного текста – это поможет Вам разумно распределить свои силы и время.
• Важно разобраться, кто будет «читателем» Вашей работы.
• Начинать писать серьезную работу следует не раньше, чем возникнет ощущение, что по работе с источниками появились идеи, которыми можно поделиться.
• Должна быть идея, а для этого нужно научиться либо относиться к разным явлениям и фактам несколько критически (своя идея – как иная точка зрения), либо научиться увлекаться какими-то известными идеями, которые нуждаются в доработке (идея – как оптимистическая позиция и направленность на дальнейшее совершенствование уже известного).
• Писать следует ясно и понятно, стараясь основные положения формулировать четко и недвусмысленно, а также стремясь структурировать свой текст.
• Объем текста и различные оформительские требования во многом зависят от принятых в конкретном учебном заведении порядков.

Методические рекомендации по выполнению контрольных работ

Контрольная работа выполняется по вариантам. На бланке указывается факультет, курс, группа, ФИО студента. Вопросы строятся на основе тестовых и ситуативных заданий. В тестовых заданиях, выбирается правильный(ые) ответ(ы). При решении ситуативных заданий выбирается правильная последовательность действий в рассматриваемой ситуации.
Проверка контрольной работы позволяет выявить и исправить допущенные студентами ошибки, указать, какие вопросы дисциплины (модуля) ими недостаточно усвоены и требуют доработки. Студент должен внимательно ознакомиться с письменными замечаниями преподавателя и приступить к их исправлению, для чего еще раз повторить соответствующий материал.

Методические рекомендации по подготовке к коллоквиуму

Коллоквиумом называется собеседование преподавателя и студента по заранее определенным контрольным вопросам. Целью коллоквиума является формирование у студента навыков анализа теоретических проблем на основе самостоятельного изучения учебной и научной литературы. На коллоквиум выносятся крупные, проблемные, нередко спорные теоретические вопросы. Упор делается на монографические работы профессора-автора данного спецкурса. От студента требуется:
- владение изученным в ходе учебного процесса материалом, относящимся к рассматриваемой проблеме;
- знание разных точек зрения, высказанных в научной литературе по соответствующей проблеме, умение сопоставлять их между собой;
- наличие собственного мнения по обсуждаемым вопросам и умение его аргументировать.
Коллоквиум - это не только форма контроля, но и метод углубления, закрепления знаний студентов, так как в ходе собеседования преподаватель разъясняет сложные вопросы, возникающие у студента в процессе изучения данного источника. Однако коллоквиум не консультация и не экзамен. Его задача добиться глубокого изучения отобранного материала, пробудить у студента стремление к чтению дополнительной социологической литературы. Подготовка к коллоквиуму начинается с установочной консультации преподавателя, на которой он разъясняет развернутую тематику проблемы, рекомендует литературу для изучения и объясняет процедуру проведения коллоквиума. Как правило, на самостоятельную подготовку к коллоквиуму студенту отводится 3-4 недели. Методические указания состоят из рекомендаций по изучению источников и литературы, вопросов для самопроверки и кратких конспектов ответа с перечислением основных фактов и событий, относящихся к пунктам плана каждой темы. Это должно помочь студентам целенаправленно организовать работу по овладению материалом и его запоминанию. При подготовке к коллоквиуму следует, прежде всего, просмотреть конспекты лекций и практических занятий и отметить в них имеющиеся вопросы коллоквиума. Если какие-то вопросы вынесены преподавателем на самостоятельное изучение, следует обратиться к учебной литературе, рекомендованной преподавателем в качестве источника сведений.
Коллоквиум проводится в форме индивидуальной беседы преподавателя с каждым студентом или беседы в небольших группах (2-3 человека). Обычно преподаватель задает несколько кратких конкретных вопросов, позволяющих выяснить степень добросовестности работы с литературой, проверяет конспект. Далее более подробно обсуждается какая-либо сторона проблемы, что позволяет оценить уровень понимания. По итогам коллоквиума выставляется дифференцированная оценка по пятибалльной системе.

Методические рекомендации по устному опросу/самоподготовке

После изучения определенной темы по записям в конспекте и учебнику, а также решения достаточного количества соответствующих задач на практических занятиях и самостоятельно студенту рекомендуется, используя лист опорных сигналов,
воспроизвести по памяти определения, выводы формул, формулировки основных положений и доказательств. В случае необходимости следует рекомендовать еще раз внимательно разобраться в материале. Иногда недостаточность усвоения того или иного вопроса выясняется только при изучении дальнейшего материала. В этом случае надо вернуться назад и повторить плохо усвоенный материал. Важный критерий усвоения теоретического материала – умение решать задачи или пройти тестирование по пройденному материалу. Однако преподавателю следует помнить, что правильное решение задачи может получиться в результате применения механически заученных формул без понимания сущности теоретических положений.

Методические рекомендации по подготовке к семинарским занятиям

Одним из видов внеаудиторной самостоятельной работы является подготовка к семинарским занятиям. Семинар – форма учебно-практических занятий, при которой студенты обсуждают сообщения, доклады и рефераты, выполненные ими по результатам учебных или научных исследований под руководством преподавателя. Преподаватель в этом случае является координатором обсуждений темы семинара, подготовка к которому является обязательной. Поэтому тема семинара и основные источники обсуждения предъявляются до обсуждения для детального ознакомления, изучения. Цели обсуждений направлены на формирование навыков профессиональной полемики и закрепление обсуждаемого материала. Семинар – это такая форма организации обучения, при которой на этапе подготовки доминирует самостоятельная работа учащихся с учебной литературой и другими дидактическими средствами над серией вопросов, проблем и задач, а в процессе семинара идут активное обсуждение, дискуссии и выступления учащихся, где они под руководством преподавателя делают обобщающие выводы и заключения. Семинар предназначен для углубленного изучения дисциплины, овладения методологией научного познания, то главная цель семинарских занятий – обеспечить студентам возможность овладеть навыками и умениями использования теоретического знания применительно к особенностям изучаемой отрасли.

Методические рекомендации по подготовке к эссе

Одним из видов самостоятельной работы студентов является написание творческой работы по заданной либо согласованной с преподавателем теме. Творческая работа (эссе) представляет собой оригинальное произведение объемом 500-700 слов, посвященное какой-либо значимой классической либо современной проблеме в определенной теоретической и практической области. Творческая работа не является рефератом и не должна носить описательный характер, большое место в ней должно быть уделено аргументированному представлению своей точки зрения студентами, критической оценке рассматриваемого материала и проблематики, что должно способствовать раскрытию творческих и аналитических способностей. Цели написания эссе – научиться логически верно и аргументировано строить устную и письменную речь; работать над углублением и систематизацией своих философских знаний; овладеть способностью использовать основы знаний для формирования мировоззренческой позиции. Приступая к написанию эссе, изложите в одном предложении, что

именно вы будете утверждать и доказывать (свой тезис).

Методические рекомендации по подготовке к докладу

Для подготовки доклада необходимо выбрать актуальную тему. Желательно, чтобы тема была интересна докладчику и вызывала желание качественно подготовить материалы. Подготовка доклада предполагает: определение цели доклада; подбор необходимого материала, определяющего содержание доклада; составление плана доклада, распределение собранного материала в необходимой логической последовательности.
Композиция доклада имеет вступление, основную часть и заключение.
Вступление должно содержать: название доклада; сообщение основной идеи; современную оценку предмета изложения; краткое перечисление рассматриваемых вопросов; интересную для слушателей форму изложения. Основная часть, в которой необходимо раскрыть суть темы, обычно строится по принципу отчёта. Задача основной части: представить достаточно данных для того, чтобы слушатели заинтересовались темой.
Заключение – чёткое обобщение и краткие выводы по излагаемой теме.

Методические рекомендации по подготовке к собеседованию

Собеседование – средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.п.
Цель собеседования: проверка усвоения знаний; умений применять знания; сформированности профессионально значимых личностных качеств.
Подготовка к собеседованию предполагает повторение пройденного материала и приобретение навыка свободного владения терминологией и фактическими данными по определенному разделу дисциплины (модуля).

Методические рекомендации по подготовке к тестированию/ итоговому тестированию

Тестирование/итоговое тестирование – это система стандартизированных заданий, определенного содержания и упорядоченных в рамках определенной стратегии предъявления, позволяющая качественно оценить структуру и эффективно измерить уровень знаний, умений и навыков по дисциплине (модулю). Тестирование позволяет оценить у студентов уровень знаний фактического материала, умения логически мыслить, способности к рефлексии и творческому подходу к решению поставленной задачи на каждом этапе их обучения.
При самостоятельной подготовке к тестированию студенту необходимо:
- четко выяснить все условия тестирования заранее (сколько тестов будет предложено, сколько времени отводится на тестирование, какова система оценки результатов);
- проконсультироваться с преподавателем по вопросу выбора учебной литературы;
- проработать информационный материал по разделу дисциплине;
- конспективно выписать из соответствующих разделов учебной дисциплины основные понятия, ключевые идеи, теоретические концепции и подходы;
- повторить теоретический материал лекций, самостоятельно изученной учебной и научной литературы, семинарских занятий.
При выполнении тестовых заданий рекомендуется:
- внимательно полностью прочитать вопрос и предлагаемые варианты ответов, выбрать правильные из них (их может быть несколько);
- при затруднении при ответе на сложный для студента вопрос целесообразно переходить к другим вопросам теста. По завершению ответов на все последующие вопросы теста необходимо вернуться к трудному вопросу и дать на него продуманный ответ;
- по окончании тестирования следует проверить правильность данных ответов на вопросы теста, чтобы избежать механических ошибок.

Методические рекомендации по подготовке к экзамену

Изучение многих общепрофессиональных и специальных дисциплин завершается экзаменом. Подготовка к экзамену способствует закреплению, углублению и обобщению знаний, получаемых, в процессе обучения, а также применению их к решению практических задач. Готовясь к экзамену, студент ликвидирует имеющиеся пробелы в знаниях, углубляет, систематизирует и упорядочивает свои знания. На экзамене студент демонстрирует то, что он приобрел в процессе обучения по конкретной дисциплине (модулю). Экзаменационная сессия – это серия экзаменов, установленных учебным планом. Между экзаменами интервал 2-4 дня, в течение студент систематизирует уже имеющиеся знания. На консультации перед экзаменом студенты должны быть ознакомлены с основными требованиями и получить ответы на возникающие в процессе подготовки
вопросы. Необходимо ориентировать студентов на систематическую подготовку к занятиям в течение семестра, что позволит использовать время экзаменационной сессии для
систематизации знаний.

Методические рекомендации по подготовке к зачету/зачету с оценкой

В ходе подготовки к зачету/зачету с оценкой студент, в первую очередь, должен систематизировать знания, полученные в ходе изучения дисциплины. К зачету/зачету с оценкой необходимо готовиться целенаправленно, регулярно, систематически и с первых дней обучения по данной дисциплине (модулю). В самом начале учебного курса познакомьтесь со следующей

учебно-методической документацией:
- программой дисциплины (модуля);
- перечнем знаний, умений и навыков, которыми студент должен владеть;
- тематическими планами лекций, семинарских занятий;
- учебниками, учебными пособиями по дисциплине, а также электронными ресурсами;
- перечнем вопросов к зачету/зачету с оценкой.

После этого у обучающихся должно сформироваться четкое представление об объеме и характере знаний и умений, которыми надо будет овладеть по дисциплине (модулю). Систематическое выполнение учебной работы на лекциях и лабораторных занятиях позволит успешно освоить дисциплину (модуль) и создать хорошую базу для сдачи зачета/зачета с оценкой.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1. Рекомендуемая литература	
7.1.1. Основная литература	
Л.1.1	Мельников В.П., Куприянов А.И., Мельников В.П. Информационная безопасность [Электронный ресурс]:Учебник. - Москва: КноРус, 2025. - 267 с. – Режим доступа: https://book.ru/book/955528
Л.1.2	Прохорова О. В. Информационная безопасность и защита информации [Электронный ресурс]:учебник для вузов. - Санкт-Петербург: Лань, 2025. - 124 с. – Режим доступа: https://e.lanbook.com/book/462293
Л.1.3	Корецкий В. П. Информационная безопасность и защита информации [Электронный ресурс]:учебное пособие. - Москва: РТУ МИРЭА, 2025. - 479 с. – Режим доступа: https://e.lanbook.com/book/515271
Л.1.4	Медведев В.А. Информационная безопасность. Введение в специальность + еПриложение:Тесты [Электронный ресурс]:Учебник. - Москва: КноРус, 2024. - 143 с. – Режим доступа: https://book.ru/book/951878
Л.1.5	Медведев В.А. Информационная безопасность. Введение в специальность + еПриложение:Тесты [Электронный ресурс]:Учебник. - Москва: КноРус, 2024. - 143 с. – Режим доступа: https://book.ru/book/951878
Л.1.6	Раченко Т. А. Информационная безопасность [Электронный ресурс]:. - Тольятти: ТГУ, 2024. - 135 с. – Режим доступа: https://e.lanbook.com/book/427130
Л.1.7	Басаргин А. А. Информационная безопасность и защита информации : практикум [Электронный ресурс]:. - Новосибирск: СГУГиТ, 2024. - 80 с. – Режим доступа: https://e.lanbook.com/book/484910
7.2. Лицензионное и свободно распространяемое программное обеспечение в том числе отечественного производства	
7.2.1	Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition
7.2.2	Microsoft Windows 10 Pro
7.2.3	Microsoft Office 2013 Pro Plus
7.2.4	Microsoft Visual Studio Professional 2017
7.3. Перечень профессиональных баз данных, информационных справочных систем и ресурсов сети Интернет	
7.3.1	Электронно-библиотечная система "Лань". Режим доступа: https://e.lanbook.com/
7.3.2	Электронно-библиотечная система "Университетская библиотека онлайн". Режим доступа: https://biblioclub.ru/
7.3.3	Электронно-библиотечная система "BOOK.ru". Режим доступа: https://book.ru/
7.3.4	Электронно-библиотечная система "Университетская библиотека онлайн". Режим доступа: https://biblioclub.ru/
7.3.5	Электронно-библиотечная система "Лань". Режим доступа: https://e.lanbook.com/
7.3.6	ПЛАТФОРМА ОНЛАЙН-ОБРАЗОВАНИЯ «РАЗУМ». Режим доступа: https://razoom.mgutm.ru/

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

8.1	Адрес: 215119, Смоленская область, Вяземский район, город Вязьма, ул. Ленина, д. 77: аудитория 18-1310 - Лаборатория Учебная аудитория для проведения занятий лекционного типа; занятий семинарского типа, лабораторных и практических занятий; для курсового проектирования (выполнения курсовых работ); для проведения групповых и индивидуальных консультаций; для текущего контроля и промежуточной аттестации : Рабочие места обучающихся; Рабочее место преподавателя; Классная доска; 15 рабочих мест обучающихся оснащенные ПЭВМ с подключением к сети интернет и обеспечением доступа в электронную информационно-образовательную среду; Ноутбук переносной; Переносной проектор; Переносной экран; Учебно-наглядные пособия
8.2	Адрес: 215119, Смоленская область, Вяземский район, город Вязьма, ул. Ленина, д. 77: аудитория 18-1312 - Лаборатория Учебная аудитория для проведения занятий лекционного типа, лабораторных и практических занятий; занятий семинарского типа; для курсового проектирования (выполнения курсовых работ); для проведения групповых и индивидуальных консультаций; для текущего контроля и промежуточной аттестации : Рабочие места обучающихся; Рабочее место преподавателя; Маркерная доска; 15 рабочих мест обучающихся оснащенные ПЭВМ с подключением к сети интернет и обеспечением доступа в электронную информационно-образовательную среду; Учебно-наглядные пособия

9. ОРГАНИЗАЦИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Организация образовательного процесса для лиц с ограниченными возможностями здоровья осуществляется в соответствии с «Методическими рекомендациями по организации образовательного процесса для инвалидов и лиц с ограниченными возможностями здоровья в образовательных организациях высшего образования, в том числе

оснащенности образовательного процесса» Министерства образования и науки РФ от 08.04.2014г. № АК-44/05вн. В образовательном процессе используются социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений с другими студентами, создании комфортного психологического климата в студенческой группе. Студенты с ограниченными возможностями здоровья, в отличие от остальных студентов, имеют свои специфические особенности восприятия, переработки материала. Подбор и разработка учебных материалов производится с учетом индивидуальных особенностей. Предусмотрена возможность обучения по индивидуальному графику, при составлении которого возможны различные варианты проведения занятий: в академической группе и индивидуально, на дому с использованием дистанционных образовательных технологий.

Актуализация с учетом развития науки, техники, культуры, экономики, техники, технологий и социальной сферы
Руководитель ОПОП
_____

Рабочая программа актуализирована, обсуждена и одобрена на заседании обеспечивающей кафедры
Системной автоматизации и информационных технологий
Протокол от __ _____ 2027 г. № __
Зав. кафедрой Кузьмин Константин Анатольевич_____

Рабочая программа согласована на заседании выпускающей кафедры
Системной автоматизации и информационных технологий
Протокол от __ _____ 2027 г. № __
Зав. кафедрой Кузьмин Константин Анатольевич _____

==========

Актуализация с учетом развития науки, техники, культуры, экономики, техники, технологий и социальной сферы
Руководитель ОПОП
_____

Рабочая программа актуализирована, обсуждена и одобрена на заседании обеспечивающей кафедры
Системной автоматизации и информационных технологий
Протокол от __ _____ 2028 г. № __
Зав. кафедрой Кузьмин Константин Анатольевич_____

Рабочая программа согласована на заседании выпускающей кафедры
Системной автоматизации и информационных технологий
Протокол от __ _____ 2028 г. № __
Зав. кафедрой Кузьмин Константин Анатольевич _____

==========

Актуализация с учетом развития науки, техники, культуры, экономики, техники, технологий и социальной сферы
Руководитель ОПОП
_____

Рабочая программа актуализирована, обсуждена и одобрена на заседании обеспечивающей кафедры
Системной автоматизации и информационных технологий
Протокол от __ _____ 2029 г. № __
Зав. кафедрой Кузьмин Константин Анатольевич_____

Рабочая программа согласована на заседании выпускающей кафедры
Системной автоматизации и информационных технологий
Протокол от __ _____ 2029 г. № __
Зав. кафедрой Кузьмин Константин Анатольевич _____

==========

Актуализация с учетом развития науки, техники, культуры, экономики, техники, технологий и социальной сферы
Руководитель ОПОП
_____

Рабочая программа актуализирована, обсуждена и одобрена на заседании обеспечивающей кафедры
Системной автоматизации и информационных технологий
Протокол от __ _____ 2030 г. № __
Зав. кафедрой Кузьмин Константин Анатольевич_____

Рабочая программа согласована на заседании выпускающей кафедры
Системной автоматизации и информационных технологий
Протокол от __ _____ 2030 г. № __
Зав. кафедрой Кузьмин Константин Анатольевич _____

Приложение № 1

Задания к практическим работам

Практическая работа № 1

Тема: Настройка брандмауэра для защиты промышленной сети АСУ ТП

Цель работы

Приобрести практические навыки настройки брандмауэра операционной системы Windows для контроля входящего и исходящего трафика промышленных протоколов, применяемых в системах автоматизации технологических процессов и производств.

Студент должен уметь:

- создавать правила брандмауэра для разрешения и блокировки сетевого трафика по портам и протоколам;
- применять принцип «белого списка» (разрешено только явно указанное) к промышленным сетевым сервисам;
- экспортировать и документировать политику безопасности брандмауэра.

Программное обеспечение: Windows Defender Firewall with Advanced Security – встроен в Windows 10/11, установка не требуется.

Теоретическая часть

1. Место брандмауэра в системе защиты АСУ ТП

Инженер по автоматизации технологических процессов в своей профессиональной деятельности неизбежно сталкивается с задачами обеспечения информационной безопасности промышленных объектов. Это обусловлено тем, что современные АСУ ТП представляют собой сложные распределённые вычислительные системы, в которых программируемые логические контроллеры (ПЛК), серверы SCADA, автоматизированные рабочие места (АРМ) операторов и полевые устройства объединены в промышленную сеть Ethernet. Такая архитектура, обеспечивая высокую функциональность и удобство управления, одновременно создаёт потенциальные векторы кибератак, последствия которых в промышленной среде принципиально отличаются от инцидентов в корпоративных IT-системах: нарушение работы АСУ ТП может повлечь технологическую аварию, остановку производства или угрозу жизни персонала.

Брандмауэр (межсетевой экран, firewall) – это программный или аппаратно-программный комплекс, осуществляющий фильтрацию сетевого трафика на основе заранее сформулированных правил. По существу, брандмауэр реализует принцип **«контролируемого пропускного пункта»**: каждый сетевой пакет, входящий в систему

или исходящий из неё, сопоставляется с набором правил, и на основании этого сопоставления принимается решение – пропустить пакет или отбросить его.

В контексте защиты информации, рассмотренной на предыдущих лекциях, брандмауэр является инструментом обеспечения сразу двух принципов триады CIA. Во-первых, он обеспечивает **конфиденциальность**, не позволяя несанкционированным внешним субъектам получить доступ к промышленным сервисам и данным. Во-вторых, он обеспечивает **доступность**, защищая систему от атак типа «отказ в обслуживании» (DoS/DDoS), направленных на перегрузку и остановку сетевых служб.

2. Особенности сетевой архитектуры АСУ ТП и необходимость защиты по портам

Для понимания практики настройки брандмауэра необходимо усвоить, каким образом устройства в промышленной сети взаимодействуют между собой на транспортном уровне. Каждый промышленный протокол использует фиксированный **порт** – числовой идентификатор, позволяющий операционной системе определить, какому приложению адресован входящий пакет. Порты в диапазоне 0–1023 называются «хорошо известными» (well-known ports) и зарегистрированы за конкретными протоколами. Именно по номеру порта брандмауэр может различить, является ли входящий пакет легитимным Modbus-запросом от ПЛК или попыткой несанкционированного доступа.

Протокол	Стандартный порт	Уровень АСУ ТП	Применяемое оборудование
Modbus TCP	TCP 502	Полевой / Управления	ПЛК ОВЕН, Schneider Modicon, Siemens; датчики и исполнительные механизмы
OPC UA	TCP 4840	Управления / SCADA	Серверы OPC UA, SCADA-системы (MasterSCADA, Infinity, WinCC)
EtherNet/IP	TCP/UDP 44818	Управления	ПЛК Allen-Bradley (Rockwell Automation)
S7 (Siemens ISO-TSAP)	TCP 102	Управления	ПЛК Siemens серий S7-300/400/1200/1500
DNP3	TCP/UDP 20000	Управления / диспетчерский	Энергетические объекты, подстанции
RDP (удалённый рабочий стол)	TCP 3389	SCADA-сервер / АРМ	АРМ операторов, серверы с удалённым доступом

Таблица демонстрирует практическую значимость фильтрации по портам для инженера-автоматизатора. Если порт 502 (Modbus TCP) открыт на сервере SCADA и доступен из внешней сети или корпоративного сегмента – любой злоумышленник, подключившись к этому порту, получает возможность отправлять произвольные Modbus-команды напрямую к ПЛК, минуя все средства аутентификации. Именно через подобную незащищённость порта реализуется значительная часть атак на промышленные объекты.

3. Принцип «минимальных привилегий» применительно к сетевому доступу

Настройка брандмауэра для промышленной сети строится на основополагающем принципе информационной безопасности – принципе **минимальных привилегий** (Principle of Least Privilege). Применительно к сетевому доступу он формулируется следующим образом: каждому устройству или пользователю предоставляется только тот сетевой доступ, который необходим для выполнения его функций, – не более.

На практике этот принцип реализуется через два взаимодополняющих подхода. **Подход «чёрного списка»** (blacklisting) предполагает, что по умолчанию весь трафик разрешён, а запрещается только явно перечисленное – исторически это был распространённый подход, однако он ненадёжен, поскольку невозможно предусмотреть все потенциальные угрозы заранее. **Подход «белого списка»** (whitelisting) противоположен: по умолчанию весь трафик блокируется, а разрешается только то, что явно необходимо и перечислено в правилах. Международный стандарт кибербезопасности промышленных систем МЭК 62443 однозначно предписывает применение именно подхода «белого списка» для защиты промышленных сетей.

Таким образом, грамотно настроенный брандмауэр для сервера SCADA должен выглядеть следующим образом: **всё запрещено**, кроме явно разрешённых соединений – например, Modbus TCP (порт 502) только от ПЛК с IP-адресом 192.168.10.5, OPC UA (порт 4840) только от инженерной станции с IP-адресом 192.168.10.10, и так далее по каждому сервису.

4. Windows Defender Firewall with Advanced Security как инструмент практики

Windows Defender Firewall with Advanced Security (далее – WDFW) – встроенный в операционные системы Windows 10/11 и Windows Server брандмауэр с функциями фильтрации пакетов с отслеживанием состояния (stateful packet inspection). Термин «с отслеживанием состояния» означает, что брандмауэр анализирует не каждый пакет изолированно, а весь контекст TCP-сессии целиком: разрешив входящее соединение, он

автоматически пропускает ответные пакеты в обратном направлении, не требуя отдельного исходящего правила.

WDFW поддерживает три сетевых профиля, что имеет прямое значение для инженерной практики:

Профиль	Условие активации	Типичный сценарий применения
Доменный (Domain)	Компьютер входит в домен Active Directory	Корпоративная инфраструктура предприятия с централизованным управлением
Частный (Private)	Пользователь пометил сеть как «доверенную»	Локальная промышленная сеть цеха или диспетчерской
Публичный (Public)	Неизвестная или публичная сеть	Ноутбук инженера при подключении к внешним сетям

Возможность применять различные наборы правил для каждого профиля позволяет, например, разрешить подключение к Modbus-порту только в «Частном» профиле (промышленная сеть цеха), полностью закрыв его в «Публичном» профиле (при подключении к корпоративной или внешней сети). Это существенно снижает риск случайного открытия промышленных сервисов на всеобщий доступ.

Практическое задание: Настройка политики брандмауэра для сервера SCADA

Исходные условия

Вы – инженер по информационной безопасности условного нефтеперерабатывающего предприятия. Ваш рабочий компьютер моделирует **сервер SCADA**, к которому должны иметь доступ:

- **ПЛК цеха** с IP-адресом 192.168.1.10 – по протоколу Modbus TCP (порт 502);
- **Инженерная станция** с IP-адресом 192.168.1.20 – по протоколу OPC UA (порт 4840).

Все прочие подключения к промышленным портам должны быть **заблокированы**. Кроме того, порт удалённого рабочего стола (RDP, порт 3389) должен быть закрыт полностью – удалённое управление SCADA-сервером по RDP является грубой ошибкой конфигурации и прямым нарушением требований Приказа ФСТЭК России №31.

Шаг 1. Открытие консоли управления брандмауэром

Откройте консоль управления брандмауэром одним из способов:

- Win + R → введите wf.msc → Enter
- Поиск Windows → «Брандмауэр Windows в режиме повышенной безопасности»

Главное окно отображает текущий статус трёх профилей и сводку активных правил.

СКРИНШОТ 1 – вставить здесь: *главное окно консоли wf.msc. Должны быть видны три профиля (Доменный, Частный, Публичный) и их текущий статус (включён/выключен).*

Шаг 2. Аудит существующих правил

До начала любых изменений необходимо задокументировать исходное состояние – это стандартная процедура аудита конфигурации.

1. Откройте **командную строку от имени администратора** (Win + X → «Терминал Windows (администратор)»).
2. Выполните команду, которая экспортирует полный список правил в текстовый файл:

netsh advfirewall firewall show rule name=all > C:\audit_before.txt

3. Откройте файл C:\audit_before.txt в Блокноте и найдите количество строк Rule Name: – это количество существующих правил. Запишите это число в отчёт.
4. Дополнительно выполните команду, которая покажет, открыт ли сейчас порт RDP:

netsh advfirewall firewall show rule name=all | findstr /i "3389\|Remote Desktop"

Зафиксируйте в отчёте: присутствует ли разрешающее правило для порта 3389 в системе по умолчанию?

СКРИНШОТ 2 – вставить здесь: *вывод второй команды в окне терминала, показывающий найденные правила с упоминанием 3389 или Remote Desktop.*

Шаг 3. Блокировка порта RDP (3389)

Порт 3389 открыт в Windows по умолчанию. В условиях промышленного объекта это неприемлемо: подбор учётных данных через RDP является одним из наиболее распространённых способов первоначального проникновения в сеть АСУ ТП.

1. В левой панели консоли wf.msc нажмите правой кнопкой мыши на **«Правила для входящих подключений» → «Создать правило»**.
2. Тип правила: **«Порт»** → «Далее».
3. Протокол: **TCP**. Конкретные локальные порты: **3389** → «Далее».
4. Действие: **«Блокировать подключение»** → «Далее».
5. Профили: отметьте все три (**Доменный, Частный, Публичный**) → «Далее».

6. Имя правила: **SECURITY_BLOCK_RDP_3389**, описание: Блокировка RDP на сервере SCADA согласно требованиям ФСТЭК Приказ №31 → «Готово».

СКРИНШОТ 3 – вставить здесь: *диалог «Создать правило для входящего подключения», шаг «Протокол и порты» с заполненным полем «3389» и выбранным TCP.*

Шаг 4. Блокировка всех входящих подключений на промышленные порты

Согласно принципу «белого списка», сначала необходимо создать **запрещающие** правила для промышленных портов, а затем – разрешающие правила для конкретных источников. Это объясняется тем, что Windows обрабатывает правила в следующем порядке приоритетов: запрещающие правила имеют больший приоритет, кроме того, более специфичные правила (с указанием конкретного IP) применяются раньше общих. Поэтому корректная последовательность – сначала «запретить всем», затем «разрешить конкретным».

Создайте запрещающее правило для порта Modbus TCP:

1. Правой кнопкой → **«Создать правило»** → **«Порт»** → TCP → порт **502** → «Далее».
2. Действие: **«Блокировать подключение»** → «Далее».
3. Все профили → «Далее».
4. Имя: **SECURITY_BLOCK_Modbus502_ALL** → «Готово».

Создайте запрещающее правило для порта OPC UA самостоятельно, по аналогии с предыдущим пунктом:

- Порт: **4840**
- Имя: **SECURITY_BLOCK_OPCUA4840_ALL**

Шаг 5. Создание разрешающих правил «белого списка»

Теперь необходимо разрешить подключение к порту 502 только от ПЛК (192.168.1.10), а к порту 4840 – только от инженерной станции (192.168.1.20).

Разрешающее правило для ПЛК по Modbus TCP:

1. **«Создать правило»** → **«Порт»** → TCP → **502** → «Далее».
2. Действие: **«Разрешить подключение»** → «Далее».
3. Профили: только **«Частный»** (промышленная сеть является доверенной локальной сетью) → «Далее».
4. Имя: **SECURITY_ALLOW_Modbus502_PLC_192.168.1.10** → «Готово».

5. После создания **дважды кликните** по новому правилу, чтобы открыть его свойства.

6. Перейдите на вкладку **«Область»**.

7. В разделе **«Удалённые IP-адреса»** выберите «Указанные IP-адреса» → «Добавить» → введите 192.168.1.10 → ОК.

СКРИНШОТ 4 – вставить здесь: *вкладка «Область» созданного правила, в разделе «Удалённые IP-адреса» отображается адрес 192.168.1.10.*

Самостоятельно создайте разрешающее правило для OPC UA:

- Порт: **4840**
- Профиль: только **Частный**
- Разрешить только с IP: 192.168.1.20
- Имя: **SECURITY_ALLOW_OPCUA4840_ENG_192.168.1.20**

Шаг 6. Проверка созданной политики

6.1. Убедитесь, что все пять созданных правил присутствуют в консоли. В разделе «Правила для входящих подключений» отсортируйте список по столбцу «Имя» и найдите все правила с префиксом SECURITY_.

6.2. Выполните итоговую проверку через терминал:

```
netsh advfirewall firewall show rule name=all | findstr "SECURITY_"
```

В выводе должны присутствовать все пять правил: три блокирующих (BLOCK_RDP, BLOCK_Modbus502_ALL, BLOCK_OPCUA4840_ALL) и два разрешающих (ALLOW_Modbus502, ALLOW_OPCUA4840).

6.3. Экспортируйте итоговую конфигурацию для документирования:

```
netsh advfirewall firewall show rule name=all > C:\audit_after.txt
```

Откройте файл и подсчитайте, на сколько правил стало больше по сравнению с начальным состоянием из Шага 2.

СКРИНШОТ 5 – вставить здесь: *вывод команды проверки в терминале – все пять созданных правил с префиксом SECURITY_ в одном кадре.*

Содержание отчёта

Отчёт по практической работе должен содержать следующие разделы:

1. **О**тветы на контрольные вопросы (см. ниже).

2. **Ход выполнения работы** – описание каждого шага с вставленными скриншотами (5 скриншотов).

3. **Таблица созданных правил** – сводная таблица со столбцами: Имя правила | Порт | Протокол | Действие | Удалённый IP | Профиль.

4. **Вывод** – анализ результатов: как созданные правила реализуют принцип «белого списка» и принцип минимальных привилегий? Какие угрозы они нейтрализуют?

Контрольные вопросы

1. Объясните разницу между подходами «чёрного списка» и «белого списка» при настройке брандмауэра. Почему для АСУ ТП предпочтителен второй подход?

2. Почему открытый порт RDP (3389) на сервере SCADA является недопустимой конфигурацией безопасности?

3. Для чего необходимо создавать сначала запрещающее правило для всех IP, а затем разрешающее для конкретного IP, а не сразу одно разрешающее правило?

4. Какой профиль брандмауэра (Доменный, Частный, Публичный) следует использовать для правил, ограничивающих доступ к промышленному сегменту сети? Обоснуйте.

5. Какие порты, помимо рассмотренных в работе, следует закрыть на сервере SCADA? Обоснуйте свой ответ, опираясь на таблицу промышленных протоколов из теоретической части.

Практическая работа № 2

Защита операционных систем: настройка политик безопасности Windows

Теоретическая часть

1. Операционная система как объект защиты в АСУ ТП

Операционная система – это фундамент, на котором работает всё программное обеспечение промышленной системы: SCADA-сервер, OPC-сервер, historian, веб-интерфейс конфигуратора. Компрометация ОС означает компрометацию всего, что на ней работает, – независимо от того, насколько хорошо защищены сами промышленные приложения. Именно поэтому операционная система является первоочередным объектом атаки и первоочередным объектом защиты.

В АСУ ТП под управлением ОС Windows работают серверы SCADA (MasterSCADA, DevelSCADA, Wonderware), серверы историков (OSIsoft PI), рабочие станции операторов и инженеров. Согласно статистике компании Dragos, более 70% промышленных рабочих станций под управлением Windows содержат хотя бы одну критическую уязвимость, связанную с некорректной настройкой политик безопасности ОС – а не с уязвимостями самих промышленных приложений.

2. Поверхность атаки операционной системы

Прежде чем настраивать защиту, необходимо понять, через какие механизмы злоумышленник может атаковать операционную систему промышленной рабочей станции.

Слабые учётные данные – наиболее распространённый вектор. Если учётная запись пользователя имеет простой пароль (или вовсе пустой, как это нередко встречается на промышленных рабочих станциях «для удобства операторов»), злоумышленник, получивший доступ к сети, может подобрать его атакой по словарю за считанные минуты. Особую опасность представляет встроенная учётная запись `Administrator` с пустым или стандартным паролем – именно она является первоочередной целью автоматизированных атак.

Отсутствие блокировки после неудачных попыток входа – без ограничения числа попыток аутентификации атака перебором паролей ничем не сдерживается. Злоумышленник может автоматически перебирать тысячи паролей в секунду – особенно актуально для RDP-доступа (порт 3389), который, как было рассмотрено в Практической работе №1, нередко остаётся открытым.

Отсутствие аудита действий – без включённого журналирования событий безопасности ОС атака может быть проведена и завершена незаметно. Системный администратор не сможет ни обнаружить вторжение в реальном времени, ни восстановить хронологию событий после инцидента.

Избыточные права пользователей – оператор SCADA, работающий под учётной записью с правами администратора «для удобства», представляет двойную угрозу: во-первых, случайная или намеренная ошибка оператора может привести к деструктивным последствиям; во-вторых, если рабочая станция оператора заражена вредоносным ПО, оно получает права администратора автоматически.

3. Локальная политика безопасности Windows (Local Security Policy)

Windows предоставляет встроенный централизованный инструмент управления параметрами безопасности операционной системы – **Локальную политику безопасности** (Local Security Policy, secpol.msc). Этот инструмент позволяет настраивать три ключевые группы параметров, непосредственно влияющих на защиту рабочей станции АСУ ТП.

Политика паролей (Password Policy) определяет требования к паролям всех локальных учётных записей системы. Ключевые параметры: минимальная длина пароля, требования к сложности (обязательное наличие букв разного регистра, цифр, специальных символов), максимальный срок действия пароля, запрет повторного использования предыдущих паролей. Для рабочих станций АСУ ТП минимальная длина пароля не должна быть ниже 12 символов, а требования сложности – обязательно включены.

Политика блокировки учётных записей (Account Lockout Policy) – механизм автоматической блокировки учётной записи после заданного числа неудачных попыток входа. Три параметра работают в связке: **Порог блокировки** (Account Lockout Threshold) – число допустимых неудачных попыток; **Продолжительность блокировки** (Account Lockout Duration) – время, на которое блокируется учётная запись; **Счётчик блокировки** (Reset Account Lockout Counter After) – время, через которое счётчик неудачных попыток сбрасывается. Для промышленных рабочих станций рекомендуется порог блокировки 5 попыток с блокировкой на 30 минут.

Политика аудита (Audit Policy) определяет, какие события безопасности будут записываться в **Журнал безопасности Windows** (Windows Security Event Log). Ключевые категории: аудит входа в систему (Audit Logon Events) – фиксирует все попытки входа, успешные и неудачные; аудит управления учётными записями (Audit Account Management) – фиксирует создание, изменение и удаление учётных записей; аудит

изменения политик (Audit Policy Change) – фиксирует любые изменения самих политик безопасности.

4. Журнал безопасности Windows и идентификаторы событий

Журнал безопасности Windows (eventvwr.msc → Журналы Windows → Безопасность) содержит записи всех событий, для которых включён аудит. Каждое событие имеет уникальный **идентификатор (Event ID)**, позволяющий точно определить тип события:

Event ID	Событие	Значение для АСУ ТП
4624	Успешный вход в систему	Контроль легитимных сеансов работы
4625	Неудачная попытка входа	Признак атаки перебором или несанкционированного доступа
4740	Учётная запись заблокирована	Сработала политика блокировки – требует анализа
4720	Создана новая учётная запись	Возможное создание «backdoor»-аккаунта
4732	Пользователь добавлен в группу Администраторы	Критическое событие – несанкционированное повышение привилегий
4719	Изменена политика аудита	Возможное сокрытие следов вторжения

Умение читать журнал безопасности и правильно интерпретировать Event ID – обязательный навык инженера по безопасности АСУ ТП. Именно этот навык формируется в данной практической работе.

Практическое задание

Цель работы

Научиться настраивать политики безопасности операционной системы Windows применительно к рабочей станции АСУ ТП: сконфигурировать политику паролей, политику блокировки учётных записей и политику аудита, после чего проверить работу настроенных политик и проанализировать результаты в журнале безопасности.

Используемое программное обеспечение

- Операционная система **Windows 10/11** (любая редакция, кроме Home)
- Встроенная оснастка **secpol.msc** (Локальная политика безопасности)
- Встроенная оснастка **eventvwr.msc** (Просмотр событий)
- Встроенная утилита **net user** (командная строка, запущенная от имени администратора)

Примечание: на редакции Windows Home оснастка secpol.msc недоступна. В этом случае используйте учебную виртуальную машину с Windows 10 Pro.

Шаг 1. Создание тестовой учётной записи

Откройте командную строку от имени администратора (правая кнопка мыши на меню «Пуск» → «Терминал (администратор)» или «Windows PowerShell (администратор)») и выполните команду создания тестового пользователя:

```
net user SCADA_Operator_Test P@ssword1234 /add
```

Убедитесь, что учётная запись создана успешно – система должна вывести сообщение «Команда выполнена успешно».

Затем проверьте, что учётная запись существует:

```
net user SCADA_Operator_Test
```

В выводе команды обратите внимание на поля «Последний вход в систему» (пока что «Никогда»), «Счётчик неверных попыток входа» (0) и «Учётная запись активна» (Да). Сделайте **скриншот** вывода этой команды и подпишите его «Шаг 1 – Исходное состояние учётной записи».

Шаг 2. Настройка политик безопасности

Откройте оснастку Локальной политики безопасности: нажмите `Win + R`, введите `secpol.msc`, нажмите Enter.

2.1 Политика паролей

В левой панели разверните дерево: **Политики учётных записей → Политика паролей**.

Настройте параметры в соответствии с таблицей, дважды щёлкая по каждому параметру:

Параметр	Значение
Минимальная длина пароля	**12** символов
Пароль должен отвечать требованиям сложности	**Включён**
Максимальный срок действия пароля	**90** дней
Минимальный срок действия пароля	**1** день
Хранить историю паролей	**5** паролей

После настройки каждого параметра нажимайте «Применить» и «ОК». Сделайте **скриншот** окна «Политика паролей» с применёнными настройками и подпишите его «Шаг 2.1 – Политика паролей».

2.2 Политика блокировки учётных записей

В левой панели перейдите: **Политики учётных записей → Политика блокировки учётной записи**.

Настройте параметры:

Параметр	Значение
Порог блокировки учётной записи	**5** ошибок входа
Продолжительность блокировки учётной записи	**30** минут
Сброс счётчика блокировки через	**15** минут

Обратите внимание: после установки порога блокировки Windows автоматически предложит установить рекомендуемые значения для двух оставшихся параметров. Примите их, затем скорректируйте в соответствии с таблицей.

Сделайте **скриншот** окна «Политика блокировки учётной записи» и подпишите его «Шаг 2.2 – Политика блокировки».

2.3 Политика аудита

В левой панели перейдите: **Локальные политики → Политика аудита**.

Настройте параметры:

Параметр	Значение
Аудит входа в систему	**Успех, Отказ**
Аудит управления учётными записями	**Успех, Отказ**
Аудит изменения политики	**Успех**
Аудит использования привилегий	**Отказ**

Сделайте **скриншот** окна «Политика аудита» и подпишите его «Шаг 2.3 – Политика аудита».

Шаг 3. Проверка работы политики блокировки

Теперь смоделируем атаку перебором пароля – многократный неудачный ввод пароля для учётной записи SCADA_Operator_Test – и убедимся, что политика блокировки срабатывает корректно.

В командной строке (от имени администратора) выполните следующую команду **6 раз подряд**, каждый раз вводя заведомо неверный пароль wrongpassword:

```
runas /user:SCADA_Operator_Test cmd
```

После запроса пароля вводите wrongpassword и нажимайте Enter. Система откажет в доступе. Повторите 6 раз.

После шестой попытки выполните команду проверки состояния учётной записи:

```
net user SCADA_Operator_Test
```

В выводе найдите поле **«Учётная запись заблокирована»** – оно должно принять значение **«Да»**. Также обратите внимание на поле «Счётчик неверных попыток входа».

Сделайте **скриншот** вывода команды с заблокированной учётной записью и подпишите его «Шаг 3 – Учётная запись заблокирована».

Разблокируйте учётную запись вручную для дальнейшей работы:

```
net user SCADA_Operator_Test /active:yes
```

Шаг 4. Анализ журнала безопасности

Откройте оснастку просмотра событий: нажмите Win + R, введите eventvwr.msc, нажмите Enter.

В левой панели разверните: **Журналы Windows → Безопасность**.

Вы увидите список событий безопасности. Для удобства поиска нажмите **«Фильтровать текущий журнал»** (правая панель) и в поле **«Коды событий»** введите:

```
4625, 4740
```

Нажмите ОК. Журнал отфильтрует только интересующие нас события – неудачные попытки входа (4625) и блокировку учётной записи (4740).

Найдите событие с кодом **4740** («Учётная запись заблокирована») и дважды щёлкните по нему для открытия подробного описания. В тексте события найдите и запишите в отчёт следующую информацию:

- **Имя учётной записи** – какая учётная запись была заблокирована;
- **Вызвано учётной записью** – от имени какой учётной записи выполнялись попытки входа;
- **Имя компьютера-источника** – с какого узла зафиксированы попытки входа;
- **Дата и время** события.

Сделайте **скриншот** открытого события 4740 с читаемыми деталями и подпишите его «Шаг 4 – Событие блокировки в журнале».

Затем снимите фильтр (правая панель → «Очистить фильтр») и найдите событие с кодом **4719** – это должно быть событие изменения политики аудита, которое было зафиксировано на Шаге 2.3. Найдите его, откройте и запишите время события.

Сделайте **скриншот** события 4719 и подпишите его «Шаг 4 – Событие изменения политики аудита».

Шаг 5. Уборка – удаление тестовой учётной записи

По завершении работы обязательно удалите тестовую учётную запись:

```
net user SCADA_Operator_Test /delete
```

Убедитесь, что учётная запись удалена:

```
net user
```

В списке пользователей учётная запись SCADA_Operator_Test должна отсутствовать.

Сделайте **скриншот** списка пользователей и подпишите его «Шаг 5 – Учётная запись удалена».

Содержание отчёта

Отчёт оформляется в текстовом редакторе (MS Word) и должен содержать следующие разделы:

1. Таблица настроенных политик – сводная таблица всех настроенных параметров (политика паролей, блокировки, аудита) с указанием установленных значений и обоснованием каждого значения применительно к защите рабочей станции АСУ ТП.

2. Скриншоты выполненных шагов – все 7 скриншотов в порядке выполнения, каждый с подписью.

3. Анализ событий журнала безопасности – таблица с найденными событиями:

Event ID	Описание события	Дата и время	Имя учётной записи	Компьютер-источник
4740				
4719				

4. Ответы на контрольные вопросы (см. ниже).

5. Вывод – 3–5 предложений о том, какие угрозы безопасности рабочей станции АСУ ТП нейтрализуют настроенные политики и почему аудит событий является обязательным элементом системы защиты.

Контрольные вопросы

1. Объясните разницу между политикой паролей и политикой блокировки учётных записей. Какую конкретную атаку предотвращает каждая из них?
2. Почему значение «Продолжительность блокировки учётной записи» не следует устанавливать равным нулю (что означает блокировку до ручного вмешательства администратора) для рабочей станции оператора АСУ ТП?
3. Какую угрозу выявляет серия событий Event ID 4625 с одним и тем же именем учётной записи в журнале безопасности за короткий промежуток времени?
4. Почему аудит должен фиксировать не только «Отказ», но и «Успех» для события «Вход в систему»?
5. Какое событие в журнале безопасности должно немедленно привлечь внимание администратора АСУ ТП – Event ID 4732 или 4625? Аргументируйте ответ.

Практическая работа № 3

Перехват и анализ безопасности мобильных приложений

Используемое программное обеспечение

Инструмент	Описание	Лицензия	Ссылка
jadx-gui	Декомпилятор APK с графическим интерфейсом	Apache 2.0 – полностью бесплатно	github.com/skylot/jadx/releases
DIVA.apk	Намеренно уязвимое Android-приложение для обучения	Открытый исходный код	github.com/payatu/diva-android

Установка не требуется. jadx-gui распространяется в виде ZIP-архива – достаточно распаковать и запустить файл jadx-gui.bat (Windows) или jadx-gui (Linux/macOS). JDK 11+ должен быть установлен в системе – он входит в стандартную поставку большинства учебных рабочих мест. Либо скачайте и установите с сайта Oracle https://www.oracle.com/java/technologies/downloads/

Теоретическая часть

1. Мобильные приложения в промышленной среде и зачем их анализировать

Современные промышленные предприятия активно используют мобильные приложения для мониторинга и управления технологическими процессами. Мобильный клиент SCADA-системы на планшете обходчика, приложение для просмотра архивных трендов на смартфоне главного технолога, утилита конфигурирования ПЛК через Bluetooth – всё это реальная и повсеместная практика.

Разработчики таких приложений нередко допускают типовые ошибки безопасности, которые превращают мобильное приложение в уязвимое звено системы защиты АСУ ТП. Ключевая особенность этих ошибок состоит в том, что они **обнаруживаются не в процессе работы приложения, а путём его анализа** – исследования кода, ресурсов и конфигурации, скрытых внутри установочного файла. Именно такой анализ называется **статическим** и является темой настоящей практической работы.

Android-приложение распространяется в виде файла с расширением **.APK (Android Package Kit)**. Несмотря на то что APK-файл внешне выглядит как единый бинарный объект, по своей структуре он представляет собой ZIP-архив, содержащий скомпилированный Java-байткод, ресурсы приложения, изображения, XML-файлы конфигурации и, что особенно важно для нас, **файл манифеста** с полным описанием структуры и разрешений приложения. Инструмент **jadx** позволяет «раскрыть» этот архив и декомпилировать байткод обратно в читаемый Java-код – фактически восстановив

исходный код приложения с достаточной точностью для анализа.

2. Статический анализ как метод выявления уязвимостей

Статический анализ – это исследование приложения **без его запуска**, путём изучения кода и конфигурации. В контексте безопасности мобильных приложений он позволяет обнаруживать уязвимости, которые разработчик «зашил» в само приложение и которые остаются в нём независимо от того, где и как оно запускается.

Это принципиально отличает статический анализ от **динамического**, при котором приложение запускается на реальном устройстве или эмуляторе и его поведение наблюдается в реальном времени – перехватывается сетевой трафик, отслеживаются обращения к файловой системе. Динамический анализ требует значительно более сложной инфраструктуры; статический же анализ требует только исходного APK-файла и декомпилятора.

3. Четыре класса уязвимостей, обнаруживаемых статическим анализом

Жёстко закодированные секреты (Hardcoded Secrets) – пароли, API-ключи, токены аутентификации, IP-адреса серверов, напрямую вписанные в исходный код или ресурсные файлы приложения. Разработчики поступают так из соображений удобства – «чтобы не усложнять». Последствия для промышленной системы могут быть катастрофическими: злоумышленник, извлёкший APK с планшета обходчика (или просто скачавший приложение), получает готовые учётные данные для подключения к SCADA-серверу или OPC UA-серверу предприятия.

Небезопасное хранение данных (Insecure Data Storage) – сохранение конфиденциальных данных в незашифрованном виде: в файлах SharedPreferences (стандартное хранилище настроек Android), в текстовых файлах на SD-карте, в базе данных SQLite без шифрования. Если приложение сохраняет учётные данные в SharedPreferences «для удобства автоматического входа», любое другое приложение на устройстве с root-доступом может их прочитать.

Избыточные разрешения (Overprivileged Permissions) – приложение запрашивает у операционной системы Android значительно больше разрешений, чем требуется для его функций. Промышленное приложение для просмотра трендов не имеет никаких оснований запрашивать доступ к камере, микрофону, геолокации или списку контактов. Наличие таких разрешений может свидетельствовать либо о небрежности разработчика, либо о наличии нежелательного функционала.

Небезопасная передача данных (Insecure Communication) – код приложения

содержит явные HTTP-адреса вместо HTTPS, отключённую проверку SSL-сертификатов (TrustAllCerts, HostnameVerifier возвращающий true для всех хостов) или отключённый Network Security Config. В промышленном контексте это означает, что трафик между мобильным приложением и SCADA-сервером может быть перехвачен любым устройством в той же сети без каких-либо специальных инструментов.

4. OWASP Mobile Top 10 и их связь с АСУ ТП

Организация OWASP, уже знакомая нам по OWASP Top 10 для веб-приложений, публикует аналогичный список для мобильных приложений – **OWASP Mobile Top 10**. Три из десяти позиций непосредственно связаны с уязвимостями, обнаруживаемыми статическим анализом:

Позиция **M1 (Improper Credential Usage)** – именно жёстко закодированные учётные данные. Для промышленных мобильных приложений это наиболее критичная уязвимость: обнаруженный в коде пароль от SCADA-сервера немедленно открывает злоумышленнику доступ к управлению технологическим процессом.

Позиция **M2 (Inadequate Supply Chain Security)** – приложение содержит устаревшие сторонние библиотеки с известными уязвимостями (аналог OWASP A06 для веб-приложений). Статический анализ позволяет выявить версии используемых библиотек и сверить их с базой CVE.

Позиция **M9 (Insecure Data Storage)** – незашифрованное хранение конфиденциальных данных, непосредственно обнаруживаемое в исходном коде при декомпиляции APK.

5. Инструмент: jadx и что он умеет

jadx – открытый декомпилятор Android-приложений, разрабатываемый сообществом с 2013 года. В отличие от ранних инструментов, требовавших цепочки из нескольких утилит (apktool → dex2jar → JAD), jadx выполняет полный цикл декомпиляции в одном шаге и предоставляет удобный графический интерфейс **jadx-gui**.

После открытия APK-файла jadx предоставляет три основных представления. **Исходный код** – дерево пакетов и классов с декомпилированным Java-кодом, допускающим поиск по всему проекту. **Ресурсы** – все ресурсные файлы приложения: XML-разметки экранов, строковые ресурсы, файлы конфигурации. **AndroidManifest.xml** – главный файл манифеста приложения в читаемом XML-формате.

Именно функция **полнотекстового поиска** по всему декомпилированному коду (Text search, сочетание клавиш Ctrl+Shift+F) является главным инструментом

обнаружения hardcoded secrets: поиск по ключевым словам password, passwd, secret, token, api_key, 192.168, http:// позволяет за минуты выявить то, что разработчик намеренно или случайно оставил в коде.

Практическое задание

Цель работы

Освоить метод статического анализа Android-приложений для выявления уязвимостей безопасности: научиться обнаруживать жёстко закодированные секреты, небезопасное хранение данных и избыточные разрешения в APK-файле промышленного назначения на примере учебного уязвимого приложения DIVA.

Шаг 1. Подготовка инструментария

Откройте браузер и перейдите по адресу github.com/skylot/jadx/releases. Найдите последний релиз (Latest release) и скачайте архив с именем вида jadx-X.X.X.zip. Распакуйте архив в удобное место – например, C:\Tools\jadx\.

Перейдите в папку bin внутри распакованного архива и запустите файл jadx-gui.bat (Windows). Откроется главное окно jadx с пустым рабочим пространством.

Параллельно перейдите по адресу github.com/payatu/diva-android и скачайте файл diva-beta.apk по ссылке в описании репозитория (кнопка «Download» или прямая ссылка на файл в разделе releases). Сохраните файл в доступном месте, например C:\Tools\diva-beta.apk.

Сделайте **скриншот** запущенного окна jadx-gui и подпишите его «Шаг 1 – jadx-gui запущен».

Шаг 2. Открытие APK и изучение структуры

В главном окне jadx-gui нажмите **File → Open files** и откройте скачанный файл diva-beta.apk. Инструмент выполнит декомпиляцию – это займёт 10–20 секунд. После завершения в левой панели появится дерево проекта.

Разверните дерево проекта. Вы увидите несколько разделов. Раздел **Source code** содержит декомпилированный Java-код приложения, организованный по пакетам. Раздел **Resources** содержит все ресурсные файлы. Файл **AndroidManifest.xml** расположен непосредственно в корне дерева – найдите его и откройте двойным щелчком.

Изучите содержимое манифеста. Найдите секцию <uses-permission> – список всех разрешений, которые приложение запрашивает у операционной системы. Выпишите в таблицу отчёта все найденные разрешения и для каждого укажите: является ли оно обоснованным для учебного приложения или избыточным. Обратите особое внимание на

разрешения класса DANGEROUS по классификации Android – они требуют явного подтверждения пользователя и несут наибольший риск.

Кроме разрешений, обратите внимание на атрибут android:debuggable в теге <application>. Если он установлен в значение true – это критическая уязвимость для производственного приложения: режим отладки открывает возможность подключения отладчика к работающему приложению и извлечения данных из его памяти в реальном времени.

Сделайте **скриншот** открытого файла AndroidManifest.xml с видимыми разрешениями и подпишите его «Шаг 2 – AndroidManifest.xml».

Шаг 3. Поиск жёстко закодированных секретов

Откройте функцию полнотекстового поиска сочетанием клавиш Ctrl+Shift+F. В появившемся окне поиска последовательно выполните поиск по следующим ключевым словам и записывайте все найденные совпадения в таблицу отчёта:

Сначала выполните поиск по слову password. Для каждого найденного совпадения дважды щёлкните по строке результата – откроется соответствующий фрагмент кода. Проанализируйте контекст: это просто название переменной или поля, или же переменной присвоено конкретное строковое значение? Если присвоено конкретное значение – зафиксируйте его в отчёте как обнаруженный hardcoded secret.

Затем выполните поиск по слову secret и аналогично зафиксируйте все значимые находки.

Далее выполните поиск по фрагменту http:// – это позволит обнаружить незашифрованные HTTP-адреса серверов, жёстко прописанные в коде. В промышленном контексте такие адреса означают, что трафик между приложением и сервером передаётся в открытом виде и может быть перехвачен в сети предприятия без каких-либо специальных инструментов.

Наконец, выполните поиск по слову SharedPreferences. Найдите место в коде, где данные записываются в SharedPreferences – обратите внимание, применяется ли при записи какое-либо шифрование (вы увидите вызовы криптографических функций) или данные записываются в открытом виде методами putString, putInt напрямую.

Для каждого найденного секрета или уязвимого паттерна сделайте **скриншот** соответствующего фрагмента кода. Всего должно быть не менее трёх скриншотов – по одному на каждый обнаруженный тип уязвимости.

Шаг 4. Анализ класса с жёстко закодированными учётными данными

В левой панели разверните раздел **Source code**, затем пакет jakhar.asher.diva. Найдите и откройте класс HardCodeActivity. Этот класс реализует экран приложения, демонстрирующий уязвимость hardcoded credentials.

Внимательно прочитайте декомпилированный код этого класса. Найдите строку, в которой выполняется сравнение введённого пользователем значения с жёстко закодированным в коде. Ответьте на следующие вопросы и запишите ответы в отчёт.

Каково жёстко закодированное значение, с которым сравнивается ввод пользователя? Представьте, что это – пароль для подключения мобильного клиента к OPC UA-серверу промышленного предприятия. Какие действия злоумышленник может предпринять, получив это значение из APK? Каким образом разработчику следовало реализовать проверку, чтобы избежать этой уязвимости?

Сделайте **скриншот** открытого класса HardCodeActivity с видимым уязвимым кодом и подпишите его «Шаг 4 – Hardcoded credentials в HardCodeActivity».

Шаг 5. Анализ класса с небезопасным хранением данных

В том же пакете найдите и откройте класс InsecureDataStorage1Activity. Этот класс демонстрирует уязвимость небезопасного хранения – сохранение чувствительных данных в SharedPreferences без шифрования.

Найдите в коде строку, реализующую запись данных. Обратите внимание на следующее: какой режим доступа передаётся в метод getSharedPreferences – MODE_PRIVATE или MODE_WORLD_READABLE? Режим MODE_WORLD_READABLE означает, что файл с сохранёнными данными доступен для чтения любому приложению на устройстве – это означало бы критическую уязвимость даже без root-доступа. Хотя в современных версиях Android этот режим уже не работает, его присутствие в коде свидетельствует о том, что приложение разрабатывалось без учёта требований безопасности.

Какие конкретно данные сохраняются в SharedPreferences и под какими ключами? Если бы это было приложение для мониторинга АСУ ТП, сохраняющее таким образом учётные данные оператора, какие последствия это могло бы иметь?

Сделайте **скриншот** открытого класса с видимым кодом записи в SharedPreferences и подпишите его «Шаг 5 – Небезопасное хранение данных».

Содержание отчёта

Отчёт оформляется в MS Word и должен содержать следующие разделы.

1. Таблица разрешений приложения – результаты анализа AndroidManifest.xml:

Разрешение	Категория (Normal/Dangerous)	Обосновано для приложения АСУ ТП?	Комментарий

2. Таблица обнаруженных уязвимостей – сводная таблица всех найденных проблем:

№	Тип уязвимости	Класс/файл	Обнаруженное значение или паттерн	Потенциальные последствия для АСУ ТП
1	Hardcoded credential	HardCodeActivity		
2	Insecure data storage	InsecureDataStorage1Activity		
3	Cleartext HTTP			

3. Скриншоты – все скриншоты (не менее 6) в порядке выполнения шагов, каждый с подписью.

4. Ответы на контрольные вопросы (см. ниже).

5. Вывод – 3–5 предложений о том, почему статический анализ APK является обязательной процедурой перед внедрением мобильного приложения в состав АСУ ТП, и какие организационные меры должны сопровождать эту процедуру.

Контрольные вопросы

1. Почему жёстко закодированный пароль в APK-файле промышленного мобильного приложения является более критичной уязвимостью, чем тот же пароль, сохранённый в незашифрованном файле конфигурации на сервере SCADA?

2. Объясните разницу между режимами `MODE_PRIVATE` и `MODE_WORLD_READABLE` при сохранении данных в SharedPreferences. Почему даже `MODE_PRIVATE` является недостаточным для хранения паролей подключения к OPC UA-серверу?

3. Атрибут `android:debuggable="true"` в манифесте приложения является критической уязвимостью для производственной среды. Какие конкретные возможности открывает злоумышленнику этот режим?

4. Разработчик промышленного мобильного приложения возражает: «Мы раздаём APK только проверенным сотрудникам, посторонние его не получат – значит, анализ APK невозможен». Приведите два контраргумента.

5. Какое разрешение Android из найденных в манифесте DIVA является наиболее опасным для корпоративного устройства, используемого на промышленном

предприятии? Обоснуйте ответ.

Задания к лабораторным работам

Лабораторная работа № 1

Тема: Анализ сетевого трафика и обнаружение аномальной активности

Цель работы

Сформировать практические навыки захвата и анализа сетевого трафика с использованием программного анализатора протоколов Wireshark, а также научиться применять фильтры для выявления аномальной сетевой активности, характерной для атак на промышленные системы автоматизации.

Студент должен уметь:

- захватывать трафик на сетевом интерфейсе и читать структуру сетевых пакетов;
- применять фильтры отображения для выделения трафика конкретных протоколов и хостов;
- отличать нормальный сетевой трафик от аномального по характерным признакам;
- настраивать фильтры захвата для регистрации потенциально опасной активности.

Программное обеспечение: Wireshark – свободное программное обеспечение с открытым исходным кодом (лицензия GNU GPL), скачивается бесплатно по адресу wireshark.org/download.html.

Теоретическая часть

1. Зачем инженеру-автоматизатору уметь читать сетевой трафик

Инженер по автоматизации технологических процессов проектирует, вводит в эксплуатацию и обслуживает системы, в которых программируемые логические контроллеры, серверы SCADA, панели операторов и полевые приборы непрерывно обмениваются данными по промышленной сети. Именно этот обмен – основа работы всей АСУ ТП, и именно он является объектом атак.

На практике, когда в работе промышленной сети возникает нештатная ситуация – будь то подозрение на несанкционированное подключение, необъяснимые задержки опроса ПЛК или неожиданная перегрузка канала связи – первым инструментом диагностики, к которому обращается обслуживающий инженер, является **анализатор сетевого трафика**. Он позволяет буквально «увидеть» всё, что происходит в сети: кто с кем общается, по какому протоколу, с какой частотой и каким объёмом данных. Без этого

навыка инженер вынужден действовать вслепую: он знает, что система ведёт себя неправильно, но не может установить причину.

Помимо диагностики неисправностей, анализ трафика является ключевым инструментом **обнаружения кибератак** на АСУ ТП. Международный стандарт кибербезопасности промышленных систем МЭК 62443 прямо предписывает наличие на объекте средств мониторинга сетевых событий как обязательного элемента защиты. Умение использовать эти средства, интерпретировать их результаты и отличать нормальный трафик от аномального – практическая компетенция, которая входит в профессиональные обязанности инженера, обслуживающего АСУ ТП.

2. Структура сетевого пакета и модель OSI

Чтобы грамотно читать трафик, необходимо понимать, как устроен сетевой пакет. В соответствии с моделью OSI каждый уровень добавляет к данным собственный заголовок. В итоге одна прикладная команда – например, запрос на считывание регистра ПЛК по протоколу Modbus – «упаковывается» в несколько вложенных оболочек:

Уровень OSI	Заголовок	Что содержит	Пример для Modbus TCP
2 – Канальный	Ethernet II	MAC-адреса источника и назначения	MAC-адрес ПЛК и MAC-адрес сервера SCADA
3 – Сетевой	IPv4	IP-адреса источника и назначения	192.168.1.10 → 192.168.1.100
4 – Транспортный	TCP	Порты, флаги, номера последовательности	Порт 502 (стандартный порт Modbus)
7 – Прикладной	Modbus	Код функции, адрес регистра, данные	Функция 03h: чтение регистров удержания

Именно эту структуру Wireshark «разбирает» и отображает послойно, позволяя инженеру увидеть содержимое каждого уровня. Анализ трафика должен охватывать все уровни: IP-адреса (уровень 3) показывают, кто с кем общается; флаги TCP (уровень 4) – характер соединения; прикладные данные – конкретные команды управления.

3. Нормальный трафик и признаки аномалий

Нормальный трафик промышленной сети обладает характерными признаками: он **периодичен** (опрос датчиков выполняется с постоянным интервалом), **источники фиксированы** (конкретные IP-адреса известных устройств), **интенсивность стабильна** (резких скачков объёма нет).

Любое отклонение от этой нормы – повод для проверки. Наиболее характерные типы аномалий в промышленных сетях:

Тип аномалии	Признаки в трафике	Что означает
Сканирование портов	Серия TCP SYN-пакетов с одного IP на разные порты за короткое время	Разведка сети – кто-то выясняет, какие сервисы доступны
Нетипичный источник	Запросы на промышленные порты (502, 4840) с неизвестного IP	Несанкционированное устройство в сети
Аномальная интенсивность	Резкое возрастание числа запросов от одного источника	Попытка перегрузки ПЛК или сервера SCADA
ARP-спуфинг	Одному IP соответствуют разные MAC-адреса в разное время	Попытка перехвата трафика (атака Man-in-the-Middle)

4. Два типа фильтров Wireshark

Wireshark предоставляет два принципиально разных типа фильтров, которые важно не путать:

Фильтры захвата (Capture Filters) задаются **до** начала захвата и определяют, какие пакеты вообще записываются в память. Всё, что не соответствует фильтру, отбрасывается немедленно и безвозвратно. Синтаксис – BPF (Berkeley Packet Filter). Применяются для снижения нагрузки при работе на загруженных промышленных сетях, где за секунду проходят тысячи пакетов.

Фильтры отображения (Display Filters) применяются **после** захвата и лишь скрывают ненужные пакеты из отображения – сами пакеты остаются в файле захвата. Написаны в собственном синтаксисе Wireshark, значительно богаче и гибче BPF. Применяются при анализе уже захваченного трафика для поиска конкретных событий.

Практическое задание

Исходные условия

В ходе работы вы выступаете в роли **инженера-технолога**, обслуживающего АСУ ТП на условном производственном объекте. Поступила информация о нештатном поведении сети – периодических задержках опроса ПЛК и появлении неизвестных пакетов на коммутаторе. Ваша задача – освоить инструмент анализа трафика, изучить структуру пакетов вашей рабочей станции и научиться распознавать признаки аномальной активности.

Шаг 1. Установка Wireshark и первый запуск

Скачайте Wireshark с официального сайта wireshark.org/download.html – выберите **«Windows x64 Installer»** актуальной стабильной версии. При установке оставьте все

компоненты по умолчанию. Особенно важен компонент **Npcap** – это драйвер захвата пакетов; без него Wireshark не сможет перехватывать трафик. Убедитесь, что при установке Npcap отмечена галочка **«Support loopback traffic»** – она понадобится в Шаге 4.

После запуска Wireshark отображает список доступных сетевых интерфейсов с мини-графиком активности рядом с каждым. Интерфейс с движущейся линией – активный, через него идёт трафик. Для Шагов 2–3 и 5 используйте **Ethernet** или **Wi-Fi** – тот, через который ваш компьютер подключён к сети.

СКРИНШОТ 1 – вставить здесь: *стартовое окно Wireshark со списком сетевых интерфейсов. Должны быть видны минимум один активный интерфейс (Ethernet или Wi-Fi) с движущимся графиком, а также адаптер «Adapter for loopback traffic capture».*

Как получить: *запустите Wireshark и сделайте скриншот инструментом «Ножницы» (Win + Shift + S), не начиная захват.*

Шаг 2. Узнайте адрес вашего сетевого шлюза

Прежде чем начинать захват, выполните подготовительный шаг – узнайте IP-адрес шлюза по умолчанию вашей сети. Он понадобится в Шагах 3 и 5 для генерации тестового трафика внутри локальной сети.

Откройте **командную строку** (Win + R → cmd → Enter) и выполните:

ipconfig

Найдите строку **«Основной шлюз» (Default Gateway)** для вашего активного адаптера. Запишите этот адрес – например, 192.168.1.1. Далее по тексту этот адрес обозначается как **[ШЛЮЗ]** – подставляйте своё значение везде, где встречается эта метка.

Шаг 3. Захват трафика и изучение структуры пакетов

3.1. На стартовом экране Wireshark дважды кликните по интерфейсу **Ethernet** или **Wi-Fi** – начнётся захват. Список пакетов начнёт заполняться.

3.2. Сгенерируйте разнообразный трафик: откройте браузер и перейдите на 2–3 сайта. Затем в командной строке выполните:

ping [ШЛЮЗ] -n 5

nslookup ya.ru

(пример: ping 192.168.1.1 -n 5)

Команда ping к шлюзу выбрана намеренно: шлюз всегда доступен внутри локальной сети независимо от политик безопасности предприятия, поэтому ICMP-ответы гарантированно придут.

3.3. Через 30 секунд нажмите **красный квадрат** на панели инструментов – захват остановлен.

3.4. В списке пакетов найдите строку, у которой в столбце **«Protocol»** написано **TCP**. Кликните на неё.

Важно: выбирайте именно TCP-пакет, а не DNS, ICMP или UDP – иначе в дереве разбора не будет раздела с флагами TCP и заполнить таблицу ниже не получится. Если TCP-пакетов не видно – откройте браузер, перейдите на любой сайт, новые пакеты появятся в конце списка.

В средней панели **«Дерево разбора»** последовательно раскройте все узлы и заполните таблицу в отчёте:

Поле пакета	Уровень OSI	Где найти в Wireshark	Ваше значение
MAC-адрес источника	Канальный (L2)	Ethernet II → Source	
MAC-адрес назначения	Канальный (L2)	Ethernet II → Destination	
IP-адрес источника	Сетевой (L3)	Internet Protocol → Source Address	
IP-адрес назначения	Сетевой (L3)	Internet Protocol → Destination Address	
Порт источника	Транспортный (L4)	Transmission Control Protocol → Source Port	
Порт назначения	Транспортный (L4)	Transmission Control Protocol → Destination Port	
Флаги TCP	Транспортный (L4)	Transmission Control Protocol → Flags	

СКРИНШОТ 2 – вставить здесь: *окно Wireshark с выбранным TCP-пакетом. В средней панели должны быть раскрыты все уровни: Ethernet II, Internet Protocol, Transmission Control Protocol – с видимыми значениями полей.*

Шаг 4. Применение фильтров отображения

Введите каждый фильтр в строку фильтрации (поле над списком пакетов) и нажмите **Enter**. Строка подсвечивается **зелёным** – синтаксис верен, **красным** – ошибка в написании. Для перехода к следующему фильтру просто сотрите предыдущий и введите новый, либо нажмите кнопку «×» справа от строки фильтра, чтобы сбросить его.

Фильтр 1 – только DNS-запросы:

dns

DNS – это «телефонная книга» интернета: прежде чем подключиться к любому сайту или серверу, компьютер сначала запрашивает его IP-адрес у DNS-сервера. Для инженера АСУ ТП необычные DNS-запросы с промышленной рабочей станции – возможный признак вредоносного ПО, пытающегося связаться с командным сервером.

Запишите в отчёт: на какой IP-адрес уходят DNS-запросы с вашего компьютера? Какие доменные имена были запрошены?

Фильтр 2 – пакеты ping (ICMP):

icmp

Найдите пакеты, соответствующие ранее выполненной команде ping [ШЛЮЗ]. Вы увидите пары: Echo (ping) request – запрос от вас к шлюзу, и Echo (ping) reply – ответ шлюза.

Запишите в отчёт: сколько пар запрос/ответ присутствует? Чему равно значение поля **TTL** в ответных пакетах (найдёте в разделе Internet Protocol → Time to Live)?

Фильтр 3 – все попытки установки TCP-соединений:

tcp.flags.syn == 1 && tcp.flags.ack == 0

Этот фильтр показывает только первые пакеты TCP-рукопожатия – те, которыми клиент инициирует соединение с сервером. В нормальной работе таких пакетов немного, и они направлены на известные адреса.

Запишите в отчёт: сколько SYN-пакетов было отправлено за время захвата? На какие порты назначения?

Фильтр 4 – контрольная проверка промышленных портов:

tcp.port == 502 || tcp.port == 4840

Этот фильтр показывает весь Modbus TCP (порт 502) и OPC UA (порт 4840) трафик. На учебной рабочей станции, не подключённой к реальным ПЛК, результат будет пустым – и это **правильно**. Если же трафик на этих портах есть – это немедленный повод для расследования: откуда он берётся?

Запишите в отчёт: есть ли трафик на промышленных портах? Если да – с каких IP-адресов?

СКРИНШОТ 3 – вставить здесь: *окно Wireshark с применённым фильтром tcp.flags.syn == 1 && tcp.flags.ack == 0. Строка фильтра подсвечена зелёным. В списке пакетов видны только SYN-пакеты.*

Шаг 5. Симуляция и обнаружение сканирования портов

Сценарий: одним из первых признаков подготовки атаки на АСУ ТП является **сканирование портов** – злоумышленник последовательно проверяет, какие сервисы доступны на целевом устройстве, прежде чем выбрать вектор атаки. Вам предстоит воспроизвести эту активность и увидеть, как она выглядит в трафике.

5.1. Переключение на адаптер loopback

Нажмите красный квадрат для остановки захвата. Нажмите Ctrl+W, чтобы закрыть текущий файл захвата и вернуться на стартовый экран Wireshark.

В списке интерфейсов найдите **«Adapter for loopback traffic capture»** – этот адаптер регистрирует трафик, адресованный на 127.0.0.1 (адрес локальной петли самого компьютера). Через обычный Ethernet-адаптер такой трафик не проходит и не виден, поэтому переключение обязательно.

Если адаптер не отображается: при установке Wireshark галочка «Support loopback traffic» в компоненте Npcap не была отмечена. Откройте «Программы и компоненты» → найдите Npcap → нажмите «Изменить» → добавьте компонент. Либо переустановите Wireshark полностью, отметив нужную опцию.

Дважды кликните по **«Adapter for loopback traffic capture»** – начнётся захват на loopback-интерфейсе.

5.2. Генерация трафика сканирования

Откройте **PowerShell** и выполните команды, которые последовательно проверяют доступность пяти портов на локальной машине:

```
Test-NetConnection -ComputerName 127.0.0.1 -Port 80
Test-NetConnection -ComputerName 127.0.0.1 -Port 502
Test-NetConnection -ComputerName 127.0.0.1 -Port 3389
Test-NetConnection -ComputerName 127.0.0.1 -Port 4840
Test-NetConnection -ComputerName 127.0.0.1 -Port 102
```

Дождитесь завершения всех пяти команд (каждая занимает 3–5 секунд). Остановите захват.

5.3. Обнаружение аномалии

Примените фильтр отображения:

tcp.flags.syn == 1 && ip.dst == 127.0.0.1

Вы увидите серию SYN-пакетов на порты 80, 502, 3389, 4840, 102 – **один источник, разные порты, короткий промежуток времени**. Именно так выглядит сканирование портов в реальной промышленной сети, когда посторонний узел проводит разведку перед атакой.

5.4. Определение открытых и закрытых портов

Сбросьте фильтр. Примените новый:

tcp.flags.reset == 1

Пакет **TCP RST** означает «порт закрыт» – система отвергла попытку подключения. Пакет **TCP SYN-ACK** (флаги syn == 1 && ack == 1) означает «порт открыт, сервис работает».

Запишите в отчёт: на какие из пяти проверенных портов пришёл RST (порт закрыт), а на какие – SYN-ACK (порт открыт)? Как эта информация могла бы быть использована злоумышленником при планировании атаки на АСУ ТП?

СКРИНШОТ 4 – вставить здесь: *окно Wireshark с применённым фильтром tcp.flags.syn == 1 && ip.dst == 127.0.0.1. В списке пакетов видна серия SYN-пакетов на разные порты (80, 502, 3389, 4840, 102) от одного источника – картина сканирования портов.*

Шаг 6. Настройка фильтра захвата для мониторинга промышленных портов

В реальной эксплуатации инженер не просматривает весь трафик вручную – на загруженной промышленной сети за одну секунду может проходить несколько тысяч пакетов. Вместо этого настраивается **фильтр захвата**, который сохраняет только события, представляющие интерес с точки зрения безопасности.

6.1. Вернитесь на стартовый экран (Ctrl+W). Откройте **Capture → Options** (Ctrl+K).

6.2. Выберите **Ethernet** или **Wi-Fi** интерфейс (возвращаемся на реальный сетевой адаптер). В поле **«Capture filter for selected interfaces»** введите:

tcp port 502 or tcp port 4840 or tcp port 102 or tcp port 20000

Нажмите **Start**.

6.3. Для генерации тестового трафика выполните в PowerShell:

Test-NetConnection -ComputerName [ШЛЮЗ] -Port 502

Test-NetConnection -ComputerName [ШЛЮЗ] -Port 4840

(пример: Test-NetConnection -ComputerName 192.168.1.1 -Port 502)

Дождитесь завершения команд. Откройте браузер, перейдите на несколько сайтов – это создаст «фоновый» трафик, который фильтр должен игнорировать. Остановите захват.

Обратите внимание: в списке пакетов присутствуют **только** пакеты на промышленные порты. Весь браузерный трафик, DNS-запросы и прочее – отсутствуют, фильтр их отсёк ещё на входе.

Запишите в отчёт: сколько пакетов захвачено с фильтром? Сравните с общим количеством пакетов из Шага 3 (без фильтра). Объясните, почему именно такой режим работы практичен при мониторинге промышленной сети в режиме реального времени.

СКРИНШОТ 5 – вставить здесь: *диалог «Capture Options» с заполненным полем фильтра захвата tcp port 502 or tcp port 4840 or tcp port 102 or tcp port 20000, выбранным Ethernet/Wi-Fi интерфейсом.*

Содержание отчёта

1. **Шаг 2** – IP-адрес вашего шлюза.
2. **Шаг 3** – заполненная таблица из семи полей пакета + Скриншот 2.
3. **Шаг 4** – результаты по каждому из четырёх фильтров с наблюдениями + Скриншот 3.
4. **Шаг 5** – таблица результатов сканирования (порт – открыт/закрыт), ответ на вопрос о возможном использовании этих данных злоумышленником + Скриншот 4.
5. **Шаг 6** – сравнение количества пакетов с фильтром и без + Скриншот 5.
6. **Вывод** – в чём принципиальное отличие нормального трафика от аномального? Почему анализ трафика является мерой обнаружения, а не предотвращения атак?

Контрольные вопросы

1. Почему инженеру по автоматизации технологических процессов необходимо владеть навыками анализа сетевого трафика, даже если на предприятии есть выделенная служба информационной безопасности?
2. Объясните разницу между фильтром захвата и фильтром отображения. В каком случае применяется каждый?
3. Какой паттерн сетевого трафика является признаком сканирования портов? По каким полям пакета TCP это можно определить?

4. Что означают ответы TCP RST и TCP SYN-ACK на попытку подключения? Какую информацию они дают о состоянии сервиса?

Почему появление трафика на порту 502 с неизвестного IP-адреса является поводом для немедленного расследования в промышленной сети АСУ ТП?

Лабораторная работа № 2

Разработка стратегии безопасности

Теоретическая часть

1. Что такое стратегия безопасности и зачем она нужна

В предыдущих темах курса мы рассматривали конкретные технические меры защиты: настройку брандмауэра, анализ сетевого трафика, политики паролей, шифрование. Каждая из этих мер сама по себе решает частную задачу – закрывает определённый порт, фиксирует событие, защищает конкретный файл. Однако набор отдельных технических мер, применённых бессистемно, не является безопасностью. Это лишь набор заплат на костюме, который может быть дырявым в совершенно других местах.

Стратегия информационной безопасности – это документ верхнего уровня, определяющий: что именно мы защищаем, от кого и от чего, какими средствами, в какой последовательности и как проверяем, что защита работает. Стратегия переводит разговор о безопасности с языка технических решений на язык **управленческих решений**: она объясняет руководству предприятия, почему безопасность требует инвестиций, и объясняет техническим специалистам, чем обусловлен выбор тех или иных мер.

Ключевое свойство стратегии – **приоритизация**. Ресурсы любого предприятия ограничены: нельзя одновременно защитить всё от всего с максимальной надёжностью. Стратегия отвечает на вопрос «что защищать в первую очередь» на основе объективной оценки рисков – а не интуиции, случайности или давления поставщика конкретного защитного решения. Без стратегии безопасность АСУ ТП деградирует в хаотичный набор мер: где-то установили антивирус, где-то поменяли пароли, брандмауэр настроен – но никто не может объяснить, от каких конкретных угроз это защищает и защищает ли вообще.

Разработка стратегии проходит строго последовательно через пять этапов, каждый из которых служит входными данными для следующего:

1. **Описание объекта** – что представляет собой система и как она устроена;
2. **Модель нарушителя** – кто может атаковать систему и зачем;
3. **Реестр активов** – что именно нужно защищать и насколько это ценно;
4. **Модель угроз** – как конкретно нарушитель может воздействовать на конкретные активы через конкретные уязвимости;

5. **План защитных мер** – что делать в первую очередь, исходя из оценённых рисков.

2. Этап 1. Описание объекта защиты

Стратегия безопасности всегда создаётся под конкретную систему – «универсальной стратегии» не существует. Поэтому работа начинается с тщательного изучения объекта: какое оборудование входит в состав системы, как оно соединено, какие протоколы используются, есть ли подключение к внешним сетям и на каких условиях.

Для промышленной системы описание объекта должно включать два обязательных элемента: **текстовое описание** состава и назначения системы и **схему сетевой топологии** – визуальное представление того, как компоненты связаны между собой.

Схема топологии особенно важна для анализа безопасности, потому что именно она позволяет увидеть **точки сочленения** различных сегментов – места, где трафик переходит из одной зоны в другую. Злоумышленник, проникший в корпоративную сеть предприятия, может попасть в промышленный сегмент только через такую точку сочленения. Если этой точки нет (сети физически изолированы) – промышленный сегмент недостижим из корпоративного. Если точка есть, но защищена маршрутизатором с правилами фильтрации – доступ ограничен. Если сети объединены без какой-либо фильтрации – злоумышленник в корпоративной сети автоматически оказывается в промышленной.

При изучении объекта задания в данной лабораторной работе обратите внимание на следующие детали, которые имеют прямое отношение к безопасности: наличие открытого RDP на порту 3389, отсутствие упоминания о разделении сетей на уровне VLAN, использование протокола Modbus TCP (который не имеет встроенных механизмов аутентификации), а также то, что сервер исторических данных (база данных) размещён на том же физическом сервере, что и SCADA.

3. Этап 2. Построение модели нарушителя

3.1 Зачем нужна модель нарушителя

Защитные меры всегда создаются против конкретных угроз. Угрозы исходят от конкретных нарушителей. Разные нарушители обладают разными возможностями, мотивами и методами – и это напрямую влияет на то, какие именно угрозы реализуемы в данной системе, а какие нет.

Рассмотрим простой пример. Угроза «физическое уничтожение сервера SCADA кувалдой» теоретически существует для любого предприятия. Однако реализуема ли она зависит от нарушителя. Для внешнего хакера, атакующего систему через интернет, эта

угроза нереализуема вовсе – у него нет физического доступа к оборудованию. Для действующего сотрудника предприятия с психическим расстройством – гипотетически реализуема. Без модели нарушителя мы не можем сделать такое разграничение и будем либо тратить ресурсы на защиту от нереалистичных угроз, либо упускать реальные.

3.2 Категории нарушителей и их характеристики

В практике безопасности АСУ ТП принято рассматривать четыре основные категории нарушителей.

Внешний злоумышленник – лицо или группа, не имеющие никакого легитимного доступа к системе. Это наиболее «медийная» категория нарушителей, которую представляют в виде «хакера в тёмной комнате». В реальности внешний злоумышленник, атакующий промышленное предприятие, чаще всего действует opportunistically – то есть ищет любые доступные уязвимости через интернет с помощью автоматизированных инструментов (сканеры, боты), а не целенаправленно охотится именно за вашим предприятием. Мотив такого нарушителя – финансовая выгода (установка шифровальщика-вымогателя, продажа доступа к системе на подпольных форумах) или демонстрация возможностей. Уровень подготовки – от низкого (использование готовых эксплойтов без понимания их работы, так называемые «скрипт-кидди») до высокого (написание собственных инструментов). Доступ к системе – только через внешние интерфейсы: открытые порты в интернете, фишинговые письма сотрудникам.

Ключевое уязвимое место для внешнего злоумышленника в нашем объекте – **открытый RDP на порту 3389**, доступный из интернета. Именно такие открытые порты сканируют автоматизированные боты непрерывно, 24 часа в сутки. По данным сервиса Shodan, порт 3389 является одним из наиболее сканируемых портов в интернете – каждый час миллионы IP-адресов по всему миру проверяются на наличие открытого RDP.

Недобросовестный конкурент – юридическое или физическое лицо, имеющее коммерческий интерес в получении информации о производственных процессах конкурирующего предприятия. Для пищевого производства это в первую очередь производственные рецептуры и технологические параметры – информация, которую предприятие годами разрабатывало и защищает как коммерческую тайну. Мотив – конкурентное преимущество, не разрушение. Это важно: конкурент не заинтересован в останове производства, авариях или публичном скандале – ему нужна тихая кража данных, незаметная для жертвы. Уровень подготовки – как правило, высокий: конкурент

располагает финансовыми ресурсами для найма профессиональных специалистов. Доступ – чаще всего через внешние интерфейсы или через вербовку инсайдера.

Бывший сотрудник – лицо, ранее имевшее легитимный доступ к системе и сохранившее технические знания о её устройстве, а возможно – и активные учётные данные, если администраторы забыли их отозвать при увольнении. Мотив – личная обида, желание нанести ущерб бывшему работодателю, реже – шантаж или финансовая выгода. Опасность этой категории в том, что нарушитель обладает знанием внутренней структуры системы: он знает IP-адреса, знает логины и пароли (которые могут быть не изменены с момента его увольнения), знает режим работы предприятия и время минимальной активности персонала. Такой нарушитель действует целенаправленно и эффективно даже при относительно невысоком уровне технической подготовки. Типичный вектор атаки: попытка входа в систему через RDP или VPN с ранее использованными учётными данными.

Инсайдер – действующий сотрудник предприятия, злоупотребляющий легитимным доступом к системе. Это наиболее опасная и наиболее трудно обнаруживаемая категория нарушителей. Инсайдер уже находится внутри защитного периметра – все технические барьеры, которые мы выстраиваем против внешних злоумышленников, для него не существуют. Мотивы инсайдера разнообразны: финансовая выгода (продажа рецептур конкурентам), шантаж (давление со стороны конкурентов или преступных группировок), недовольство условиями работы. Действия инсайдера сложно отличить от легитимных: оператор SCADA, копирующий файл с рецептурой на USB-флешку, делает то, что он и должен делать – работает с данными системы.

3.3 Как заполнить Таблицу 1: пример рассуждения

Мотив: финансовая выгода – установить шифровальщик-вымогатель на SCADA-сервер и потребовать выкуп за восстановление работоспособности, либо продать доступ к системе.

Уровень подготовки: средний – использует готовые инструменты для сканирования открытых RDP-портов и подбора паролей (hydra, ncrack), не разрабатывает собственных эксплойтов.

Доступ к системе: только внешний – через открытый RDP-порт 3389, доступный из интернета.

Вероятные методы: автоматизированный перебор паролей к RDP (атака «brute force»); использование известных уязвимостей RDP (BlueKeep, EternalBlue при устаревшей ОС); фишинговое письмо сотрудникам с вредоносным вложением.

По такой же логике заполняются строки для остальных трёх категорий нарушителей.

4. Этап 3. Составление реестра активов

4.1 Что такое актив в контексте безопасности

Актив (Asset) – это любой ресурс, имеющий ценность для предприятия и требующий защиты. В промышленной системе активы не ограничиваются физическим оборудованием – серверами и контроллерами. Активом является и **информация**: программа ПЛК, которую создавали инженеры годами, база данных historian с пятилетним архивом технологических параметров, рецептуры продуктов – всё это информационные активы, утрата или компрометация которых причинит предприятию реальный ущерб.

Активом является и **функциональность**: способность системы выполнять своё назначение в реальном времени. Остановка линии пастеризации из-за кибератаки – это не потеря данных, это потеря производительности, порча сырья, нарушение договорных обязательств.

4.2 Триада CIA и оценка ценности актива

Каждый актив оценивается по трём параметрам – известной вам **триаде CIA** (Confidentiality – Integrity – Availability):

Конфиденциальность (Confidentiality) – насколько критично, что посторонние узнают содержание этого актива. Для рецептур пищевого продукта конфиденциальность критически важна: это коммерческая тайна. Для программы ПЛК – менее важна: сам по себе алгоритм управления не является коммерческой тайной, хотя и не подлежит публичному раскрытию. Для управляющих команд в реальном времени – вопрос конфиденциальности второстепенен по сравнению с их целостностью.

Целостность (Integrity) – насколько критично, что содержание актива будет несанкционированно изменено. Именно этот параметр является ключевым для промышленных систем. Изменённая уставка температурного регулятора пастеризатора – это не просто технический сбой, это потенциальная угроза здоровью потребителей продукции. Изменённая запись в базе данных historian – это фальсификация архива качества, за которой может скрываться реальная производственная авария. Именно

поэтому целостность должна получать оценку 3 («критическая») для всех активов, связанных с управлением технологическим процессом.

Доступность (Availability) – насколько критично, что актив окажется недоступен (система остановится, данные окажутся заблокированы). Для линии пастеризации непрерывного действия недоступность системы управления означает немедленную остановку производства – оценка 3. Для архива historian временная недоступность менее критична – производство может продолжаться без доступа к историческим данным – оценка 2.

4.3 Как правильно выставить оценки: типичные ошибки

Наиболее распространённая ошибка при оценке активов – **завышение всех параметров до максимума** («всё важно, всё критично»). Если каждый актив получает оценку 3-3-3, реестр теряет смысл: он не помогает расставить приоритеты. Оценки должны реально отражать различия между активами.

Программа ПЛК-1, ПЛК-2 (алгоритм управления пастеризатором):

- Конфиденциальность: 2 – алгоритм имеет техническую ценность, его утечка нежелательна, но не катастрофична;
- Целостность: 3 – несанкционированное изменение программы ПЛК немедленно нарушает технологический процесс и может привести к аварии; это критично;
- Доступность: 3 – ПЛК должен работать непрерывно; если программа ПЛК оказывается недоступной (контроллер перезагружен или прошивка уничтожена), линия останавливается немедленно.
- Суммарная ценность: 8 из 9.

Журнал аудита и события безопасности:

- Конфиденциальность: 2 – журнал содержит информацию о действиях пользователей; его утечка нежелательна, но не катастрофична;
- Целостность: 3 – если злоумышленник может изменить или удалить журнал, он скрывает следы своего вторжения; расследование инцидента становится невозможным;
- Доступность: 1 – недоступность журнала не останавливает производство; это серьёзно, но не критично в краткосрочной перспективе.
- Суммарная ценность: 6 из 9.

Такое рассуждение – явное и письменное – должно сопровождать каждую строку вашего реестра активов в колонке «Обоснование».

5. Этап 4. Построение модели угроз

5.1 Структура угрозы: четыре элемента

Прежде чем заполнять таблицу угроз, необходимо понять, из каких элементов состоит полное описание угрозы. Неполное описание ведёт к неверной оценке риска и выбору неэффективных мер защиты.

Каждая угроза описывается четырьмя элементами, которые отражены в столбцах Таблицы 3:

Формулировка угрозы – что именно происходит. Правильная формулировка угрозы должна быть конкретной: не «взлом системы» (слишком абстрактно), а «несанкционированный вход в операционную систему SCADA-сервера через протокол RDP». Угроза всегда описывается как действие нарушителя над конкретным активом.

Уязвимость – почему это действие возможно. Угроза не реализуется «из воздуха» – для её реализации в системе должна существовать конкретная уязвимость. Уязвимость – это слабость: техническая (открытый порт, отсутствие аутентификации, устаревшее ПО) или организационная (отсутствие регламента, безграмотность персонала). Без уязвимости угроза нереализуема: например, угроза «проникновение из интернета в промышленный сегмент» нереализуема если промышленный сегмент физически изолирован – уязвимость отсутствует.

Нарушитель – кто реализует угрозу. Это прямая связь с Таблицей 1: каждая угроза должна быть соотнесена с конкретной категорией нарушителя из модели. Некоторые угрозы могут быть реализованы несколькими категориями нарушителей – в этом случае берётся нарушитель с наиболее высокой вероятностью реализации.

Актив – что является целью или объектом воздействия. Прямая связь с Таблицей 2.

5.2 Оценка вероятности: как рассуждать

Вероятность реализации угрозы – наиболее субъективный параметр оценки, требующий наиболее развёрнутого обоснования. Рассмотрим конкретные факторы, влияющие на вероятность.

Публичность уязвимости. Если уязвимость хорошо известна и для неё существуют готовые инструменты эксплуатации – вероятность высокая. Открытый RDP без ограничения числа попыток входа – это именно такой случай: инструменты для автоматического перебора паролей (Hydra, Medusa) общедоступны и не требуют специальных знаний. Вероятность – 4.

Сложность эксплуатации. Если для реализации угрозы нарушителю нужны редкие технические знания, специальное оборудование или физический доступ к конкретному оборудованию – вероятность ниже. Угроза «перехват трафика между ПЛК и SCADA через атаку «человек посередине»» требует физического доступа к промышленному коммутатору или возможности подключить своё устройство в промышленный сегмент сети. Для внешнего злоумышленника это практически нереализуемо, для инсайдера – возможно, но требует технической подготовки. Вероятность – 2–3.

Мотивация нарушителя. Если у нарушителя есть сильная конкретная мотивация атаковать именно этот объект – вероятность выше. Если объект случаен для нарушителя – ниже.

Наличие существующих защитных мер. Если в системе уже реализованы меры, снижающие вероятность реализации угрозы – это должно быть учтено. Однако на этапе построения модели угроз мы оцениваем систему в её текущем состоянии – до применения новых мер. Меры, которые только планируются, не влияют на текущую оценку вероятности.

Пример рассуждения для угрозы № 1 из Таблицы 3 – подбор пароля к RDP:

«RDP-порт открыт в интернете. Автоматические сканеры ежедневно находят этот порт. Инструменты перебора паролей общедоступны. Если пароль имеет среднюю сложность (8–10 символов) без политики блокировки – перебор словарными атаками реален. Вероятность: 4 (вероятно)».

5.3 Оценка ущерба: как рассуждать

Ущерб от реализации угрозы нужно оценивать не формально («взломают – это плохо»), а через конкретные последствия для производственного процесса и предприятия.

Для промышленной системы ущерб имеет несколько измерений, которые нужно рассмотреть совокупно: прямой финансовый ущерб (стоимость восстановления, выплата выкупа, штрафы), производственный ущерб (остановка линии, порча сырья, срыв контрактов), репутационный ущерб (публичный скандал, потеря клиентов) и, наиболее серьёзно – ущерб здоровью или жизни (нарушение безопасности технологического процесса).

Пример рассуждения для угрозы № 3 – несанкционированное изменение уставок пастеризатора:

«Пастеризация – критический процесс с точки зрения безопасности пищевых продуктов. Снижение температуры пастеризации ниже регламентного значения

приводит к недостаточному обеззараживанию продукта. Последствия: продукт с патогенной микрофлорой поступает к потребителям; массовые случаи пищевого отравления; отзыв партии продукции; проверка Роспотребнадзора; уголовная ответственность руководства предприятия. Это наихудший сценарий с угрозой жизни потребителей. Ущерб: 5 (критический)».

5.4 Как самостоятельно сформулировать угрозы для строк 9 и 10

В Таблице 3 строки 9 и 10 студент заполняет самостоятельно. Чтобы грамотно сформулировать угрозу, воспользуйтесь следующим алгоритмом.

Посмотрите на состав объекта и найдите компоненты, которые ещё не фигурировали в строках 1-8. В описании объекта упомянуты: промышленный коммутатор Cisco SG350 с веб-интерфейсом управления; маршрутизатор MikroTik с интерфейсом конфигурации; ПЛК-3 ОВЕН ПЛК110 с возможностью перепрограммирования; корпоративная сеть с 1С и выходом в интернет. Для каждого из этих компонентов спросите себя: какой нарушитель может воздействовать на этот компонент, через какую уязвимость, и что произойдёт с активами системы в результате?

Например: «ПЛК ОВЕН ПЛК110 имеет веб-интерфейс конфигурирования, доступный по сети. Если пароль к этому интерфейсу не изменён с заводского значения, любой пользователь промышленного сегмента (в том числе заражённый офисный ПК, получивший доступ через маршрутизатор) может изменить программу ПЛК-3, управляющего линией фасовки». Это и есть угроза – конкретная, с указанием нарушителя (заражённый узел в корпоративной сети), уязвимости (заводские учётные данные на ПЛК) и затрагиваемого актива (программа ПЛК-3).

5.5 Построение матрицы рисков

После заполнения всех строк таблицы необходимо визуализировать результаты в виде **матрицы рисков**. Матрица представляет собой таблицу 5×5, по оси X которой откладывается вероятность (1–5), по оси Y – ущерб (1–5). Каждая ячейка закрашивается цветом в зависимости от произведения координат:

- Ячейки с произведением 1–4 закрашиваются **зелёным** (низкий риск);
- Ячейки с произведением 5–9 – **жёлтым** (средний риск);
- Ячейки с произведением 10–16 – **оранжевым** (высокий риск);
- Ячейки с произведением 17–25 – **красным** (критический риск).

Каждая угроза из Таблицы 3 наносится на матрицу своим номером в соответствующую ячейку. После нанесения всех угроз матрица наглядно показывает: угрозы в красных и оранжевых ячейках требуют немедленного внимания, в жёлтых – планового, в зелёных – мониторинга.

Вот как выглядит заполненная матрица в текстовом виде (У – ущерб по вертикали, В – вероятность по горизонтали):

У \ В	1	2	3	4	5
5	[5]	[10]	[15]	[20]	[25]
4	[4]	[8]	[12]	[16]	[20]
3	[3]	[6]	[9]	[12]	[15]
2	[2]	[4]	[6]	[8]	[10]
1	[1]	[2]	[3]	[4]	[5]

Цвет: зелёный=1–4, жёлтый=5–9, оранжевый=10–16, красный=17–25 Разместите номера своих угроз в соответствующих ячейках матрицы и закрасьте ячейки в соответствии со шкалой. В отчёте матрица оформляется как цветная таблица в MS Word.

6. Этап 5. Разработка плана защитных мер

6.1 Принцип выбора мер: от риска к мере

Каждая защитная мера должна быть обоснована конкретной угрозой и конкретной уязвимостью. Типичная ошибка – предлагать «установить антивирус» как ответ на любую угрозу. Антивирус не защищает от подбора пароля к RDP, не закрывает уязвимость в Modbus TCP и не препятствует инсайдеру копировать данные на USB.

Правильный алгоритм выбора меры таков: смотрим на уязвимость, через которую реализуется угроза, и выбираем меру, которая **устраняет уязвимость** или делает её эксплуатацию значительно сложнее. Для угрозы «подбор пароля к RDP» уязвимость – открытый порт 3389 и отсутствие блокировки после неудачных попыток. Меры: перенести RDP на нестандартный порт (усложняет автоматическое сканирование), включить блокировку учётной записи (практическая работа №3), настроить VPN и требовать подключения к RDP только через VPN-тоннель (полностью убирает доступ из открытого интернета).

6.2 Технические и организационные меры: в чём разница

Техническая мера – это изменение конфигурации оборудования или программного обеспечения: включение шифрования, настройка правил брандмауэра, обновление программного обеспечения, разделение сетей на VLAN. Техническая мера работает

автоматически, не требуя постоянного участия человека, – и именно поэтому она предпочтительна там, где её можно применить.

Организационная мера – это регламент, инструкция, политика или обучение: «запрещено подключать личные USB-носители», «инженер-интегратор обязан использовать VPN», «плановое обновление паролей – раз в 90 дней». Организационная мера опирается на человеческое исполнение, и именно поэтому её нарушение возможно. Организационные меры незаменимы там, где техническая мера неприменима – например, невозможно технически запретить инсайдеру смотреть на экран монитора, но можно организационно ограничить круг лиц, имеющих доступ в помещение.

Наиболее эффективна **комбинированная мера** – сочетание технической и организационной составляющих. Например, для защиты от несанкционированного копирования данных: технически отключить USB-порты через политику Windows (практическая работа №3) + организационно ввести регламент, запрещающий использование личных носителей, и ознакомить с ним всех сотрудников под подпись.

6.3 Как обоснованно назначить ответственного и срок

Ответственный за реализацию меры назначается исходя из её типа и области применения. Технические меры на уровне сетевого оборудования (маршрутизатор, коммутатор) – ответственность **системного администратора АСУ ТП** или **сетевого инженера**. Технические меры на уровне SCADA-сервера и рабочих станций – **системный администратор АСУ ТП**. Организационные меры, касающиеся регламентов и инструкций для персонала – **начальник производства** или **специалист по ИБ**. Меры, требующие изменений в конфигурации ПЛК или SCADA-приложения – **инженер-интегратор** (организация, осуществлявшая внедрение системы).

Срок реализации определяется двумя факторами: критичностью риска и сложностью меры. Для критических рисков из красной зоны матрицы – **немедленно**, в течение одной недели. Приоритет обусловлен тем, что каждый день промедления означает день работы системы с критической уязвимостью. Для высоких рисков – **краткосрочно**, в течение одного месяца. Для средних рисков – **среднесрочно**, 3–6 месяцев (плановые мероприятия в рамках следующего бюджетного цикла). Для низких рисков – **долгосрочно**, до года.

7. Этап 6. Проверка эффективности мер

Принятые меры защиты необходимо регулярно проверять: работают ли они в действительности или только на бумаге. Проверка строится по принципу: «воспроизвести действия нарушителя в контролируемых условиях и убедиться, что мера их блокирует».

Для угрозы «подбор пароля к RDP»: метод проверки – попытаться намеренно ввести неверный пароль пять раз подряд и убедиться, что учётная запись заблокирована (метод отработан в Практической работе №3). После этого проверить журнал безопасности Windows и убедиться, что события 4625 и 4740 зафиксированы. Периодичность – ежеквартально.

Для угрозы «проникновение из корпоративного сегмента в промышленный»: метод проверки – с корпоративного ПК попытаться выполнить ping или traceroute до IP-адресов в промышленном сегменте (192.168.10.x) и убедиться, что пакеты не проходят (если настроена фильтрация) или проходят только к разрешённым адресам. Периодичность – ежемесячно.

Для угрозы «несанкционированное изменение программы ПЛК»: метод проверки – убедиться, что контрольная сумма (хэш) загруженной в ПЛК программы совпадает с эталонным значением, зафиксированным при последней авторизованной загрузке. Многие среды программирования ПЛК (STEP 7, TIA Portal, CODESYS) предоставляют встроенные инструменты сравнения онлайн-программы с архивным проектом. Периодичность – еженедельно.

8. Нормативная база

Разработка стратегии безопасности АСУ ТП в России опирается на несколько ключевых нормативных документов.

Приказ ФСТЭК России №31 является главным отраслевым документом: он определяет обязательный перечень мер защиты АСУ ТП, сгруппированных по классам (УПД – управление доступом, АУД – аудит безопасности, ЗНИ – защита носителей информации и другие). Для объектов КИИ перечень мер является обязательным; для прочих промышленных объектов – рекомендательным, но служит общепринятым ориентиром.

Методика оценки угроз безопасности информации ФСТЭК России (версия 2021 года) задаёт официальную методологию построения модели угроз для государственных информационных систем. Именно эта методика лежит в основе подхода, применяемого в данной лабораторной работе.

МЭК 62443 – международный стандарт безопасности промышленных систем автоматизации. Часть 3-2 стандарта посвящена оценке рисков безопасности для систем управления и практически полностью соответствует методологии, которую вы применяете в данной работе.

Практическое задание

Цель работы

Разработать стратегию информационной безопасности для типовой АСУ ТП производственного предприятия на основе методики оценки рисков: построить модель нарушителя, составить реестр активов, сформировать модель угроз с количественной оценкой рисков и разработать приоритизированный план защитных мер.

Объект защиты

Все студенты выполняют работу на одном объекте – типовой АСУ ТП **линии производства пищевых продуктов** (пастеризация, розлив, фасовка).

Состав АСУ ТП объекта:

Компонент	Описание
ПЛК-1, ПЛК-2	Siemens S7-1200; управляют температурой и давлением пастеризатора
ПЛК-3	ОВЕН ПЛК110; управляет линией розлива и фасовки
SCADA-сервер	ПК под Windows 10; MasterSCADA 4D; IP 192.168.10.5
АРМ оператора	ПК под Windows 10; IP 192.168.10.20
Historian	Microsoft SQL Server на SCADA-сервере; хранит 5 лет архива
Промышленный коммутатор	Cisco SG350; объединяет все устройства в сегмент 192.168.10.0/24
Маршрутизатор	MikroTik; связывает промышленный сегмент с корпоративной сетью 192.168.1.0/24
Корпоративная сеть	15 офисных ПК, 1С:Предприятие, выход в интернет
Удалённый доступ	Открытый RDP (порт 3389) на SCADA-сервере для обслуживания интегратором

Шаг 1. Построение модели нарушителя

Заполните **Таблицу 1 – Модель нарушителя**, описав четыре категории нарушителей. Для каждой категории подробно укажите мотив, уровень технической подготовки, предполагаемый начальный доступ к системе и вероятные методы атаки применительно к описанному объекту. Рассуждайте по алгоритму, описанному в разделе 3.3 теоретической части.

Категория нарушителя	Мотив	Уровень технической подготовки	Предполагаемый доступ к системе	Вероятные методы атаки
Внешний				

злоумышленник				
Недобросовестный конкурент				
Бывший сотрудник				
Инсайдер (действующий сотрудник)				

Шаг 2. Составление реестра активов

Заполните **Таблицу 2 – Реестр активов**. Для каждого актива выставьте оценку по шкале 1–3 по каждому параметру триады CIA, рассчитайте суммарную ценность и запишите развёрнутое обоснование. Руководствуйтесь примерами рассуждений из раздела 4.3 теоретической части.

№	Актив	Конфиден-циальность	Целост-ность	Доступ-ность	Суммарная ценность	Обоснование
1	Программа ПЛК-1, ПЛК-2					
2	База данных historian					
3	Технологические рецептуры					
4	Учётные данные операторов SCADA					
5	Конфигурация коммутатора					
6	Управляющие команды в реальном времени					
7	Журнал аудита и события безопасности					
8	Настройки удалённого доступа RDP					

Шаг 3. Построение модели угроз и матрица рисков

Заполните **Таблицу 3 – Модель угроз** (не менее 10 угроз). Заданные угрозы (строки 1–8) дополните оценками и мерами; строки 9–10 сформулируйте самостоятельно по алгоритму из раздела 5.4. Для оценки вероятности и ущерба используйте рассуждения по образцу из разделов 5.2–5.3.

После заполнения таблицы постройте цветную матрицу рисков (5×5) и нанесите на неё все угрозы по их номерам.

№	Угроза	Уязвимость	Актив (№ из Табл.2)	Нарушитель	В	У	Р	Уровень	Мера защиты
1	Подбор пароля к RDP	Открытый порт 3389 без блокировки							
2	Перехват трафика Modbus TCP	Отсутствие аутентификации Modbus							
3	Изменение уставок пастеризатора		1						
4	SQL-инъекция через веб-historian		2						
5	Шифровальщик через корпоративную сеть	Отсутствие сегментации сетей							
6	Кража резервной копии рецептур через USB		3	Инсайдер					
7	Подмена показаний датчиков (MitM)		6						
8	Удаление журнала аудита		7						
9	*(самостоятельно)*								
10	*(самостоятельно)*								

Шаг 4. План защитных мер

На основе модели угроз заполните **Таблицу 4 – План защитных мер**, упорядочив меры по убыванию уровня риска. Для каждой меры укажите тип (техническая / организационная / комбинированная), ответственного и срок реализации. Руководствуйтесь разделами 6.1-6.3 теоретической части.

Приоритет	№ угрозы	Уровень риска	Защитная мера	Тип меры	Ответственный	Срок
1						
2						
...						

Шаг 5. План проверки эффективности

Для трёх угроз с наибольшим уровнем риска разработайте процедуру проверки эффективности принятых мер и заполните **Таблицу 5 – План проверки**.

№ угрозы	Принятая мера	Метод проверки	Периодичность	Ожидаемый результат	Кто проверяет

Контрольные вопросы

1. Объясните, почему оценка риска строится как произведение вероятности и ущерба, а не как их сумма. Приведите пример двух угроз с одинаковым уровнем риска, но принципиально разными значениями вероятности и ущерба, и объясните, почему они могут требовать разных по типу мер защиты.

2. Почему открытый RDP на порту 3389 является угрозой даже при наличии сложного пароля? Назовите не менее двух векторов атаки через RDP, которые не зависят от сложности пароля.

3. Чем отличается организационная защитная мера от технической? Приведите пример ситуации, когда организационная мера является более эффективной, чем техническая.

4. В модели нарушителя рассматривается инсайдер – действующий сотрудник. Почему инсайдерская угроза считается наиболее трудно нейтрализуемой? Назовите конкретные технические и организационные меры, частично снижающие этот риск.

5. Что такое «остаточный риск»? Если уровень угрозы после принятия мер снизился с 20 до 6 баллов, означает ли это, что система полностью защищена? Что делать с остаточным риском?

Лабораторная работа № 3

Защита информации и криптография: хеширование, симметричное шифрование и цифровая подпись

Используемое программное обеспечение

Инструмент	Описание	Лицензия	Ссылка
gpg4win	Реализация OpenPGP для Windows: шифрование, подпись, управление ключами	GNU GPL – бесплатно	gpg4win.org
Kleopatra	Графический интерфейс для GnuPG, входит в gpg4win	GNU GPL – бесплатно	входит в gpg4win
CertUtil	Встроенная утилита Windows для вычисления хешей	Встроена в Windows	встроена
HashCalc	Утилита для вычисления хешей нескольких алгоритмов одновременно	Бесплатно	https://sourceforge.net/projects/hashcalc/
VeraCrypt	Программа для создания зашифрованных контейнеров и дисков	Apache 2.0 – бесплатно	https://sourceforge.net/projects/veracrypt/
Блокнот (Notepad)	Встроенный текстовый редактор Windows	Встроена в Windows	встроена

Подготовка рабочего места: перед началом работы создайте папку C:\CryptoLab\ и установите gpg4win и VeraCrypt. Оба дистрибутива скачиваются с официальных сайтов и не требуют лицензионных ключей.

Теоретическая часть

1. Криптография в АСУ ТП: зачем это нужно инженеру-автоматизатору

Слово «криптография» нередко ассоциируется исключительно с засекреченной перепиской или банковскими транзакциями. В действительности криптографические механизмы пронизывают всю современную промышленную систему – просто работают незаметно, «под капотом» протоколов и приложений.

Когда инженер подключается к веб-интерфейсу SCADA-сервера по протоколу HTTPS – работает криптография (TLS). Когда система сигнализирует об изменении программы ПЛК с момента последней авторизованной загрузки – работает криптография (хеш-функция). Когда оператор входит в систему по смарт-карте вместо пароля – работает криптография (асимметричное шифрование). Когда резервная копия базы historian шифруется перед записью на внешний носитель – работает криптография (симметричное

шифрование). Когда производитель ПЛК публикует обновление прошивки и подтверждает его подлинность – работает криптография (цифровая подпись).

Понимание криптографических механизмов необходимо инженеру по нескольким причинам. Во-первых, чтобы **правильно конфигурировать** системы, использующие криптографию: выбирать алгоритмы с достаточной стойкостью, правильно управлять ключами, не допускать типовых ошибок реализации. Во-вторых, чтобы **грамотно ставить задачи** разработчикам и интеграторам: понимать, что именно просить, и проверять, что это реализовано корректно. В-третьих, чтобы **выявлять уязвимости**: распознавать ситуации, когда приложение использует слабые или устаревшие алгоритмы – например, MD5 вместо SHA-256 или DES вместо AES.

Данная лабораторная работа охватывает весь практический арсенал прикладной криптографии, применяемый в защите промышленных систем: хеш-функции, симметричное шифрование файлов, создание зашифрованных контейнеров, генерацию ключевых пар, асимметричное шифрование и цифровую подпись.

2. Три задачи криптографии: конфиденциальность, целостность, аутентичность

Криптография решает три принципиально разные задачи, и для каждой из них существует свой класс инструментов. Важно понимать, что ни один класс не решает все три задачи одновременно в полной мере – именно поэтому реальные системы безопасности используют их в комбинации.

Конфиденциальность – гарантия того, что данные прочитает только тот, кому они предназначены. Даже если злоумышленник перехватит зашифрованные данные, он получит лишь бессмысленный набор байт. Конфиденциальность обеспечивается симметричным и асимметричным шифрованием.

Целостность – гарантия того, что данные не были изменены с момента их создания или последней авторизованной модификации. Это критически важно для промышленных систем: программа ПЛК, тихо изменённая злоумышленником, опаснее, чем открыто уничтоженная – ведь система продолжает работать, но непредсказуемо. Целостность обеспечивается хеш-функциями и цифровой подписью.

Аутентичность – гарантия того, что данные или сообщение действительно созданы заявленным источником. Файл конфигурации ПЛК, пришедший «от интегратора» по электронной почте – действительно ли от него? Команда на изменение уставки реактора действительно пришла от авторизованного инженера, а не была подделана атакой

«человек посередине»? Аутентичность обеспечивается цифровой подписью.

В реальных системах все три задачи решаются комплексно. Протокол TLS, используемый для защиты веб-интерфейса SCADA, одновременно обеспечивает конфиденциальность (шифрование трафика алгоритмом AES), целостность (MAC-коды сообщений) и аутентичность (сертификаты X.509). Однако понять комплексную систему невозможно без чёткого понимания каждого элемента по отдельности.

3. Хеш-функции: математический отпечаток данных

3.1 Принцип работы и ключевые свойства

Хеш-функция (функция свёртки, дайджест-функция) – это математическая функция, преобразующая данные произвольного размера в строку фиксированной длины, называемую **хешем** или **дайджестом**. Неважно, что именно подаётся на вход – один байт или гигабайтный архив проекта SCADA – результат всегда имеет фиксированный размер: 256 бит для SHA-256, 512 бит для SHA-512, 256 или 512 бит для российского алгоритма ГОСТ Р 34.11-2012 (Стрибог).

Хеш-функция обладает четырьмя ключевыми свойствами, определяющими её пригодность для задач безопасности.

Детерминированность: одни и те же входные данные всегда дают один и тот же хеш. Это необходимо для проверки целостности: вычислили хеш файла сегодня, через месяц вычислили снова – если хеш совпал, файл не изменился. Именно на этом свойстве строится контроль целостности программ ПЛК: эталонный хеш фиксируется в журнале при авторизованной загрузке, а затем регулярно сверяется с актуальным.

Необратимость (односторонность): зная хеш, невозможно восстановить исходные данные за приемлемое время. Хеш – это «отпечаток пальца» данных, но не сами данные. Именно поэтому пароли хранятся не в открытом виде и не в зашифрованном, а в виде хешей: даже получив базу данных пользователей, злоумышленник не может немедленно узнать исходные пароли.

Лавинный эффект: минимальное изменение входных данных приводит к кардинально иному хешу. Изменение одного бита в файле программы ПЛК приводит к тому, что итоговый хеш изменяется примерно на половину своих битов – результат становится совершенно непохожим на исходный. Это делает невозможным «угадать» исходные данные, зная хеш, или незаметно внести «небольшое» изменение.

Устойчивость к коллизиям: практически невозможно найти два разных файла с одинаковым хешем. Это критически важно: если бы злоумышленник мог подобрать

«вредоносный» файл с тем же хешем, что и легитимный, вся система контроля целостности стала бы бесполезной.

3.2 Актуальные и устаревшие алгоритмы

Не все хеш-алгоритмы одинаково надёжны, и выбор алгоритма имеет принципиальное значение для безопасности.

Алгоритмы **MD5** и **SHA-1** считаются криптографически устаревшими и не должны применяться для задач безопасности. Для MD5 ещё в 2004 году были продемонстрированы практические коллизии – два разных файла с одинаковым MD5-хешем. Для SHA-1 коллизия была найдена командой Google в 2017 году (атака SHAttered). Использование этих алгоритмов для проверки целостности или подписи недопустимо: злоумышленник может сформировать вредоносный файл с тем же хешем, что и легитимный.

Актуальными и рекомендованными алгоритмами являются **SHA-256** и **SHA-512** (семейство SHA-2) и **SHA3-256** (семейство SHA-3). Для объектов КИИ в России обязательным является российский стандарт **ГОСТ Р 34.11-2012** (алгоритм Стрибог) – использование SHA-256 в сертифицированных СКЗИ на объектах КИИ формально недостаточно.

В данной лабораторной работе мы будем работать с SHA-256 как с наиболее распространённым и наглядным примером современного хеш-алгоритма, а также сравним его с MD5, чтобы наглядно увидеть разницу в длине хеша и убедиться, что оба алгоритма демонстрируют одинаковые свойства – хотя надёжность MD5 уже не соответствует требованиям безопасности.

3.3 Практическое применение в АСУ ТП

Контроль целостности программ ПЛК. После авторизованной загрузки программы в контроллер вычисляется хеш файла проекта и фиксируется в журнале изменений с указанием даты, времени и ответственного инженера. При каждом плановом обслуживании специалист повторно вычисляет хеш и сравнивает с эталоном. Совпадение означает, что программа не изменялась. Расхождение требует немедленного расследования – кто, когда и зачем изменил программу ПЛК.

Верификация обновлений ПО. Производители SCADA-систем и прошивок ПЛК публикуют официальные хеш-суммы своих дистрибутивов. Перед установкой обновления системный администратор вычисляет хеш скачанного файла и сравнивает с официально опубликованным. Это защищает как от случайного повреждения файла при загрузке, так и

от целенаправленной подмены дистрибутива – атаки, известной под названием «supply chain attack» (атака на цепочку поставок).

Хранение паролей. В любой правильно реализованной системе аутентификации пароли хранятся в виде хешей – SCADA, historian, веб-интерфейс коммутатора. При входе система вычисляет хеш введённого пароля и сравнивает с хранимым хешем. Исходный пароль никогда не хранится в открытом виде – даже администратор системы не может его «посмотреть», только сбросить.

4. Симметричное шифрование: быстрая защита данных одним ключом

4.1 Принцип работы

Симметричное шифрование – это схема, в которой для шифрования и расшифровки используется **один и тот же секретный ключ**. Отправитель шифрует данные ключом, получает зашифрованный текст (шифртекст), передаёт его получателю, и получатель расшифровывает тем же ключом, восстанавливая исходные данные.

Ключ представляет собой случайную последовательность битов. Современный стандарт – 256-битный ключ. Для подбора такого ключа перебором потребовалось бы проверить 2^{256} вариантов – число, несопоставимо превышающее количество атомов во Вселенной. Даже если объединить вычислительную мощность всех компьютеров планеты, перебор такого ключа потребовал бы времени, многократно превышающего возраст Вселенной.

Главный алгоритм симметричного шифрования в мире – **AES (Advanced Encryption Standard)**, принятый в 2001 году и остающийся стандартом по сей день. В России для сертифицированных СКЗИ используется **ГОСТ Р 34.12-2015** (алгоритмы «Кузнечик» с длиной блока 128 бит и «Магма» с длиной блока 64 бита).

4.2 Режимы работы блочного шифра

AES является **блочным шифром** – он шифрует данные блоками по 128 бит. Для шифрования данных произвольного размера (файла любой длины) блочный шифр применяется в определённом **режиме работы**. Выбор режима существенно влияет на безопасность.

Режим ECB (Electronic Code Book) – наиболее простой: каждый блок данных шифруется независимо тем же ключом. Это режим с критической уязвимостью: одинаковые блоки открытого текста дают одинаковые блоки шифртекста. В результате шифртекст сохраняет статистические закономерности исходных данных. Режим ECB

недопустим для использования в реальных системах.

Режим CBC (Cipher Block Chaining) – каждый блок перед шифрованием объединяется (XOR) с предыдущим зашифрованным блоком, что устраняет проблему ECB. Требует вектора инициализации (IV) – случайного значения для первого блока. Является безопасным режимом, широко применяемым в большинстве приложений.

Режим GCM (Galois/Counter Mode) – наиболее современный и рекомендуемый режим, применяемый в TLS 1.3. Сочетает шифрование с аутентификацией: помимо обеспечения конфиденциальности, вычисляет **Authentication Tag** – криптографическую «подпись» зашифрованного блока, позволяющую обнаружить любое изменение шифртекста. AES-256-GCM одновременно обеспечивает конфиденциальность и целостность.

4.3 Главная проблема симметричного шифрования и как она решается

Симметричное шифрование чрезвычайно быстро и эффективно – AES-256 на современном процессоре с аппаратным ускорением (инструкции AES-NI) работает со скоростью нескольких гигабайт в секунду. Именно поэтому оно применяется для шифрования больших объёмов данных: резервных копий, архивов, дисковых разделов.

Однако у симметричного шифрования есть фундаментальная проблема: **как безопасно передать ключ получателю?** Если шифровать файл и отправлять его коллеге на другое предприятие, как сообщить ему ключ расшифровки? По электронной почте – злоумышленник, перехватывающий переписку, получит и ключ, и расшифрует все файлы. По телефону – неудобно и не масштабируется на сотни получателей.

Именно эту проблему – **проблему распределения ключей** – решает асимметричное шифрование. На практике большинство современных систем применяют **гибридное шифрование**: ключ сессии (случайный симметричный ключ) шифруется асимметричным алгоритмом (безопасная передача), а само сообщение шифруется симметричным алгоритмом этим ключом (высокая скорость). Именно так работает TLS, PGP и большинство других криптографических протоколов.

5. Зашифрованные контейнеры VeraCrypt: защита данных на носителе

Отдельного внимания заслуживает задача защиты данных, хранимых на физическом носителе – жёстком диске, USB-флешке, резервном носителе с архивом. Симметричное шифрование отдельных файлов решает задачу частично, но неудобно при работе с большим числом файлов в структуре папок. Для этого применяются **зашифрованные контейнеры** и **шифрование разделов**.

VeraCrypt – открытый инструмент для создания зашифрованных контейнеров (файлов-образов) и шифрования разделов дисков. Зашифрованный контейнер представляет собой файл с произвольным именем и расширением, внутри которого находится зашифрованная файловая система. При монтировании контейнера (с вводом правильного пароля или ключевого файла) он подключается в системе как обычный логический диск. Все операции чтения и записи выполняются «на лету» – прозрачно для приложений, работающих с файлами внутри контейнера.

В контексте АСУ ТП зашифрованные контейнеры применяются для защиты резервных копий баз данных historian (контейнер с резервной копией можно безопасно хранить на съёмном носителе или передавать по сети), защиты конфигурационных файлов и архивов проектов ПЛК (папка проекта SCADA или CODESYS монтируется из зашифрованного контейнера), защиты архивов на переносных носителях (USB-флешка, используемая для переноса конфигураций между объектами).

VeraCrypt поддерживает алгоритм AES-256 в режиме XTS – специализированном режиме для шифрования блочных носителей, обеспечивающем независимое шифрование каждого сектора диска. Помимо пароля, VeraCrypt поддерживает **ключевые файлы** (Key Files) – дополнительный фактор аутентификации: контейнер открывается только при наличии правильного пароля **и** правильного ключевого файла. Даже зная пароль, без ключевого файла открыть контейнер невозможно.

6. Асимметричное шифрование: пара ключей для безопасной передачи

6.1 Принцип работы

Асимметричное шифрование использует **математически связанную пару ключей**: открытый (public key) и закрытый (private key). Они генерируются вместе как единая пара на основе математических задач, решение которых в одном направлении тривиально, а в обратном – вычислительно нереализуемо (например, умножение двух простых чисел просто, а разложение их произведения на множители – крайне сложно при достаточно больших числах).

Открытый ключ можно и нужно раздавать всем желающим – публиковать на сайте, отправлять по электронной почте, размещать на сервере ключей. Он не является секретом. Открытым ключом можно **зашифровать** данные, но расшифровать их с помощью открытого ключа невозможно.

Закрытый ключ хранится только у владельца и никому не передаётся. Это самый ценный криптографический секрет. Только закрытым ключом можно **расшифровать** то,

что было зашифровано соответствующим открытым ключом.

Схема безопасной передачи данных: отправитель берёт **открытый ключ получателя** (который тот публично распространил), шифрует им данные и отправляет. Только получатель, владеющий закрытым ключом, может расшифровать. Злоумышленник, перехвативший шифртекст и даже знающий открытый ключ (он публичен), расшифровать данные не может.

6.2 Популярные алгоритмы

RSA – старейший и наиболее распространённый алгоритм асимметричного шифрования, основанный на сложности факторизации больших чисел. Стандартная длина ключа сегодня – 3072 или 4096 бит. RSA-1024 считается устаревшим и уязвимым.

ECC (Elliptic Curve Cryptography) – шифрование на основе эллиптических кривых. Обеспечивает аналогичную стойкость при значительно меньшей длине ключа: ключ ECC-256 примерно эквивалентен по стойкости ключу RSA-3072. В российском стандарте асимметричные операции реализуются алгоритмом **ГОСТ Р 34.10-2012** на эллиптических кривых.

6.3 Цифровая подпись

Пара ключей используется не только для шифрования, но и для **цифровой подписи** – механизма, одновременно обеспечивающего аутентичность и целостность. Цифровая подпись работает в «обратную сторону» по сравнению с шифрованием.

Автор документа вычисляет хеш документа и **шифрует хеш своим закрытым ключом**. Результат – цифровая подпись – прикладывается к документу. Любой получатель может **расшифровать подпись открытым ключом автора** (который публичен), получить хеш из подписи, самостоятельно вычислить хеш документа и сравнить два хеша. Если хеши совпали – подпись верна.

Это одновременно доказывает две вещи: **аутентичность** (только владелец закрытого ключа мог создать эту подпись) и **целостность** (любое изменение документа после подписания изменит хеш и сделает подпись недействительной).

7. OpenPGP, GnuPG и Web of Trust

OpenPGP (RFC 4880) – открытый стандарт шифрования и цифровой подписи. Стандарт реализует гибридное шифрование: для каждого сообщения генерируется случайный симметричный сессионный ключ, которым шифруется само сообщение; затем сессионный ключ шифруется открытым ключом получателя. Расшифровка выполняется в обратном порядке: получатель расшифровывает сессионный ключ своим закрытым

ключом, затем расшифровывает сообщение сессионным ключом.

GnuPG (GNU Privacy Guard) – открытая реализация стандарта OpenPGP, существующая с 1999 года. На Windows доступна в виде пакета **gpg4win** с графическим интерфейсом **Kleopatra**. GnuPG является промышленным стандартом де-факто и активно используется для подписания пакетов в дистрибутивах Linux, подписания официальных документов, защиты корпоративной переписки.

В OpenPGP для подтверждения принадлежности ключа используется концепция **«Сеть доверия» (Web of Trust)**: пользователи подписывают открытые ключи друг друга, удостоверяя, что данный ключ действительно принадлежит заявленному владельцу. Это децентрализованная альтернатива иерархической инфраструктуре PKI с удостоверяющими центрами.

8. Нормативная база криптографии в России

Применение криптографии на промышленных объектах в России регулируется несколькими документами. **ГОСТ Р 34.12-2015** определяет стандартные алгоритмы блочного симметричного шифрования: «Кузнечик» (128-битный блок) и «Магма» (64-битный блок). **ГОСТ Р 34.11-2012** определяет алгоритм хеширования Стрибог. **ГОСТ Р 34.10-2012** определяет алгоритм формирования и проверки цифровой подписи на основе эллиптических кривых.

На объектах КИИ применение криптографии для защиты информации ограниченного доступа допускается только с использованием **сертифицированных ФСБ России СКЗИ** (средств криптографической защиты информации), реализующих ГОСТ-алгоритмы. Это означает, что использование gpg4win с алгоритмом AES на объекте КИИ формально допустимо только для учебных целей – в боевой системе потребуется сертифицированное СКЗИ.

Практическое задание

Цель работы

Освоить полный практический арсенал прикладной криптографии: вычисление хеш-сумм и исследование свойств хеш-функций, создание и работу с зашифрованными контейнерами VeraCrypt, симметричное шифрование файлов с паролем, генерацию ключевых пар OpenPGP, асимметричное шифрование и расшифровку, а также создание и проверку цифровой подписи с демонстрацией обнаружения фальсификации.

Часть I. Хеш-функции (1,5 часа)

Шаг 1. Создание тестовых файлов

Создайте в папке C:\CryptoLab\ два текстовых файла.

Файл 1 – setpoints.txt – уставки технологического процесса:

Уставки пастеризатора № 1

Дата утверждения: [текущая дата]

Утвердил: главный технолог [ваша фамилия]

Температура пастеризации: 72°C

Время выдержки: 15 сек

Максимальная температура: 78°C

Минимальная температура: 68°C

Давление в системе: 2.5 бар

Скорость конвейера: 0.8 м/с

Файл 2 – plc_config.txt – параметры конфигурации ПЛК:

Конфигурация ПЛК-1 (Siemens S7-1200)

IP-адрес: 192.168.10.10

Маска подсети: 255.255.255.0

Шлюз по умолчанию: 192.168.10.1

Версия прошивки: V4.5.0

Дата последнего обновления: [текущая дата]

Инженер: [ваша фамилия]

Сделайте **скриншот** содержимого папки C:\CryptoLab\ с обоими файлами. Подпишите «Шаг 1 – Тестовые файлы созданы».

Шаг 2. Вычисление хешей с помощью CertUtil

Откройте командную строку и перейдите в рабочую папку:

```
cd C:\CryptoLab
```

Вычислите хеши обоих файлов несколькими алгоритмами и запишите результаты в таблицу отчёта:

```
certutil -hashfile setpoints.txt MD5
certutil -hashfile setpoints.txt SHA256
certutil -hashfile setpoints.txt SHA512
certutil -hashfile plc_config.txt MD5
certutil -hashfile plc_config.txt SHA256
certutil -hashfile plc_config.txt SHA512
```

Обратите внимание на длину хешей: MD5 даёт 32 шестнадцатеричных символа (128 бит), SHA-256 – 64 символа (256 бит), SHA-512 – 128 символов (512 бит). Запишите все значения в таблицу отчёта.

Сохраните эталонные хеши в файл hashes_reference.txt:

```
echo === Эталонные хеши файлов АСУ ТП === > hashes_reference.txt
echo Дата: %date% %time% >> hashes_reference.txt
echo. >> hashes_reference.txt
echo [setpoints.txt] >> hashes_reference.txt
certutil -hashfile setpoints.txt SHA256 >> hashes_reference.txt
echo. >> hashes_reference.txt
echo [plc_config.txt] >> hashes_reference.txt
certutil -hashfile plc_config.txt SHA256 >> hashes_reference.txt
```

Сделайте **скриншот** вывода команд в командной строке. Подпишите «Шаг 2 – Вычисление хешей».

Шаг 3. Исследование свойств хеш-функции

3.1 Лавинный эффект

Откройте setpoints.txt в Блокноте. Измените **одну цифру** в параметре температуры: 72°C → 73°C. Сохраните файл.

Вычислите новый хеш SHA-256:

```
certutil -hashfile setpoints.txt SHA256
```

Запишите новый хеш в таблицу отчёта рядом с эталонным. Подсчитайте вручную, сколько символов в хеше изменилось. Несмотря на изменение одной цифры в тексте (то есть одного символа из нескольких сотен), хеш должен измениться примерно наполовину своих 64 символов.

3.2 Детерминированность

Верните файл к исходному содержимому (73°C → 72°C). Сохраните и вычислите хеш:

```
certutil -hashfile setpoints.txt SHA256
```

Убедитесь, что хеш **точно совпал** с эталонным. Запишите вывод в отчёт.

3.3 Зависимость хеша от регистра и пробелов

Создайте файл test_case.txt со следующим содержимым – просто слово password:

```
echo password > test_case.txt
certutil -hashfile test_case.txt SHA256
```

Затем создайте файл test_case2.txt со словом Password (заглавная буква):

```
echo Password > test_case2.txt
certutil -hashfile test_case2.txt SHA256
```

Сравните хеши. Несмотря на отличие всего в одном бите (регистр буквы p), хеши должны кардинально различаться. Это объясняет, почему пароли password и Password хранятся в базе данных в виде совершенно разных хешей – даже небольшое усложнение пароля полностью меняет его хеш.

Сделайте **скриншот** сравнения всех трёх хешей (эталонный, изменённый, восстановленный) и подпишите «Шаг 3 – Свойства хеш-функции».

Шаг 4. Моделирование контроля целостности конфигурации ПЛК

Смоделируем реалистичный сценарий: системный администратор фиксирует эталонные хеши после авторизованной настройки, затем проверяет их через некоторое время.

«Зафиксируйте» эталонное состояние – хеш файла plc_config.txt уже записан в hashes_reference.txt. Теперь смоделируйте **несанкционированное изменение конфигурации**: откройте plc_config.txt и измените IP-адрес с 192.168.10.10 на 192.168.10.100 – как будто злоумышленник или недобросовестный сотрудник изменил сетевые параметры ПЛК.

Выполните проверку целостности – сравните текущий хеш с эталоном:

```
certutil -hashfile plc_config.txt SHA256
```

Полученный хеш не совпадает с записанным в hashes_reference.txt – несанкционированное изменение обнаружено. В реальной системе это должно автоматически генерировать тревожное событие в журнале безопасности.

Запишите в отчёт: что именно изменилось в файле, как это проявилось в хеше и какие действия должен предпринять ответственный специалист при обнаружении расхождения хешей в реальной АСУ ТП.

Сделайте **скриншот** обоих хешей (эталонного из файла и нового) и подпишите «Шаг 4 – Обнаружение изменения конфигурации».

Часть II. Зашифрованные контейнеры VeraCrypt (1,5 часа)

Шаг 5. Создание зашифрованного контейнера

Запустите VeraCrypt. В главном окне нажмите **«Create Volume»** (создать раздел). Выберите опцию **«Create an encrypted file container»** (создать зашифрованный файловый контейнер).

На следующем шаге выберите **«Standard VeraCrypt volume»** (стандартный контейнер).

Нажмите «Select File» и укажите путь для сохранения контейнера: C:\CryptoLab\scada_backup.vc. Именно так называется файл контейнера – его расширение и имя ничего не говорят о содержимом.

Нажмите «Next». В разделе настроек шифрования выберите:

- Алгоритм шифрования: **AES**
- Хеш-алгоритм: **SHA-512**

Нажмите «Next». Укажите размер контейнера: **10 МБ** (достаточно для учебных целей).

Нажмите «Next». Введите надёжный пароль (не менее 12 символов). Запишите пароль в отчёт.

На странице форматирования произвольно двигайте мышью внутри окна мастера – это генерирует случайные данные для инициализации ключа шифрования. После 30 секунд нажмите «Format». Контейнер будет создан.

Сделайте **скриншот** завершения создания контейнера и подпишите «Шаг 5 – Контейнер создан».

Шаг 6. Монтирование контейнера и работа с файлами

В главном окне VeraCrypt выберите любую свободную букву диска из списка (например, Z:). Нажмите **«Select File»** и укажите C:\CryptoLab\scada_backup.vc. Нажмите **«Mount»** и введите пароль.

После монтирования откройте «Этот компьютер» – вы увидите новый логический диск Z: объёмом 10 МБ. Это и есть ваш расшифрованный контейнер, смонтированный как обычный диск.

Скопируйте в диск Z: оба тестовых файла – setpoints.txt и plc_config.txt – и файл hashes_reference.txt. Убедитесь, что файлы скопировались и открываются как обычные документы.

Теперь размонтируйте контейнер: в главном окне VeraCrypt нажмите **«Dismount»**. Диск Z: исчезнет из системы.

Откройте файл контейнера scada_backup.vc в Блокноте – вы увидите нечитаемый зашифрованный поток данных. Никакого намёка на содержимое файлов нет. Злоумышленник, получивший этот файл без пароля, не сможет извлечь из него никакой

информации.

Сделайте **два скриншота**: смонтированный диск Z: с файлами в «Проводнике» («Шаг 6 – Контейнер смонтирован») и содержимое файла контейнера в Блокноте («Шаг 6 – Зашифрованное содержимое»).

Шаг 7. Проверка защиты контейнера от неверного пароля

Попробуйте смонтировать контейнер с **неверным паролем**: в VeraCrypt снова выберите файл scada_backup.vc, нажмите «Mount» и введите заведомо неверный пароль. VeraCrypt откажет в монтировании с сообщением об ошибке.

Запишите в отчёт: почему VeraCrypt не просто «запрещает доступ», а не может смонтировать контейнер вовсе – в чём принципиальное отличие от простой парольной защиты? (Подсказка: при неверном пароле расшифрованные данные выглядят как случайный шум – система не может отличить «неверный пароль» от «файл повреждён».)

Сделайте **скриншот** ошибки монтирования и подпишите «Шаг 7 – Защита от неверного пароля».

Часть III. Симметричное шифрование файлов (45 минут)

Шаг 8. Шифрование файла с паролем в Kleopatra

Откройте **Kleopatra** (входит в gpg4win). Перейдите в меню **Tools → Encrypt Files...** и выберите файл C:\CryptoLab\setpoints.txt.

В появившемся окне выберите режим **«Encrypt with password»** (зашифровать с паролем, без использования ключей OpenPGP). Нажмите «Next» и введите пароль шифрования – не менее 12 символов. Запишите пароль в отчёт.

После шифрования в папке C:\CryptoLab\ появится файл setpoints.txt.gpg. Откройте его в Блокноте – текст с уставками полностью нечитаем, заменён на зашифрованные данные.

Расшифровка

В Kleopatra выберите **Tools → Decrypt/Verify Files...**, укажите файл setpoints.txt.gpg и введите пароль. Файл расшифруется и откроется в текстовом редакторе. Убедитесь, что содержимое полностью совпадает с исходным.

Демонстрация защиты при неверном пароле

Попробуйте расшифровать с неверным паролем – Kleopatra откажет с сообщением об ошибке аутентификации.

Сделайте **три скриншота**: зашифрованный файл в Блокноте («Шаг 8 –

Шифртекст»), успешная расшифровка («Шаг 8 – Успешная расшифровка»), ошибка при неверном пароле («Шаг 8 – Ошибка расшифровки»).

Часть IV. Асимметричное шифрование и цифровая подпись (2,5 часа)

Шаг 9. Генерация ключевой пары OpenPGP

В Kleopatra нажмите **«New Key Pair»**. Выберите **«Create a personal OpenPGP key pair»**.

Введите данные:

- **Name:** ваша фамилия и имя;
- **Email:** учебный адрес электронной почты.

Нажмите **«Advanced Settings»**. Установите:

- Алгоритм: **RSA**
- Длина ключа: **4096 бит**
- Срок действия: **1 год** (в реальных системах устанавливается ограниченный срок действия ключей).

Нажмите «Create». Введите **парольную фразу** для защиты закрытого ключа – не менее 15 символов, включая буквы, цифры и специальные символы. Запишите парольную фразу в отчёт.

После генерации Kleopatra покажет **отпечаток ключа (Fingerprint)** – уникальный идентификатор длиной 40 шестнадцатеричных символов (160 бит). Запишите его в отчёт – именно по отпечатку проверяется подлинность ключа при его публичном распространении.

Экспорт открытого ключа

Щёлкните правой кнопкой по ключу в списке → **«Export»**. Сохраните файл как `my_public_key.asc` в папке `C:\CryptoLab\`.

Откройте `my_public_key.asc` в Блокноте. Вы увидите текстовый блок:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
mQINBGXr...
...
-----END PGP PUBLIC KEY BLOCK-----
```

Это и есть открытый ключ в формате ASCII Armor – именно в таком виде он публикуется, отправляется коллегам и размещается на серверах ключей. Объясните в отчёте: почему этот ключ можно передавать по открытым каналам без ущерба для

безопасности?

Сделайте **скриншот** главного окна Kleopatra с созданной ключевой парой и подпишите «Шаг 9 – Ключевая пара создана».

Шаг 10. Имитация взаимодействия двух сторон

Для полноценной демонстрации асимметричного шифрования необходимо смоделировать взаимодействие двух участников – отправителя (Инженер А) и получателя (Инженер Б). Выполняйте шаги последовательно, «переключаясь» между ролями.

10.1 Создание второй ключевой пары (роль «Инженер Б»)

Создайте вторую ключевую пару в Kleopatra с другим именем – например, «Диспетчер» и другим email-адресом. Используйте те же параметры: RSA-4096. Установите другую парольную фразу и запишите её в отчёт.

Экспортируйте открытый ключ второй пары в файл dispatcher_public_key.asc.

10.2 Шифрование для «Инженера Б» (роль «Инженер А»)

Теперь «Инженер А» хочет отправить файл с уставками «Инженеру Б» так, чтобы никто посторонний не мог его прочитать. Для этого он импортирует открытый ключ «Инженера Б».

В Kleopatra нажмите **«Import»** и импортируйте файл dispatcher_public_key.asc. Теперь в списке ключей Kleopatra появятся обе пары.

Выберите **Tools → Encrypt Files...**, укажите setpoints.txt. В следующем окне выберите опцию шифрования **с использованием ключей OpenPGP** (не с паролем). В списке получателей выберите ключ «Диспетчер». Нажмите «Encrypt».

Появится файл setpoints.txt.gpg – зашифрованный для «Инженера Б». Попробуйте расшифровать его ключом «Инженера А» – получите ошибку: файл зашифрован не для этого ключа. Расшифровать его может только «Инженер Б» своим закрытым ключом.

10.3 Расшифровка «Инженером Б»

В Kleopatra выберите **Tools → Decrypt/Verify Files...**, укажите setpoints.txt.gpg. Kleopatra автоматически определит, что файл предназначен для ключа «Диспетчер», и попросит ввести его парольную фразу. Введите парольную фразу второй ключевой пары. Файл успешно расшифруется.

Сделайте **три скриншота**: успешное шифрование («Шаг 10 – Файл зашифрован»), ошибка расшифровки чужим ключом («Шаг 10 – Ошибка: чужой ключ»), успешная расшифровка правильным ключом («Шаг 10 – Успешная расшифровка»).

Шаг 11. Создание и проверка цифровой подписи

11.1 Подписание документа

Восстановите файл setpoints.txt к исходному содержимому (температура 72°C). В Kleopatra выберите **Tools → Sign/Encrypt Files...**, укажите файл.

В следующем окне установите **только флажок «Sign»** (подписать), флажок «Encrypt» снимите – создаём именно подпись, без шифрования содержимого. Выберите ключ «Инженер А» (первая пара) как источник подписи. Введите парольную фразу первой пары.

В папке появится файл setpoints.txt.sig. Откройте его в Блокноте:

```
-----BEGIN PGP SIGNATURE-----
...
-----END PGP SIGNATURE-----
```

Запишите в отчёт: что именно содержится в файле .sig с криптографической точки зрения? (Ответ: зашифрованный закрытым ключом хеш файла setpoints.txt.) Почему файл .sig не содержит исходного текста документа?

11.2 Проверка подлинной подписи

В Kleopatra выберите **Tools → Decrypt/Verify Files...**, укажите файл setpoints.txt.sig. Kleopatra найдёт соответствующий файл setpoints.txt, расшифрует подпись открытым ключом «Инженера А», вычислит хеш файла и сравнит.

Результат: **«Valid signature»** – подпись верна. В описании результата будет указано имя и email подписавшего, дата и время подписания.

Сделайте **скриншот** результата и подпишите «Шаг 11.1 – Подпись верна».

11.3 Обнаружение фальсификации документа

Откройте setpoints.txt в Блокноте и **намеренно измените критический параметр**: снизьте температуру пастеризации с 72°C до 55°C – ниже порога безопасной пастеризации. Сохраните файл. Не переподписывайте.

Снова выполните проверку подписи: **Tools → Decrypt/Verify Files... →** setpoints.txt.sig.

Результат: **«Bad signature»** – подпись недействительна. Kleopatra обнаружила, что хеш изменённого файла не совпадает с хешем, зашифрованным в подписи при создании. Документ был изменён после подписания.

В отчёте опишите этот сценарий применительно к АСУ ТП: злоумышленник получил доступ к файлу уставок, снизил температуру пастеризации до небезопасного

уровня и отправил изменённый файл оператору как «новые рабочие инструкции». Цифровая подпись немедленно выявила бы фальсификацию.

Сделайте **скриншот** результата с недействительной подписью и подпишите «Шаг 11.2 – Фальсификация обнаружена».

11.4 Подписание и шифрование одновременно

Восстановите файл setpoints.txt к исходному содержимому. Выполните **одновременно подписание и шифрование**: в Kleopatra установите оба флажка – «Sign» (ключ «Инженер А») и «Encrypt» (для получателя «Диспетчер»).

Полученный файл одновременно зашифрован (конфиденциальность – только «Диспетчер» может прочитать) и подписан (аутентичность и целостность – «Диспетчер» может убедиться, что файл от «Инженера А» и не изменялся).

Расшифруйте и проверьте подпись: **Tools → Decrypt/Verify Files...**. Kleopatra одновременно расшифрует файл и проверит подпись, отобразив оба результата.

Сделайте **скриншот** совместного результата расшифровки и проверки подписи и подпишите «Шаг 11.3 – Шифрование и подпись одновременно».

Часть V. Итоговый анализ: комплексная защита файла прошивки ПЛК (1 час)

Шаг 12. Моделирование реального сценария: защита обновления прошивки

Смоделируем реальный производственный сценарий: **инженер-интегратор** разрабатывает обновление прошивки ПЛК и должен передать его оператору предприятия, обеспечив:

1. **Конфиденциальность** – прошивка не должна быть перехвачена конкурентами;
2. **Целостность** – оператор должен убедиться, что файл не изменялся при передаче;
3. **Аутентичность** – оператор должен убедиться, что файл действительно от интегратора, а не от злоумышленника.

Создайте файл firmware_v2.1.txt, имитирующий прошивку:

```
Прошивка ПЛК-1 версия 2.1
Дата релиза: [текущая дата]
Разработчик: ООО «Интегратор» ([ваша фамилия])
Изменения в версии 2.1:
- Исправлена ошибка переполнения буфера в модуле ПИД-регулятора
```

- Добавлена защита от несанкционированного изменения уставок

- Оптимизирован алгоритм аварийного останова

SHA256 предыдущей версии (v2.0): [впишите любой хеш из предыдущих шагов]

Сохраните файл в C:\CryptoLab\.

Выполнение защищённой передачи

Шаг А. Вычислите хеш файла прошивки и запишите в отчёт:

certutil -hashfile firmware_v2.1.txt SHA256

Шаг Б. Подпишите файл ключом «Инженер А» (роль: интегратор) и зашифруйте для получателя «Диспетчер» (роль: оператор предприятия) одновременно.

Шаг В. «Оператор» получает зашифрованный файл. Расшифровывает его своим ключом и проверяет подпись. Убеждается: файл от «Интегратора», не изменялся.

Шаг Г. Дополнительно проверьте целостность через хеш: вычислите хеш расшифрованного файла и сравните с эталоном из Шага А. Хеши должны совпасть.

Опишите в отчёте: каждый из четырёх шагов – какую криптографическую задачу он решает и какой механизм использует.

Сделайте **скриншот** финального результата и подпишите «Шаг 12 – Комплексная защита прошивки».

Содержание отчёта

Отчёт оформляется в MS Word объёмом 12–15 страниц.

1. Часть I. Хеш-функции – таблица хешей, анализ свойств, описание сценария обнаружения изменения конфигурации ПЛК:

Файл	MD5	SHA-256	SHA-512
setpoints.txt (исходный)			
setpoints.txt (изменённый)			
setpoints.txt (восстановленный)			
plc_config.txt (исходный)			
plc_config.txt (изменённый)			

2. Часть II. VeraCrypt – скриншоты, ответ на вопрос о защите при неверном пароле.

3. Часть III. Симметричное шифрование – скриншоты, объяснение главного ограничения симметричного шифрования.

4. Часть IV. Асимметричное шифрование и цифровая подпись – все скриншоты, характеристики ключевых пар (таблица), описание всех проверенных сценариев:

Сценарий	Результат Kleopatra	Объяснение
Проверка подлинной подписи		

Проверка подписи изменённого файла		
Расшифровка своим ключом		
Расшифровка чужим ключом		

5. Часть V. Итоговый сценарий – описание всех четырёх шагов с указанием: задача → механизм → результат.

6. Ответы на контрольные вопросы.

7. Вывод – 5–7 предложений о том, как рассмотренные механизмы образуют комплексную систему криптографической защиты АСУ ТП.

Контрольные вопросы

1. Хеш-функция необратима: зная хеш, нельзя восстановить исходные данные. При этом хеши паролей хранятся в базах данных. Объясните, как злоумышленник, получивший базу с хешами паролей, всё равно может узнать пароли (атака по словарю, радужные таблицы). Какая дополнительная мера при хешировании паролей нейтрализует эти атаки?

2. Объясните разницу между шифрованием файла с паролем (симметричное) и шифрованием для получателя с открытым ключом (асимметричное). В каком случае каждый из подходов предпочтительнее?

3. В шаге 10.2 вы убедились, что файл, зашифрованный открытым ключом «Инженера Б», нельзя расшифровать ключом «Инженера А». Объясните математический смысл этого свойства: почему знание открытого ключа не позволяет расшифровать зашифрованное им сообщение?

4. Производитель SCADA-системы публикует на сайте обновление и SHA-256 хеш. Злоумышленник взломал сайт и подменил файл обновления на вредоносный, но не изменил опубликованный хеш. Защитит ли проверка хеша в этом случае? Что должен дополнительно публиковать производитель?

5. Объясните, почему зашифрованный контейнер VeraCrypt **не может** быть «частично расшифрован» злоумышленником, знающим часть пароля – в отличие, например, от архива ZIP с паролем, в котором можно перебирать символы по очереди.