МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНСТИТУТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И АНАЛИЗА ДАННЫХ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

КУРСОВОЕ ПРОЕКТИРОВАНИЕ 1

Анализ уязвимостей и защищённости внутренней инфраструктуры крупных производственных предприятий

Студент _____ _____ А.П. Панин

Руководитель
канд. экон. наук, доцент _____ Е.Г. Шумик

Нормоконтролер
канд. экон. наук, доцент _____ Е.Г. Шумик
(нормоконтролер руководитель)

Владивосток 2026

Содержание

Введение

В настоящее время деятельность крупных производственных предприятий тесно связана с использованием информационных технологий. Корпоративные сети, серверное оборудование, автоматизированные системы управления технологическими процессами и специализированное программное обеспечение обеспечивают выполнение производственных и управленческих задач. Неизбежно с расширением цифровой инфраструктуры возрастает количество угроз, связанных с нарушением её безопасности.

Практика последних лет показывает, что промышленные предприятия всё чаще становятся объектами кибератак. Причиной этого является как высокая ценность обрабатываемой информации, так и наличие технологических систем, нарушение работы которых способно привести к значительным финансовым потерям. В ряде случаев последствия инцидентов информационной безопасности выходят за пределы отдельной организации и затрагивают производственные цепочки, поставщиков и потребителей продукции.

Особенностью производственных предприятий является наличие не только стандартных информационных систем, но и промышленных сегментов сети, включающих АСУ ТП, SCADA-системы и оборудование автоматизации. Многие из таких систем были разработаны без учёта современных требований кибербезопасности, что делает их потенциальной целью для злоумышленников.

В связи с этим особую актуальность приобретает анализ защищённости внутренней инфраструктуры предприятия. Выявление уязвимостей позволяет своевременно определить слабые места информационной системы, оценить возможные риски и разработать меры по их снижению.

Целью курсовой работы является исследование уязвимостей внутренней инфраструктуры крупных производственных предприятий и разработка рекомендаций по повышению уровня её защищённости.

Для достижения поставленной цели необходимо решить следующие задачи:

- рассмотреть основные понятия информационной безопасности
- изучить основные виды уязвимостей внутренней инфраструктуры предприятий
- проанализировать существующие методы и средства оценки защищённости
- исследовать нормативные документы и стандарты в области информационной безопасности
- провести анализ тестовой инфраструктуры предприятия
- разработать рекомендации по повышению уровня защищённости

Объектом исследования является внутренняя инфраструктура производственного предприятия.

Предметом исследования выступают уязвимости информационных систем, методы их выявления и способы повышения защищённости инфраструктуры.

Практическая значимость работы заключается в возможности применения полученных результатов при оценке защищённости корпоративных сетей и планировании мероприятий по обеспечению информационной безопасности предприятий.

1. Теоретические основы анализа уязвимостей и защищённости внутренней инфраструктуры предприятий

1.1. Основные понятия информационной безопасности

Внутренняя инфраструктура крупных производственных предприятий представляет собой сложную многоуровневую систему. Использование автоматизированных систем управления, корпоративных сетей, баз данных, облачных технологий и цифровых платформ значительно повышает эффективность производственных процессов, а также позволяет оптимизировать управление ресурсами и улучшать качество выпускаемой продукции.

Однако одновременно с развитием цифровизации возрастает и количество угроз, связанных с нарушением безопасности информационной инфраструктуры предприятий.

Информационная безопасность, согласно ГОСТу Р 53114-200: “Состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность”. [п. 3.1.1]

Конфиденциальность подразумевает защиту информации от несанкционированного доступа. Для производственных предприятий обеспечение конфиденциальности имеет особое значение, поскольку во внутренней инфраструктуре могут храниться технологические разработки, коммерческие данные, сведения о производственных процессах, персональные данные сотрудников и другая важная информация. Разглашение подобной информации приведёт к снижению конкурентоспособности предприятия, большому финансовому и репутационному ущербу.

Целостность – это свойство информации, которое означает что исходные данные не были изменены. Результатами нарушения целостности являются: ошибки в работе систем предприятия, создание аварийных ситуаций, повреждение оборудования, возможность появления канала утечки информации, а также возможно причинение вреда человеку. Поэтому обеспечению целостности информации следует уделять особое внимание, из-за последствий описанных выше.

Доступность – это ничто иное как, возможность получения пользователями информации и ресурсов в соответствии с предоставленными им правами доступа без неоправданных ограничений. Для производственных предприятий доступность информационных систем, несомненно, важна, так как остановка производственных процессов из-за нарушения доступности способна привести к тем же последствиям, что и нарушение целостности, как было описано ранее.

Одним из ключевых понятий в области информационной безопасности является угроза безопасности информации. Как правило это условия и факторы, создающие потенциальную возможность нанесения различного ущерба информационной системе или

инфраструктуре предприятия. Угрозы могут иметь как внешний, так и внутренний характер.

К внешним угрозам относятся действия злоумышленников, хакерские атаки, распространение вредоносного программного обеспечения, сетевые атаки, промышленный шпионаж и другие воздействия, осуществляемые извне организации. В последние годы наблюдается рост числа целенаправленных атак на промышленные предприятия, связанных с использованием программ-вымогателей, фишинговых рассылок и эксплуатации уязвимостей промышленного оборудования, а также социальной инженерии.

Внутренние угрозы связаны с действиями сотрудников предприятия, ошибками персонала, нарушением регламентов безопасности, халатностью или умышленными действиями работников.

Согласно исследованиям в области информационной безопасности, человеческий фактор остаётся одной из наиболее распространённых причин возникновения инцидентов безопасности. Неправильная настройка оборудования, использование слабых паролей, подключение несанкционированных устройств и несоблюдение политики безопасности могут привести к компрометации внутренней инфраструктуры.

И, к сожалению, подобные случаи происходят, так как нередко предприятия пренебрегают безопасностью, а причинами этого могут быть: ограниченность бюджета, отсутствие квалифицированных специалистов, отсутствие контроля, а также человеческий фактор.

Неотъемлемой частью анализа защищённости является понятие уязвимости. Уязвимость – это уже возможность, способствующая возникновению угрозы. Другими словами – недостаток или слабое место в программном обеспечении, оборудовании, сетевой архитектуре либо организационных процессах, которое может быть использовано злоумышленником для реализации угрозы.

Появляются они вследствие ошибок разработчиков программного обеспечения, неправильной конфигурации систем, отсутствия обновлений безопасности, недостаточной компетентности сотрудников или неполого контроля доступа.

На крупных производственных предприятиях особую опасность представляют уязвимости автоматизированных систем управления технологическими процессами. Многие промышленные системы разрабатывались без учёта современных требований кибербезопасности, поскольку изначально функционировали в изолированных сетях. Однако с развитием цифровых технологий и подключением производственных систем к корпоративным сетям и интернету уровень риска значительно возрос.

Среди наиболее распространённых видов уязвимостей можно выделить:

- программные уязвимости
- сетевые уязвимости
- уязвимости операционных систем
- ошибки конфигурации оборудования
- недостатки систем аутентификации
- недостаточная компетентность сотрудника
- уязвимости, возникающие из-за человеческого фактора

Для реализации угроз злоумышленники используют различные каналы проникновения во внутреннюю инфраструктуру предприятия. Одним из наиболее распространённых способов является фишинг — метод социальной инженерии, при котором сотрудникам отправляются поддельные электронные письма или сообщения с целью получения конфиденциальной информации либо установки вредоносного программного обеспечения.

Кроме того, значительную угрозу представляют сетевые атаки, направленные на эксплуатацию открытых портов, уязвимостей сетевых протоколов и недостатков системы защиты периметра предприятия. В ряде случаев злоумышленники получают доступ к внутренним ресурсам через удалённые сервисы, плохо защищённые VPN-соединения или устройства сотрудников, работающих удалённо.

В настоящее время большинство производственных процессов так или иначе связано с использованием информационных систем. Нарушение их работы может привести не только к финансовым потерям, но и к остановке отдельных участков производства. По этой причине предприятиям необходимо регулярно проводить анализ угроз и уязвимостей, а также совершенствовать существующие меры защиты информации.

Это требует комплексного подхода к обеспечению информационной безопасности, включающего технические, организационные и программные меры защиты. Анализ угроз и уязвимостей позволяет своевременно выявлять слабые места системы безопасности, минимизировать вероятность реализации атак и обеспечивать стабильное функционирование предприятия.

1.2. Типы уязвимостей во внутренней инфраструктуре предприятий

Внутренняя инфраструктура крупных производственных предприятий представляет собой сложную многоуровневую систему, включающую серверное оборудование, локальные вычислительные сети, автоматизированные системы управления технологическими процессами, базы данных, рабочие станции сотрудников, системы удалённого доступа и специализированное промышленное оборудование. Высокая степень

взаимосвязанности всех компонентов инфраструктуры обеспечивает эффективность производственных процессов, однако одновременно создаёт большое количество потенциальных уязвимостей, которые могут быть использованы злоумышленниками для реализации кибератак.

Под уязвимостью понимается слабое место в программном обеспечении, оборудовании, сетевой архитектуре или организационной структуре предприятия, которое способно привести к нарушению конфиденциальности, целостности или доступности информации. Наличие уязвимостей существенно снижает уровень защищённости внутренней инфраструктуры и повышает риск возникновения инцидентов информационной безопасности.

Одной из наиболее распространённых категорий являются сетевые уязвимости. Современные предприятия используют разветвлённые корпоративные сети, объединяющие различные подразделения, филиалы и производственные объекты. При недостаточном уровне защиты сетевой инфраструктуры злоумышленники могут получить несанкционированный доступ к внутренним ресурсам предприятия. Что могут подтвердить многочисленные инциденты, которые фиксировались в ГосСОПКА – государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы, когда незащищённое сетевое соединение приводило к утечке логинов, паролей и другой важной информации в открытый доступ.

К сетевым уязвимостям относятся:

- использование устаревших сетевых протоколов
- наличие открытых портов и сервисов
- ошибки конфигурации маршрутизаторов и коммутаторов
- отсутствие сегментации сети
- недостаточная защита удалённого доступа
- использование небезопасных VPN-соединений
- отсутствие или слабое шифрование каналов связи

Особую опасность представляет отсутствие разделения корпоративной сети и производственного сегмента. В случае компрометации офисной сети злоумышленники могут получить доступ к системам управления технологическими процессами, что способно привести к остановке производства или нарушению работы оборудования.

Важным типом уязвимостей являются программные уязвимости. Практически все современные производственные предприятия используют большое количество программного обеспечения: операционные системы, серверные платформы, ERP-системы, SCADA-системы, базы данных и специализированные приложения для управления

производством. Ошибки в коде программ, отсутствие своевременных обновлений и использование устаревших версий программного обеспечения создают благоприятные условия для проведения атак.

Программные уязвимости могут включать:

- ошибки в механизмах аутентификации
- переполнение буфера
- уязвимости веб-приложений
- недостатки систем шифрования
- ошибки обработки пользовательских данных
- возможность удалённого выполнения кода

Многие атаки происходят с уже известными уязвимостями, сведения о которых публикуются в отрытом доступе. Для решения этой проблемы был создан язык описания уязвимостей – OVAL (Open Vulnerability and Assessment Language), который использует один из инструментов анализа уязвимостей, рассматриваемых в рамках данной работы – ScanOVAL.

Если предприятие не обновляет программное обеспечение своевременно, риск компрометации инфраструктуры значительно возрастает.

Отдельно следует рассмотреть уязвимости операционных систем и серверной инфраструктуры. Серверы являются основой информационной системы предприятия, поскольку на них размещаются базы данных, корпоративные сервисы, файловые хранилища и другие критически важные ресурсы. Любые ошибки в настройке серверов способны привести к снижению уровня защищённости всей инфраструктуры.

На практике наиболее распространёнными проблемами являются использование слабых паролей, наличие стандартных учётных записей, отсутствие разграничения прав доступа и несвоевременная установка обновлений безопасности. Кроме того, на некоторых предприятиях до сих пор эксплуатируются устаревшие операционные системы, поддержка которых уже прекращена разработчиками. Подобная ситуация часто возникает из-за необходимости использования специализированного программного обеспечения, несовместимого с современными версиями операционных систем. Однако использование устаревших решений значительно повышает риск успешной эксплуатации известных уязвимостей.

Особое место занимают уязвимости промышленного оборудования и автоматизированных систем управления технологическими процессами. В отличие от обычных информационных систем, АСУ ТП и SCADA-системы напрямую связаны с

производственным оборудованием и обеспечивают управление технологическими процессами предприятия.

Многие промышленные системы были разработаны в период, когда вопросы кибербезопасности не являлись приоритетными. Предполагалось, что подобные системы будут функционировать в изолированных сетях без подключения к внешним ресурсам. Однако в настоящее время производственные сегменты всё чаще интегрируются с корпоративными сетями, а в отдельных случаях получают доступ к сети Интернет. В результате такие системы становятся потенциальной целью для злоумышленников.

Среди наиболее распространённых проблем промышленной инфраструктуры можно выделить использование стандартных паролей, отсутствие механизмов аутентификации, применение устаревших версий прошивок, передачу данных без шифрования и недостаточную защиту специализированных промышленных протоколов. Опасность подобных уязвимостей заключается в том, что последствия атак могут выражаться не только в утечке информации, но и в нарушении работы оборудования, остановке производственных процессов или возникновении аварийных ситуаций.

Значительное влияние на уровень защищённости предприятия оказывает человеческий фактор. Несмотря на постоянное развитие средств защиты информации, ошибки сотрудников по-прежнему остаются одной из наиболее частых причин возникновения инцидентов информационной безопасности. Нередко причиной компрометации инфраструктуры становится использование простых паролей, открытие подозрительных вложений в электронных письмах, передача учётных данных другим лицам или нарушение установленных требований безопасности.

Особую опасность представляют методы социальной инженерии. Злоумышленники используют различные способы психологического воздействия на сотрудников, пытаясь получить доступ к конфиденциальной информации или внутренним ресурсам организации. Наиболее распространёнными примерами являются фишинговые письма, телефонное мошенничество и поддельные сообщения от имени руководства либо технической поддержки.

Не менее важную роль играют организационные уязвимости. Даже при наличии современных технических средств защиты недостатки в управлении информационной безопасностью могут существенно снизить уровень защищённости предприятия. К таким недостаткам относятся отсутствие политики информационной безопасности, нерегулярное проведение аудитов, недостаточный контроль действий пользователей, отсутствие резервного копирования данных и формализованных процедур реагирования на инциденты.

В последние годы дополнительное внимание уделяется вопросам безопасности удалённого доступа и облачных сервисов. Распространение дистанционной работы потребовало предоставления сотрудникам доступа к корпоративным ресурсам из внешних сетей. При неправильной настройке удалённого доступа злоумышленники могут использовать подобные каналы для проникновения во внутреннюю инфраструктуру предприятия.

Таким образом, уязвимости внутренней инфраструктуры производственных предприятий могут иметь различную природу и затрагивать как технические средства, так и организационные процессы. Для снижения уровня риска необходимо регулярно проводить анализ защищённости, своевременно устранять выявленные недостатки и совершенствовать существующую систему информационной безопасности.

1.3. Методы и инструменты анализа уязвимостей

В условиях активного развития цифровых технологий и увеличения количества киберугроз обеспечение безопасности внутренней инфраструктуры крупных производственных предприятий становится одной из приоритетных задач. Для своевременного выявления слабых мест информационных систем и предотвращения возможных атак используются различные методы и инструменты анализа уязвимостей. Их применение позволяет оценить уровень защищённости инфраструктуры, определить потенциальные угрозы и разработать меры по минимизации рисков.

Анализ уязвимостей представляет собой комплекс мероприятий, направленных на поиск недостатков в программном обеспечении, сетевой инфраструктуре, системах управления и организационных процессах предприятия. Главной целью анализа является выявление потенциальных точек проникновения злоумышленников и предотвращение реализации угроз информационной безопасности.

Современные методы анализа уязвимостей подразделяются на технические, организационные и комбинированные. На практике наиболее эффективным считается комплексный подход, при котором используются сразу несколько методов оценки защищённости.

Одним из наиболее распространённых способов выявления уязвимостей является автоматизированное сканирование информационных систем. Данный подход позволяет быстро получить сведения о состоянии серверов, рабочих станций и сетевого оборудования, определить наличие известных уязвимостей, ошибок конфигурации и потенциально опасных сетевых сервисов.

Практическая ценность сканирования заключается в возможности регулярного контроля состояния инфраструктуры без необходимости проведения трудоёмких ручных проверок. Однако следует учитывать, что автоматизированные средства в первую очередь ориентированы на поиск известных проблем безопасности и не всегда способны выявить сложные логические ошибки или недостатки организационного характера. Поэтому результаты сканирования обычно рассматриваются как один из этапов комплексного анализа защищённости.

Для проведения сканирования используются инструменты анализа уязвимостей. Одними из наиболее популярных решений являются:

- ScanOVAL
- Сканер ВС

Для сравнения в работе также используется инструмент с открытым исходным кодом — Nmap. Выбор данных средств прежде всего обусловлен их доступностью и эффективностью. Также они являются наиболее популярными среди специалистов по информационной безопасности, в том числе благодаря качествам, описанным в предыдущем предложении.

ScanOVAL представляет собой средство проверки конфигураций и поиска уязвимостей, основанное на стандарте OVAL (Open Vulnerability and Assessment Language).

Стандарт OVAL предназначен для формализованного описания:

- уязвимостей
- параметров конфигурации
- состояния операционной системы

В отличие от большинства сканеров, ScanOVAL ориентирован преимущественно на локальный анализ состояния системы и используется для анализа защищённости рабочих станций и серверов, проверки корректности настроек безопасности, а также наличия обновлений и исправлений безопасности. Таким образом его можно применять для: анализа защищённости рабочих станций и серверов, проверки корректности настроек безопасности, проверки наличия обновлений и исправлений безопасности.

Также ScanOVAL позволяет выявлять:

- отсутствие необходимых обновлений
- наличие известных уязвимостей
- ошибки конфигурации
- К преимуществам ScanOVAL относятся:
- высокая точность проверок
- простота в использовании на различных операционных системах

- стандартизованный подход к анализу безопасности
- удобное формирование отчёта о результатах проверки

Недостатками являются:

- необходимость наличия доступа к проверяемым узлам
- ограниченные возможности сетевого анализа

Сканер ВС представляет собой специализированное средство анализа защищённости вычислительных систем, ориентированное на использование в защищённых и изолированных инфраструктурах. Основной функционал системы включает:

- анализ конфигурации операционных систем
- проверку параметров безопасности
- поиск уязвимостей
- контроль обновлений
- анализ прав доступа и политик безопасности

Данную систему используют как: локальное средство аудита, сетевой сканер, а также средство автоматизированного устранения уязвимостей.

Особенностью Сканера ВС является ориентация на требования российских регуляторов в области информационной безопасности. Многие решения данного класса обладают:

- сертификацией ФСТЭК
- поддержкой отечественных операционных систем
- возможностью работы в изолированных сегментах
- локальными базами проверок
- поддержкой требований ГОСТ

К преимуществам системы относятся:

- возможность эксплуатации в закрытых сетях
- поддержка российских стандартов безопасности
- Недостатками являются:
- необходимость запуска как отдельной операционной системы
- менее развитый пользовательский интерфейс
- меньшая экосистема по сравнению с зарубежными платформами

В данной работе используется демоверсия данного приложения, поэтому часть функционала недоступна.

Nmap (Network Mapper) — это свободно распространяемый инструмент для анализа компьютерных сетей и аудита информационной безопасности. Программа предназначена для обнаружения активных узлов сети, определения открытых портов, выявления

работающих сетевых служб, определения версий программного обеспечения и операционных систем.

Nmap является одним из наиболее популярных инструментов сетевой разведки и широко применяется специалистами по информационной безопасности, системными администраторами и аудиторами безопасности.

Разработчиком программы является американский специалист в области информационной безопасности Gordon Lyon, более известный под псевдонимом Fyodor. Проект был впервые представлен в 1997 году и с тех пор активно развивается сообществом разработчиков.

Исходный код Nmap распространяется в открытом доступе, что позволяет использовать программу как в образовательных целях, так и для решения профессиональных задач по анализу защищённости информационных систем.

Основным назначением Nmap является сбор информации о сетевой инфраструктуре. Помимо этого, Nmap способен выполнять определение операционной системы удалённого узла на основе анализа особенностей сетевого стека TCP/IP.

К основным преимуществам Nmap относятся:

- свободное распространение и открытый исходный код
- поддержка операционных систем Windows, Linux и macOS
- возможность определения версий сетевых служб и операционных систем
- поддержка различных методов сканирования и обнаружения хостов
- возможность глубокой настройки анализа через сценарии и командную строку

Несмотря на значительные преимущества, Nmap имеет ряд недостатков. В первую очередь программа не является полноценным сканером уязвимостей и в большинстве случаев требует дополнительного анализа полученных результатов.

Для эффективного использования Nmap пользователю необходимо обладать знаниями сетевых технологий и принципов функционирования протоколов TCP/IP и уметь пользоваться командной строкой. Также при сканировании крупных сетей может возникать значительная нагрузка на сетевую инфраструктуру и исследуемые узлы.

Тем не менее, данный продукт особенно популярен среди специалистов по информационной безопасности.

Ниже представлена таблица 1.1 со сравнением перечисленных средств анализа защищённости.

Таблица 1.1 – Сравнительная характеристика средств анализа защищённости.

Средство анализа	Назначение	Особенности

ScanOVAL	Проверка конфигурации и поиск уязвимостей ОС	Локальный анализ на основе стандарта OVAL
Сканер ВС	Анализ защищённости информационных систем	Поддержка российских требований и изолированных сред
Nmap	Исследование сетевой инфраструктуры	Поиск активных узлов, портов и сетевых сервисов

Как мы можем увидеть, что каждое из этих средств имеет различные особенности и назначение, так как каждое из этих средств создавалось под свою задачу.

Важным методом анализа защищённости является тестирование на проникновение, или пентест. Данный подход предполагает моделирование действий реального злоумышленника с целью проверки устойчивости информационной системы к атакам. В отличие от обычного сканирования, пентест позволяет оценить возможность практической эксплуатации выявленных уязвимостей и определить потенциальные последствия успешной атаки.

Тестирование на проникновение может проводиться как внешними специалистами, так и внутренними подразделениями информационной безопасности предприятия. В процессе тестирования специалисты анализируют сетевую инфраструктуру, проверяют механизмы аутентификации, исследуют защищённость веб-приложений, серверов и систем удалённого доступа.

Пентест включает несколько основных этапов:

1. Сбор информации об инфраструктуре предприятия.
2. Анализ сетевой архитектуры и выявление потенциальных уязвимостей.
3. Попытка эксплуатации обнаруженных слабых мест.
4. Получение доступа к внутренним ресурсам.
5. Подготовка отчёта с рекомендациями по устранению проблем.

Преимуществом тестирования на проникновение является возможность оценки реального уровня защищённости системы.

Однако проведение качественного пентеста требует высокой квалификации специалистов и значительных временных затрат. В процессе анализа защищённости широко применяется аудит информационной безопасности. Аудит представляет собой комплексную проверку состояния системы защиты информации на соответствие установленным требованиям и стандартам безопасности. В отличие от технического анализа уязвимостей, аудит охватывает не только программные и аппаратные компоненты, но и организационные аспекты обеспечения безопасности.

В рамках аудита проводится:

- анализ политики информационной безопасности

- проверка системы разграничения доступа
- оценка эффективности антивирусной защиты
- анализ механизмов резервного копирования
- проверка журналов событий безопасности
- оценка готовности к реагированию на инциденты

Аудит позволяет выявить недостатки в организации системы защиты информации и определить направления её совершенствования. Одним из наиболее эффективных способов выявления угроз является мониторинг событий информационной безопасности. Для этих целей используются системы класса SIEM (Security Information and Event Management). Такие системы обеспечивают централизованный сбор и анализ событий безопасности, поступающих с серверов, рабочих станций, сетевого оборудования и средств защиты информации.

SIEM-системы позволяют:

- обнаруживать подозрительную активность
- выявлять попытки несанкционированного доступа
- анализировать действия пользователей
- фиксировать сетевые атаки
- автоматически уведомлять специалистов о возникновении инцидентов

Использование SIEM особенно важно для крупных производственных предприятий, инфраструктура которых включает большое количество взаимосвязанных устройств и информационных систем.

Для защиты сетевой инфраструктуры и выявления атак также применяются системы обнаружения и предотвращения вторжений — IDS и IPS. IDS (Intrusion Detection System) предназначены для обнаружения подозрительной активности и уведомления администраторов безопасности, а IPS (Intrusion Prevention System) способны автоматически блокировать потенциально опасные действия. Данные системы анализируют сетевой трафик и сравнивают его с известными шаблонами атак. При обнаружении подозрительной активности система может:

- зафиксировать инцидент
- отправить уведомление администратору
- заблокировать вредоносное соединение
- ограничить доступ к определённым ресурсам

Особую роль в анализе защищённости играют средства анализа промышленной инфраструктуры. На производственных предприятиях используются специализированные системы мониторинга безопасности АСУ ТП и SCADA-систем, позволяющие

контролировать состояние промышленного оборудования и выявлять аномалии в технологических процессах.

Поскольку многие промышленные системы имеют ограниченные возможности обновления и работают в режиме непрерывного производства, обеспечение их безопасности требует особого подхода. Для анализа защищённости промышленных сетей используются:

- системы мониторинга промышленного трафика
- инструменты анализа SCADA-протоколов
- платформы обнаружения аномалий
- средства сегментации производственных сетей

Важным направлением анализа уязвимостей является оценка человеческого фактора. Даже при наличии современных технических средств защиты ошибки сотрудников могут привести к компрометации внутренней инфраструктуры. Для проверки уровня осведомлённости персонала проводятся учебные фишинговые рассылки, тестирование знаний сотрудников и моделирование сценариев социальной инженерии.

Кроме того, в последние годы активно развиваются методы интеллектуального анализа угроз с использованием технологий искусственного интеллекта и машинного обучения. Такие системы способны анализировать большие объёмы данных, выявлять скрытые закономерности и обнаруживать аномальное поведение пользователей и устройств.

Таким образом, анализ уязвимостей является важнейшим элементом системы обеспечения информационной безопасности крупных производственных предприятий. Использование современных методов и инструментов позволяет своевременно выявлять слабые места инфраструктуры, предотвращать реализацию угроз и повышать устойчивость информационных систем к внешним и внутренним атакам. Эффективная защита предприятия возможна только при комплексном подходе, сочетающем технические средства мониторинга, аудит безопасности, тестирование на проникновение и организационные меры защиты.

Проведённый обзор показывает, что для оценки защищённости современной инфраструктуры недостаточно использования какого-либо одного метода анализа. Каждое средство решает собственный круг задач: сканеры позволяют выявлять известные уязвимости, аудит помогает оценить организационные процессы, а тестирование на проникновение демонстрирует возможные последствия эксплуатации обнаруженных недостатков. По этой причине наиболее эффективным считается комплексный подход, при

котором различные методы дополняют друг друга и позволяют получить более полное представление о состоянии информационной безопасности предприятия.

1.4. Международные и российские стандарты в области защиты инфраструктуры

В современных условиях цифровизации и активного развития информационных технологий обеспечение безопасности внутренней инфраструктуры предприятий невозможно без использования единых стандартов и нормативных требований в области информационной безопасности. Международные и российские стандарты определяют основные подходы к защите информации, управлению рисками, организации систем безопасности и обеспечению устойчивости критически важных объектов инфраструктуры.

Пожалуй, основным документом, которым можно руководствоваться – это методика ФСТЭК от 2021 г., в которой всё подробно расписано, начиная от порядка оценки угроз, заканчивая определением актуальности угроз. Согласно нему оценка проводится как при создании системы, так и в ходе её эксплуатации и модернизации. Результаты используются для выбора и проверки эффективности мер защиты информации.

Всего в пункте 2.2 данной методики приведены 6 задач, которые решаются оценкой угроз, но их можно объединить следующим образом:

- определение возможных негативных последствий от реализации угроз
- определение объектов воздействия
- оценка возможности реализации угроз и определение их актуальности

Также в пункте 2.3 приведены источники, которыми можно руководствоваться при оценке уязвимостей:

- банк данных угроз ФСТЭК России
- описания векторов атак (CAPEC, ATT&CK, OWASP и др.)
- документацию на системы и сети
- описание бизнес-процессов
- результаты анализа рисков, уязвимостей и тестирования на проникновение

Методика выделяет основные способы, с помощью которых нарушители могут реализовать угрозы безопасности информации. К ним относятся:

- использование уязвимостей программного обеспечения, архитектуры и конфигурации систем
- внедрение вредоносного программного обеспечения
- использование недекларированных возможностей ПО и оборудования
- установка программных или аппаратных закладок
- формирование скрытых каналов передачи данных

- компрометация поставок программных и аппаратных средств
- ошибочные действия персонала при эксплуатации и настройке систем

В этой же методике указывается к чему необходим доступ нарушителю для реализации угроз:

- внешним сетевым интерфейсам таким как, Интернет, удалённый доступ
- внутренним сетевым интерфейсам
- пользовательским интерфейсам
- интерфейсам съёмных носителей
- интерфейсам администрирования и обслуживания

Более подробно в самом документе приведена схема развития сценариев, изображение которой находится в приложении А.

Также, согласно пункту 5.3.3 методики оценки угроз безопасности информации ФСТЭК России от 2021 г., угроза безопасности информации считается возможной при наличии следующих составляющих:

- источника угрозы, он же нарушитель
- объекта воздействия
- способа реализации угрозы
- негативных последствий от реализации угрозы

А уже актуальность возможных угроз безопасности информации определяется наличием сценариев их реализации, что указывается в пункте 5.3.4 данной методики.

Одним из наиболее известных международных стандартов в области информационной безопасности является стандарт International Organization for Standardization ISO/IEC 27001.

Данный стандарт определяет требования к созданию, внедрению и поддержанию системы менеджмента информационной безопасности (СМИБ). Основной целью стандарта является обеспечение системного подхода к защите информации и управлению рисками безопасности.

ISO/IEC 27001 предусматривает:

- проведение оценки рисков информационной безопасности
- внедрение мер защиты информации
- контроль доступа к информационным ресурсам
- управление инцидентами безопасности
- обеспечение непрерывности деятельности организации
- регулярный аудит и совершенствование системы защиты

Стандарт широко используется крупными международными компаниями и промышленными предприятиями, поскольку позволяет организовать комплексную систему управления информационной безопасностью в соответствии с международными требованиями.

Важным дополнением к ISO/IEC 27001 является стандарт ISO/IEC 27002, содержащий практические рекомендации по реализации мер информационной безопасности. В нём рассматриваются вопросы управления доступом, криптографической защиты, физической безопасности, защиты сетевой инфраструктуры и организации мониторинга безопасности.

Особое значение для производственных предприятий имеют стандарты, связанные с защитой промышленных систем и критической инфраструктуры. Одним из наиболее распространённых является серия стандартов IEC 62443, разработанная для обеспечения безопасности автоматизированных систем управления технологическими процессами и промышленных сетей.

Стандарты IEC 62443 определяют:

- требования к защите АСУ ТП
- сегментирование сетей
- разграничение прав доступа
- контроль безопасности
- требования к безопасной разработке промышленного программного обеспечения

Данные стандарты учитывают особенности промышленной инфраструктуры и направлены на обеспечение устойчивости технологических процессов к кибератакам.

Кроме того, в международной практике широко применяется фреймворк National Institute of Standards and Technology Cybersecurity Framework, разработанный Национальным институтом стандартов и технологий США. Он представляет собой набор рекомендаций по организации кибербезопасности предприятий и критической инфраструктуры.

Framework NIST включает пять ключевых функций:

1. Идентификация угроз и активов.
2. Защита информационных систем.
3. Обнаружение инцидентов.
4. Реагирование на угрозы.
5. Восстановление после инцидентов.

Данный подход позволяет предприятиям выстраивать эффективную систему управления информационной безопасностью и обеспечивать непрерывность производственной деятельности. Обеспечение безопасности информационной инфраструктуры регулируется государственными стандартами, федеральными законами и требованиями уполномоченных органов в области защиты информации. Особую роль в данной сфере играют требования ФСТЭК России и ФСБ России, устанавливающие правила защиты государственных информационных систем, объектов критической информационной инфраструктуры и автоматизированных систем управления.

Одним из ключевых нормативных документов является Федеральный закон №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Данный закон определяет правовые основы обеспечения безопасности объектов критической инфраструктуры, к которым относятся предприятия промышленности, энергетики, транспорта, связи и других стратегически важных отраслей.

Закон предусматривает:

- категорирование объектов критической инфраструктуры
- проведение оценки угроз безопасности
- внедрение средств защиты информации
- организацию мониторинга и реагирования на инциденты
- взаимодействие с государственными системами обнаружения кибератак

Для крупных производственных предприятий требования данного закона имеют особую важность, поскольку многие из них относятся к субъектам критической информационной инфраструктуры. Значительное место в российской системе стандартизации занимают государственные стандарты.

В области информационной безопасности применяются:

- ГОСТ Р ИСО/МЭК 27001 — требования к созданию, внедрению и поддержке системы менеджмента информационной безопасности организации
- ГОСТ Р ИСО/МЭК 27002 — практические рекомендации по применению мер и механизмов защиты информации

- ГОСТ Р 56939 — требования и рекомендации по разработке и внедрению процессов управления уязвимостями информационных систем
- ГОСТ Р 56938 — требования к защите информации при использовании виртуализации и виртуальной инфраструктуры

Российские ГОСТы во многом основаны на международных стандартах ISO, однако адаптированы с учётом национальных требований и особенностей российского законодательства. Особую роль играют методические документы ФСТЭК России, определяющие требования к защите автоматизированных систем, государственных информационных систем и объектов критической инфраструктуры. К ним относятся:

- методики моделирования угроз
- требования по защите АСУ ТП
- рекомендации по анализу уязвимостей
- правила проведения оценки соответствия средств защиты информации

Кроме того, для обеспечения безопасности промышленной инфраструктуры применяются требования по сегментации сетей, использованию сертифицированных средств защиты, организации контроля доступа и ведению журналов событий безопасности.

В последние годы в России активно развивается направление импортозамещения в сфере информационной безопасности. Крупные предприятия всё чаще внедряют отечественные средства защиты информации, сертифицированные государственными регуляторами. Это связано как с требованиями законодательства, так и с необходимостью повышения устойчивости инфраструктуры к внешним угрозам.

Несмотря на различия между международными и российскими подходами к обеспечению информационной безопасности, их основная цель остаётся общей — обеспечение устойчивой и безопасной работы информационной инфраструктуры предприятия. На практике крупные производственные организации часто используют комбинированный подход, совмещая международные стандарты управления безопасностью с выполнением требований российского законодательства и регуляторов.

Ниже приведена таблица 1.2 со сравнением зарубежных и российских стандартов и методик. Исходя из этих данных видно, что российские стандарты и ГОСТы во многом основаны на международных практиках, однако адаптированы с учётом требований законодательства и особенностей отечественной инфраструктуры.

Таблица 1.2 – Сравнение стандартов к обеспечению безопасности.

Стандарт/ методика	Страна / организация	Основное назначение	Область применения	Особенности
International Organization for Standardization ISO/IEC 27001	Международный стандарт ISO	Создание системы менеджмента информационной безопасности	Организации любого типа	Комплексный подход к управлению рисками и защите информации
International Electrotechnical Commission IEC 62443	Международная электротехническая комиссия	Защита промышленных систем и АСУ ТП	Промышленные предприятия	Ориентирован на безопасность SCADA и промышленных сетей
National Institute of Standards and Technology Cybersecurity Framework	США, NIST	Организация кибербезопасности предприятий	Критическая инфраструктура и бизнес	Основан на управлении рисками и реагировании на инциденты
International Organization for Standardization ISO/IEC 27002	Международный стандарт ISO	Практические рекомендации по мерам защиты информации	Корпоративные информационные системы	Содержит рекомендации по контролю доступа, криптографии и мониторингу
ГОСТ Р ИСО/МЭК 27002	Россия, Росстандарт	Практические меры защиты информации	Информационные системы организаций	Содержит рекомендации по обеспечению ИБ в РФ
ГОСТ Р 56939	Россия, Росстандарт	Управление и анализ уязвимостей	Информационные системы предприятий	Регламентирует процессы выявления и устранения уязвимостей
ГОСТ Р ИСО/МЭК 27001	Россия, Росстандарт	Управление системой информационной безопасности	Государственные и коммерческие организации	Адаптация ISO/IEC 27001 под российское законодательство
Методика ФСТЭК от 2021 г.	Россия, ФСТЭК	Оценка угроз безопасности информации	Разработка моделей угроз и создания систем защиты информации	Описание от абстрактного нарушителя к анализу сценариев реализации угроз с учетом

				возможного ущерба

Исходя из данных, указанных в таблице выше, напрашивается вывод, что их применение позволяет выстраивать эффективную систему информационной безопасности, а также своевременно выявлять угрозы и уязвимости. Если углубиться, в структуру этих стандартов, можно проследить большую схожесть зарубежных с Российскими, поэтому можно считать, что большая часть отечественных это переделанные зарубежные стандарты под условия России.

2. Практический анализ защищённости внутренней инфраструктуры предприятий

2.1. Описание тестовой инфраструктуры предприятия

Для проведения практического анализа защищённости внутренней инфраструктуры предприятия была развёрнута тестовая локальная сеть в виртуальной среде. Использование виртуальной инфраструктуры позволило смоделировать типовую корпоративную сеть предприятия и безопасно провести исследование уязвимостей без риска нарушения работы реальных информационных систем.

Тестовая среда включала:

- сервер под управлением операционной системы Windows Server 2016
- клиентскую рабочую станцию под управлением Windows 10
- локальную виртуальную сеть, обеспечивающую взаимодействие между устройствами

Виртуальная инфраструктура была развёрнута с использованием программного обеспечения виртуализации, таком как VMware. Все параметры безопасности операционных систем и сетевых служб находились в стандартном состоянии, без применения дополнительных средств защиты и усиления безопасности конфигурации. Такой подход даёт возможность оценить уровень защищённости системы при типичной базовой установке, которая нередко встречается в организациях.

Сервер выполнял функции хранения данных и сетевого взаимодействия между узлами тестовой сети. Клиентская машина использовалась для имитации рабочей станции сотрудника предприятия. Между устройствами была настроена локальная связь, позволяющая осуществлять обмен данными и проводить анализ сетевой активности. Изображения настроек виртуальной среды VMware приведены в приложении Б. Сетевой адрес сервера 192.168.1.229, а клиента 192.168.1.65.

В процессе исследования особое внимание уделялось:

- анализу открытых сетевых портов
- проверке настроек удалённого доступа
- оценке политики паролей
- анализу сетевых служб
- выявлению потенциальных уязвимостей операционной системы
- исследованию возможностей несанкционированного доступа

2.2. Анализ уязвимостей тестовой инфраструктуры

На первом этапе исследования был проведён анализ сетевой доступности устройств тестовой инфраструктуры. Для этого использовались инструменты сетевого сканирования, позволяющие определить активные узлы сети, открытые порты и доступные сервисы.

Для сетевого анализа были использованы инструменты Сканер ВС и Nmap, оба инструмента показали одинаковый результат, однако последний запускает проверку не атематически, здесь уже запуск происходит непосредственно через командную строку, где сначала указываются ключи, а затем сам ip адрес, который необходимо просканировать. В данной работе использовалась команда nmap -T5 -F --min-rate 2000 (ip), где T5 — шаблон настроек управления временем, min-rate – отправка запросов с интенсивностью не меньше чем 2000 в секунду, F – быстрое сканирование ограниченного количества портов, результаты приведены в приложении Д.

В результате анализа было установлено, что целевой узел 192.168.1.65 доступен в сети. На хосте обнаружено 96 закрытых TCP-портов, при этом выявлены следующие открытые сетевые порты, используемые системными службами Windows:

- 135/tcp — msrpc (Microsoft RPC)
- 139/tcp — netbios-ssn (службы NetBIOS)
- 445/tcp — microsoft-ds (SMB-службы файлового доступа)
- 5357/tcp — wsdapi (Web Services for Devices)

Полученные данные указывают на наличие стандартного набора сетевых сервисов операционной системы Windows, включая механизмы удалённого вызова процедур (RPC), службы файлового и сетевого обмена (SMB/NetBIOS), а также сервисы обнаружения и взаимодействия устройств в сети. Наличие открытых SMB и NetBIOS портов при отсутствии дополнительных ограничений безопасности может увеличивать риск несанкционированного доступа к сетевым ресурсам, а также способствовать проведению атак, связанных с перечислением ресурсов и эксплуатацией уязвимостей в службах общего доступа. Что и описывалось в главе 1.2 данной курсовой работы. Далее был проведен анализ на наличие программных уязвимостей с помощью ScanOval, подробнее данный процесс указан в приложении В и Г. Затем был проведён анализ с помощью ScanOval, где было выявлено 22 уязвимости различного уровня критичности, среди которых:

- 1 критическая уязвимость
- 11 уязвимостей высокого уровня опасности
- 10 уязвимостей среднего уровня опасности

Наибольшее количество выявленных проблем, связанных с компонентами Microsoft Defender и Microsoft Malware Protection Engine. Данные уязвимости затрагивают

встроенные механизмы защиты операционной системы и могут позволить злоумышленнику выполнить произвольный код, повысить привилегии либо обойти средства антивирусной защиты. Наибольшую опасность представляет возможность компрометации системы через обработку специально сформированных файлов без непосредственного участия пользователя. Как правило данная уязвимость устраняется обновлением встроенного антивируса операционной системы.

Далее были обнаружены уязвимости повышения привилегий. Данный тип уязвимостей позволяет злоумышленнику, уже получившему ограниченный доступ к системе, повысить свои права до уровня локального администратора или системной учётной записи. Реализация подобных атак может привести к полному контролю над сервером, отключению механизмов защиты, изменению конфигурации системы и получению доступа к конфиденциальной информации. Для снижения риска эксплуатации рекомендуется своевременно устанавливать обновления безопасности операционной системы, ограничить использование учётных записей с административными правами, применять принцип минимально необходимых привилегий и контролировать действия пользователей с повышенными полномочиями.

Сканирование выявило несколько уязвимостей, позволяющих осуществлять удалённое выполнение произвольного кода на целевой системе. Данный класс уязвимостей относится к наиболее опасным, поскольку злоумышленник может получить возможность выполнения собственных команд без физического доступа к устройству. Успешная эксплуатация подобных уязвимостей может привести к компрометации сервера, установке вредоносного программного обеспечения, хищению информации и нарушению работоспособности информационной системы. Для устранения также рекомендуется обновление и ограничить доступ к сетевым сервисам, дополнительно использовать межсетевые экраны и средства сегментации сети.

В ходе анализа была обнаружена уязвимость в криптографической библиотеке OpenSSL. Эксплуатация выявленной уязвимости может привести к нарушению конфиденциальности передаваемой информации, компрометации криптографических ключей и снижению уровня защищённости сетевого взаимодействия. Несмотря на то, что подобные уязвимости не всегда позволяют получить непосредственный контроль над системой, они создают дополнительные возможности для реализации более сложных атак. Для исключения угрозы рекомендуется обновить используемую версию OpenSSL до актуального состояния, отключить устаревшие криптографические алгоритмы и использовать современные версии протокола TLS. Анализ показал наличие уязвимостей в программном обеспечении VMware Tools, установленном в виртуальной среде. Данные

компоненты обеспечивают взаимодействие между виртуальной машиной и гипервизором, поэтому их безопасность напрямую влияет на защищённость виртуальной инфраструктуры. Использование устаревших версий VMware Tools может привести к выполнению вредоносного кода, повышению привилегий и компрометации виртуальной машины. Для устранения выявленных уязвимостей рекомендуется установить актуальную версию VMware Tools.

Также были выявлены уязвимости в дополнительных компонентах операционной системы Windows, включая Microsoft Paint 3D, Microsoft 3D Viewer и VP9 Video Extensions. Несмотря на то, что данные приложения не относятся к критически важным элементам корпоративной инфраструктуры, их наличие увеличивает поверхность атаки информационной системы. Зачастую наилучший способ решения подобных уязвимостей – удаление неиспользуемых компонентов операционной системы, если это возможно, так как некоторые из них, во-первых, возможно удалить только при изменении установочного образа, во-вторых, это может привести к нестабильности работы или вовсе полному нарушению работоспособности системы.

Полученные результаты демонстрируют, что даже небольшая тестовая инфраструктура со стандартными параметрами безопасности, отсутствием последних обновлений программного и операционного обеспечения, содержит значительное количество потенциальных уязвимостей, способных привести к печальным последствиям, описанным выше.

2.3. Рекомендации по повышению защищённости инфраструктуры

Подводя итоги анализа, были разработаны рекомендации, направленные на повышение уровня защищённости внутренней инфраструктуры предприятия. Одной из основных мер является усиление политики аутентификации пользователей, так как он не был задан для этих операционных систем. Для этого рекомендуется:

- использовать сложные пароли, более 8 символов
- настроить минимальную длину пароля
- внедрить блокировку учётной записи при множественных ошибках входа
- включить двухфакторную аутентификацию, использование логина и пароля

Важным направлением повышения безопасности является настройка сетевой инфраструктуры. Для минимизации рисков необходимо:

- закрыть неиспользуемые сетевые порты
- ограничить доступ к службам удалённого администрирования
- внедрить сегментацию сети

- разделить серверный и пользовательский сегменты
- ограничить сетевое обнаружение устройств

Особое внимание должно уделяться своевременному обновлению операционных систем и программного обеспечения. Регулярная установка обновлений безопасности позволяет устранять известные уязвимости и снижать вероятность эксплуатации системы злоумышленниками. Дополнительно рекомендуется внедрение специализированных средств защиты информации:

- систем обнаружения вторжений IDS/IPS
- SIEM-систем мониторинга безопасности
- антивирусных решений корпоративного уровня
- средств централизованного контроля событий безопасности

Для повышения устойчивости инфраструктуры к внутренним угрозам необходимо проводить обучение сотрудников основам информационной безопасности. Большое количество инцидентов связано именно с человеческим фактором, поэтому повышение уровня осведомлённости персонала играет важную роль в защите предприятия.

Также рекомендуется:

- регулярно проводить аудит безопасности
- выполнять анализ уязвимостей
- осуществлять резервное копирование данных
- контролировать действия пользователей
- разрабатывать планы реагирования на инциденты

Таким образом, проведённый анализ тестовой инфраструктуры показал, что использование стандартных настроек безопасности не обеспечивает достаточного уровня защищённости внутренней сети предприятия. Даже в небольшой локальной инфраструктуре могут присутствовать многочисленные уязвимости, создающие условия для несанкционированного доступа и реализации киберугроз. Для обеспечения надёжной защиты необходим комплексный подход, включающий технические, организационные и программные меры информационной безопасности.

Что касается средств защиты информации, то рекомендуется использовать антивирусы, например Kaspersky Endpoint Security или Dr.Web Enterprise Security Suite. Для регулярного контроля защищённости инфраструктуры рекомендуется внедрить системы управления уязвимостями MaxPatrol VM. Дополнительно следует использовать средства защиты от несанкционированного доступа, такие как Secret Net Studio или Dallas Lock 8-C, а также организовать централизованный мониторинг событий безопасности с помощью MaxPatrol SIEM.

Так как у нас виртуальная среда имеет уязвимости, связные с удалённым доступом, компрометации сетевых сервисов, то рекомендуется использовать средства контроля сетевого доступа. К таким относятся аппаратно-программный комплекс шифрования Континент 4 или программно-аппаратный комплекс для построения защищённых сетей и шифрования трафика ViPNet Coordinator.

Комплексное применение указанных средств позволит существенно повысить уровень защищённости внутренней инфраструктуры предприятия и снизить вероятность успешной реализации атак.

Однако для небольшой организации может быть достигнуто без приобретения специализированных программных комплексов. Современные версии операционных систем Windows Server и Windows 10 содержат встроенные механизмы защиты, позволяющие существенно снизить риски эксплуатации выявленных уязвимостей.

Для защиты от вредоносного программного обеспечения может использоваться встроенный антивирус Microsoft Defender, входящий в состав операционной системы. Для обеспечения эффективной защиты необходимо регулярно обновлять антивирусные базы и платформу защиты через службу Windows Update, а также активировать функции защиты в реальном времени и облачной защиты.

Для устранения уязвимостей повышения привилегий и удалённого выполнения кода необходимо обеспечить своевременную установку обновлений безопасности операционной системы. В небольших организациях данная задача может быть реализована посредством штатного механизма Windows Update без развёртывания дополнительных систем управления обновлениями.

Дополнительную защиту удалённого доступа обеспечивает встроенный Брандмауэр Защитника Windows. Рекомендуется ограничить доступ к службам удалённого рабочего стола, разрешив подключения только с доверенных IP-адресов, а также использовать аутентификацию на уровне сети.

Для предотвращения несанкционированного доступа к данным целесообразно применять встроенное средство шифрования дисков BitLocker, позволяющее защитить информацию в случае физического доступа к оборудованию или утраты носителей информации.

Для контроля действий пользователей рекомендуется использовать механизмы локальной политики безопасности Windows Local Security Policy и редактор групповых политик gpedit.msc. С их помощью можно настроить требования к сложности паролей, минимальной длине пароля, сроку действия паролей и блокировке учётных записей после нескольких неудачных попыток входа.

Контроль событий безопасности может осуществляться посредством встроенного Просмотра событий Windows Event Viewer) и системы журналирования операционной системы. Для повышения эффективности мониторинга рекомендуется включить аудит входов в систему, изменения учётных записей и использования привилегированных команд.

Для защиты файловых ресурсов рекомендуется ограничить права доступа пользователей к общим папкам в соответствии с принципом минимально необходимых привилегий и использовать механизмы разграничения доступа NTFS.

Заключение хочется сказать, даже без применения специализированных коммерческих средств защиты небольшая организация может обеспечить приемлемый результат за счёт правильной настройки встроенных механизмов безопасности Windows.

Заключение

В ходе выполнения курсовой работы были рассмотрены основные виды уязвимостей внутренней инфраструктуры предприятий, методы их выявления и нормативные документы, регламентирующие обеспечение информационной безопасности. Проведённый обзор показал, что для оценки защищённости информационных систем используются различные подходы, включая анализ конфигурации, сетевое сканирование, аудит безопасности и тестирование на проникновение.

В практической части работы была развёрнута тестовая инфраструктура на базе Windows Server 2016 и Windows 10 в виртуальной среде VMware. Для анализа сетевой инфраструктуры использовался инструмент Nmap, а для выявления программных уязвимостей — ScanOVAL. В результате сетевого сканирования были обнаружены открытые порты 135/tcp, 139/tcp, 445/tcp и 5357/tcp, обеспечивающие работу стандартных служб Windows. Наличие данных сервисов свидетельствует о необходимости дополнительного контроля сетевого доступа и настройки механизмов защиты.

Проверка средствами ScanOVAL позволила выявить 22 уязвимости различного уровня критичности, включая критическую уязвимость, а также уязвимости высокого и среднего уровня опасности. Наиболее значимые проблемы были связаны с компонентами Microsoft Defender, механизмами повышения привилегий, возможностью удалённого выполнения кода, использованием устаревших версий OpenSSL и VMware Tools. Полученные результаты показали, что даже стандартная конфигурация операционной системы без дополнительной настройки безопасности может содержать значительное количество потенциальных точек компрометации.

На основании выявленных недостатков были разработаны рекомендации по повышению защищённости инфраструктуры, включающие настройку политики паролей, ограничение сетевого доступа, сегментацию сети, своевременную установку обновлений безопасности, применение встроенных средств защиты Windows и организацию контроля событий безопасности.

Подводя итоги, можно сказать, что поставленная цель работы была достигнута. Проведённый анализ позволил выявить уязвимости тестовой инфраструктуры, оценить возможные риски их эксплуатации и сформировать практические рекомендации по повышению уровня защищённости, как информационной системы крупных предприятий, так и для небольших организаций.

Список использованной литературы

1. Федеральный закон от 26.07.2017 № 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации". [Электронный ресурс]: Официальный сайт. – Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_220885 [Дата обращения 07.05.2026]

2. Указ Президента Российской Федерации от 01.05.2022 № 250 "О дополнительных мерах по обеспечению информационной безопасности Российской Федерации». [Электронный ресурс]: Официальный сайт. – Режим доступа: https://base.garant.ru/404561984 [Дата обращения 09.05.2026]

3. Методический документ ФСТЭК России от 5 февраля 2021 г. "Методика оценки угроз безопасности информации". [Электронный ресурс]: Официальный сайт. – Режим доступа: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g [Дата обращения 10.05.2026]

4. Методический документ ФСТЭК России от 11 февраля 2014 г. "Меры защиты информации в государственных информационных системах". [Электронный ресурс]: Официальный сайт. – Режим доступа: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-11-fevralya-2014-g [Дата обращения 11.05.2026]

5. Методический документ ФСТЭК России "Мероприятия и меры по защите информации в государственных информационных системах". [Электронный ресурс]: Официальный сайт. – Режим доступа: https://fstec.ru/files/1453/--1655/2938/--.pdf [Дата обращения 10.05.2026]

6. Требования по безопасности информации к системам управления базами данных. [Электронный ресурс]: Официальный сайт. – Режим доступа: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/trebovaniya-po-bezopasnosti-informatsii-utverzhdeny-prikazom-fstek-rossii-ot-14-aprelya-2023-g-n-64 [Дата обращения 01.06.2026]

7. Требования безопасности информации к операционным системам. [Электронный ресурс]: Официальный сайт. – Режим доступа: https://fstec.ru/en/dokumenty/vse-dokumenty/informatsionnye-i-analiticheskie-materialy/informatsionnoe-soobshchenie-fstek-rossii-ot-18-oktyabrya-2016-g-n-240-24-4893 [Дата обращения 19.04.2026]

8. Методические рекомендации по обеспечению информационной безопасности при создании и эксплуатации открытых репозиториев программного обеспечения. [Электронный ресурс]: Официальный сайт. – Режим доступа:

https://digital.gov.ru/documents/metodicheskie-rekomendaczii-po-obespecheniyu-informaczionnoj-bezopasnosti-pri-sozdanii-i-ekspluataczii-otkrytyh-repozitoriev-programmnogo-obespecheniya [Дата обращения 24.04.2026]

9. Трещев И.А. Защита от несанкционированного доступа к информации на предприятии. [Электронный ресурс]: Официальный сайт. – Режим доступа: https://cyberleninka.ru/article/n/zaschita-ot-nesanktsionirovannogo-dostupa-k-informatsii-na-predpriyatii [Дата обращения 14.05.2026]

10. Марьенков А.Н. Автоматизация средств защиты от НСД: проблемы и возможности. [Электронный ресурс]: Официальный сайт. – Режим доступа:

https://cyberleninka.ru/article/n/avtomatizatsiya-sredstv-zaschity-ot-nsd-problemy-i-vozmozhnosti [Дата обращения 17.05.2026]

ISO/IEC 27001 — система менеджмента информационной безопасности, требования к организации и управлению ИБ. [Электронный ресурс]: Официальный сайт. – Режим доступа: https://www.iso.org/standard/2700 [Дата обращения 5.05.2026]

ISO/IEC 27002 — практические рекомендации по мерам информационной безопасности. [Электронный ресурс]: Официальный сайт. – Режим доступа: https://www.iso.org/standard/75652.html [Дата обращения 1.06.2026]

11. IEC 62443 — серия стандартов по безопасности промышленных систем и АСУ ТП. [Электронный ресурс]: Официальный сайт IEC. – Режим доступа: https://www.iec.ch/standards/iec-62443-series [Дата обращения 3.06.2026]

12. NIST Cybersecurity Framework — фреймворк кибербезопасности для организаций и критической инфраструктуры. [Электронный ресурс]: Официальный сайт NIST. – Режим доступа: https://www.nist.gov/cyberframework [Дата обращения 19.05.2026]

13. ГОСТ Р ИСО/МЭК 27001 — система менеджмента информационной безопасности, требования к созданию, внедрению и поддержанию системы ИБ. [Электронный ресурс]: Официальный сайт Росстандарта. – Режим доступа: https://protect.gost.ru [Дата обращения 23.05.2026]

14. ГОСТ Р ИСО/МЭК 27002 — практические рекомендации по мерам обеспечения информационной безопасности. [Электронный ресурс]: Официальный сайт Росстандарта. – Режим доступа: https://protect.gost.ru [Дата обращения 15.05.2026]

15. ГОСТ Р 56939 — требования к процессам управления уязвимостями информационных систем. [Электронный ресурс]: Официальный сайт Росстандарта. – Режим доступа: https://protect.gost.ru [Дата обращения 13.05.2026]

16. ГОСТ Р 56938 — требования к защите информации при использовании виртуализации и виртуальных инфраструктур. [Электронный ресурс]: Официальный сайт Росстандарта. – Режим доступа: https://protect.gost.ru [Дата обращения 11.05.2026]

17. ScanOVAL — средство автоматизированного анализа конфигурации и проверки защищённости информационных систем. [Электронный ресурс]: Официальный сайт. – Режим доступа: https://bdu.fstec.ru/scanoval [Дата обращения 11.05.2026]

18. Сканер-ВС — программный комплекс анализа защищённости вычислительных сетей и выявления уязвимостей. [Электронный ресурс]: Информационно-аналитический портал Anti-Malware.ru. – Режим доступа: https://www.anti-malware.ru/products/Scanner-VS/overview [Дата обращения 11.05.2026]

19. Методический документ от 5 февраля 2021 г. [Электронный ресурс]: Официальный сайт ФСТЭК – Режим доступа: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g [Дата обращения 11.05.2026]

20. Vmware — программное обеспечение для виртуализации. [Электронный ресурс]: Официальный сайт vmware.com. – Режим доступа: https://www.vmware.com [Дата обращения 19.05.2026]

21. Nmap — программа анализа сетей и выявления уязвимостей. [Электронный ресурс]: Официальный сайт nmap.org. – Режим доступа: https://nmap.org/download [Дата обращения 22.05.2026]

22. Kaspersky Endpoint Security для Windows — средство антивирусной защиты. [Электронный ресурс]: Официальный сайт kaspersky.ru. – Режим доступа: https://www.kaspersky.com/small-to-medium-business-security/endpoint-windows [Дата обращения 22.05.2026]

23. Dr. Web Enterprise Security Suite — средство антивирусной защиты. [Электронный ресурс]: Официальный сайт drweb.ru. – Режим доступа: https://products.drweb.ru/for_biz [Дата обращения 23.05.2026]

24. MaxPatrol VM — система управления уязвимостями. [Электронный ресурс]: Официальный сайт ptsecurity.com. – Режим доступа: https://ptsecurity.com/products [Дата обращения 23.05.2026]

25. MaxPatrol SIEM — система мониторинга и корреляции событий безопасности. [Электронный ресурс]: Официальный сайт ptsecurity.com. – Режим доступа: https://ptsecurity.com/products [Дата обращения 16.05.2026]

26. Континент 4 — аппаратно-программный комплекс шифрования. [Электронный ресурс]: Официальный сайт securitycode.ru. – Режим доступа: https://www.securitycode.ru/products/kontinent-4 [Дата обращения 24.05.2026]

27. Secret Net Studio — средство защиты информации от несанкционированного доступа. [Электронный ресурс]: Официальный сайт securitycode.ru. – Режим доступа: https://www.securitycode.ru/products/secret-net-studio [Дата обращения 25.05.2026]

28. Dallos Lock 8-C — средство защиты информации от несанкционированного доступа. [Электронный ресурс]: Официальный сайт dallaslock.ru. – Режим доступа: https://dallaslock.ru/products/szi-dallas-lock-8-0/szi-ot-nsd-dallas-lock-8-0-s [Дата обращения 7.05.2026]

29. ViPNet Coordinator — программно-аппаратный шлюз безопасности. [Электронный ресурс]: Официальный сайт infotecs.ru. – Режим доступа: https://infotecs.ru/products/vipnet-coordinator-hw-4 [Дата обращения 8.05.2026]

30. Продукты компании Microsoft. [Электронный ресурс]: Официальный сайт microsoft.com. – Режим доступа: https://www.microsoft.com [Дата обращения 11.05.2026]

31. ГосСОПКА – Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации. [Электронный ресурс]: Официальный сайт gossopka.ru. – Режим доступа: https:// https://gossopka.ru/doc [Дата обращения 14.05.2026]

Приложение А

Рисунки из методики ФСТЭК от 2021 г.

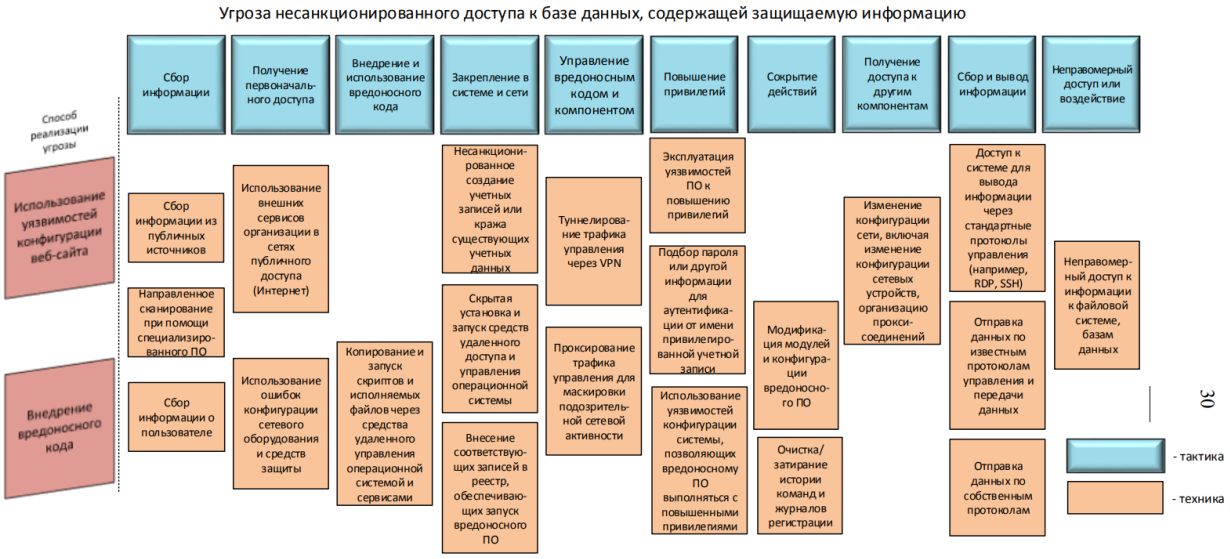

Рисунок А.1 – Схема примеров сценария реализации угроз безопасности из методики ФСТЭК от 2021 г.

Приложение Б

Изображения настроек виртуальной среды VMware

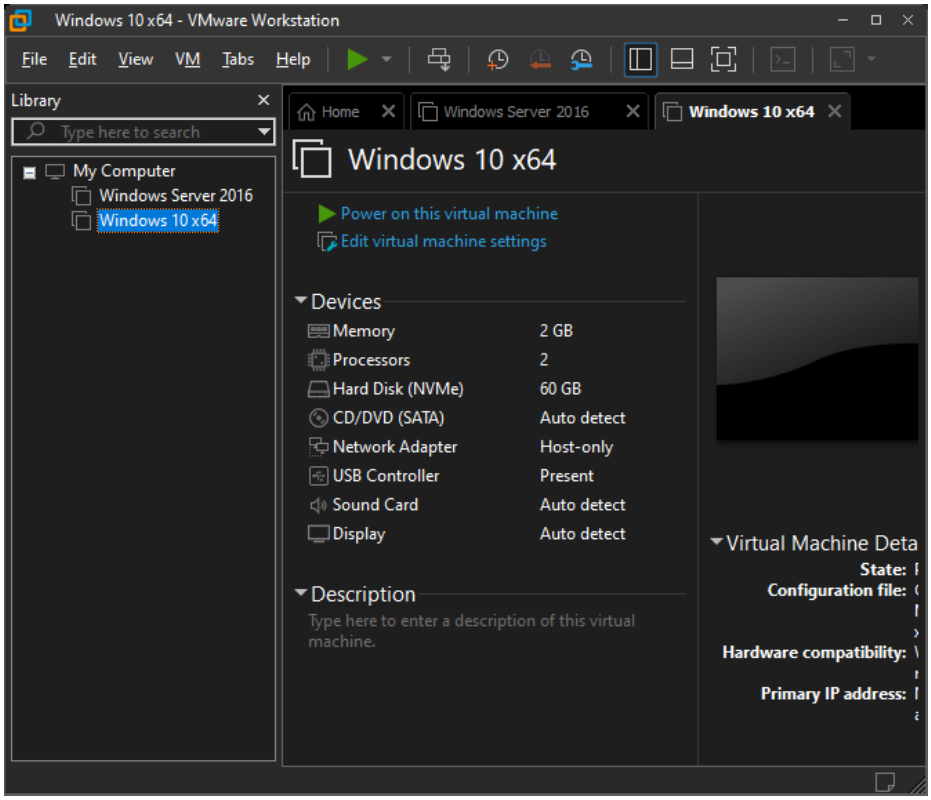

Рисунок Б.1 – перечень виртуальных машин и их параметров.

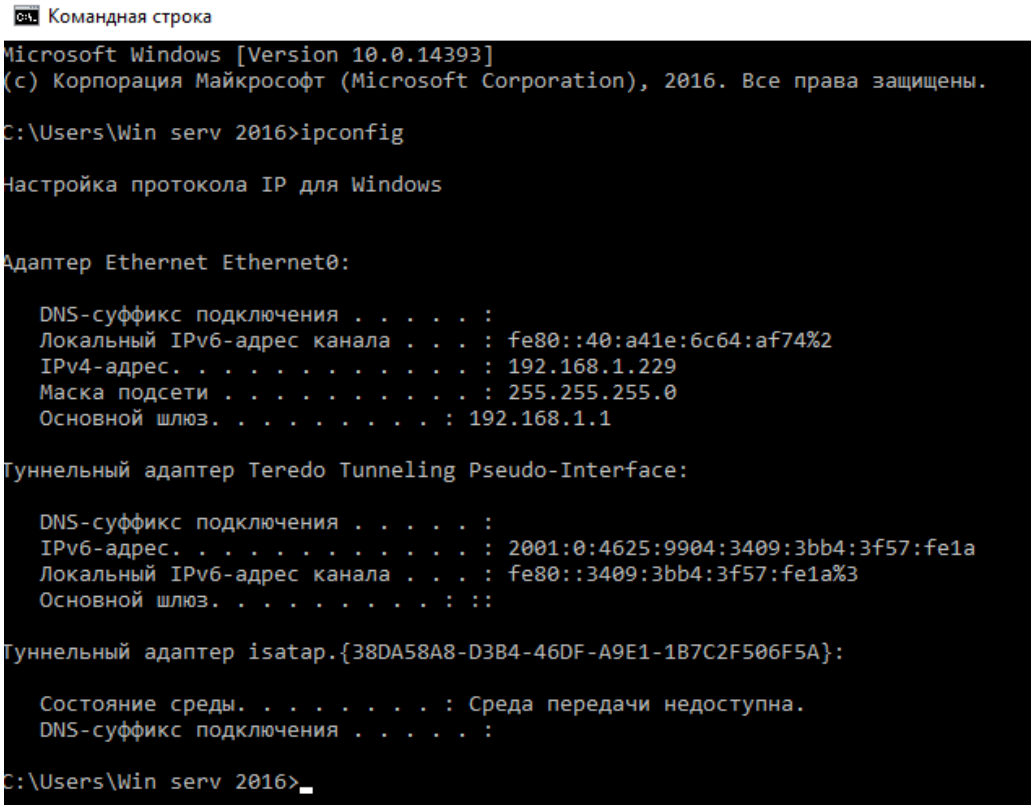

Рисунок Б.2 – параметры сетевой адресации сервера.

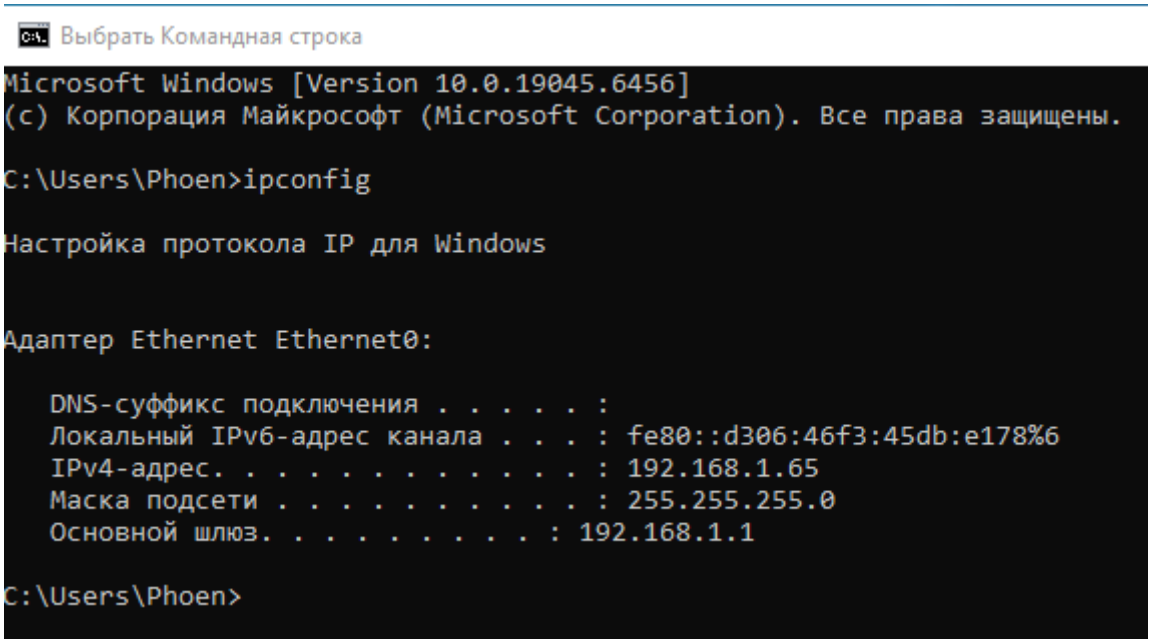

Рисунок Б.3 – параметры сетевой адресации клиента.

Приложение В

Использование приложения ScanOval

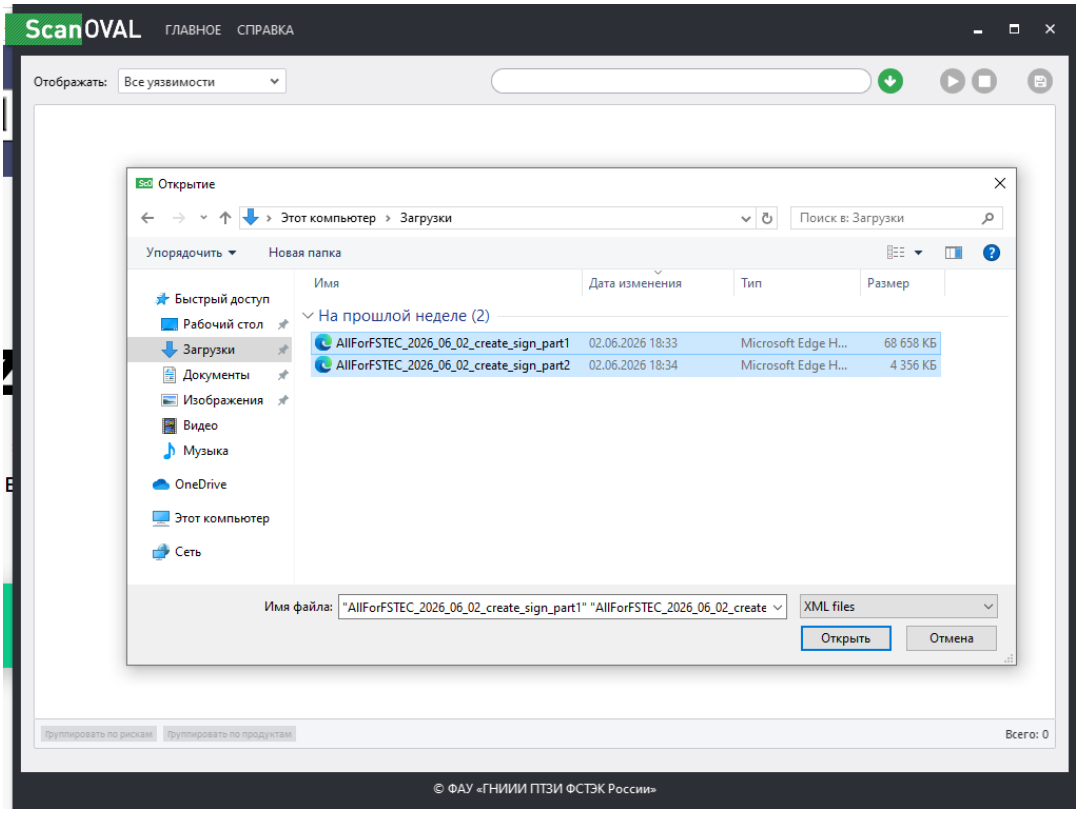

Рисунок В.1 – загрузка Oval файлов.

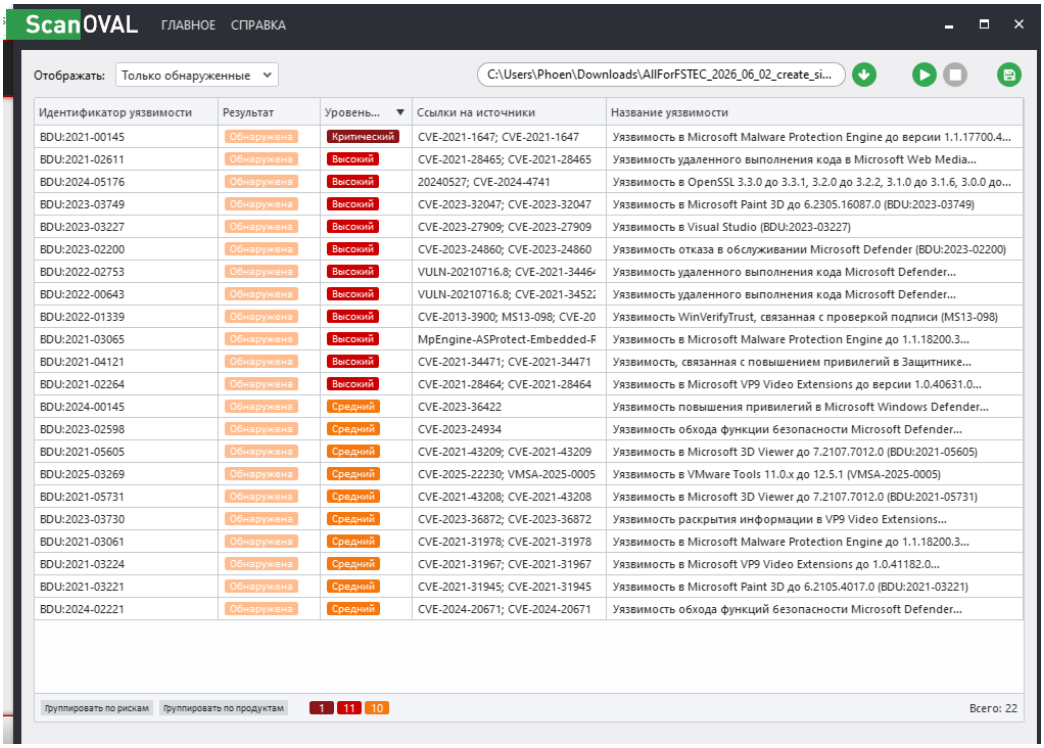

Рисунок В.2 – результаты проверки.

Приложение Г

Использование Сканер ВС

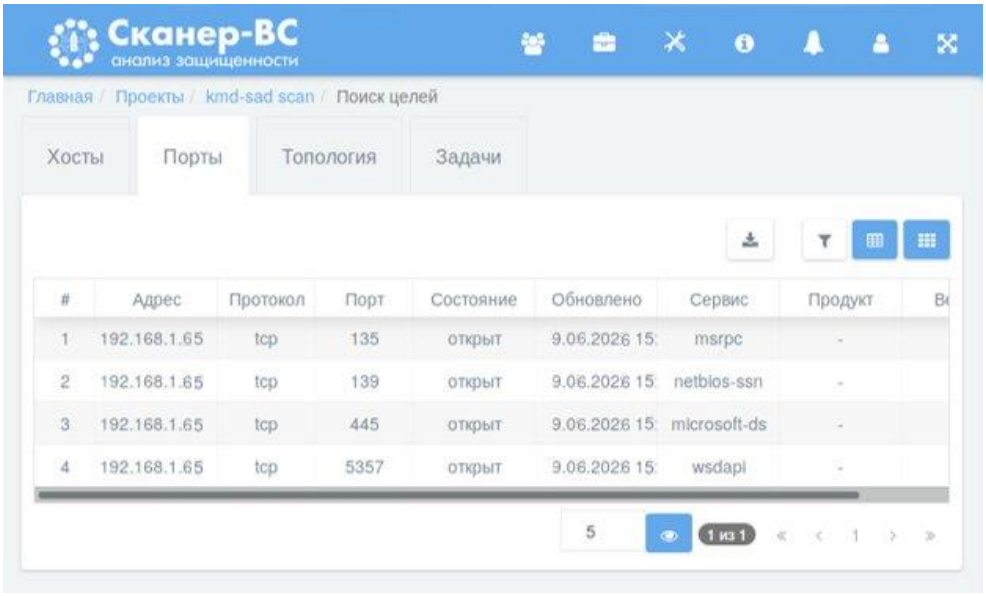

Рисунок Г.1 – результат анализа сети Сканером ВС.

Приложение Д

Использование Инструмента Nmap.

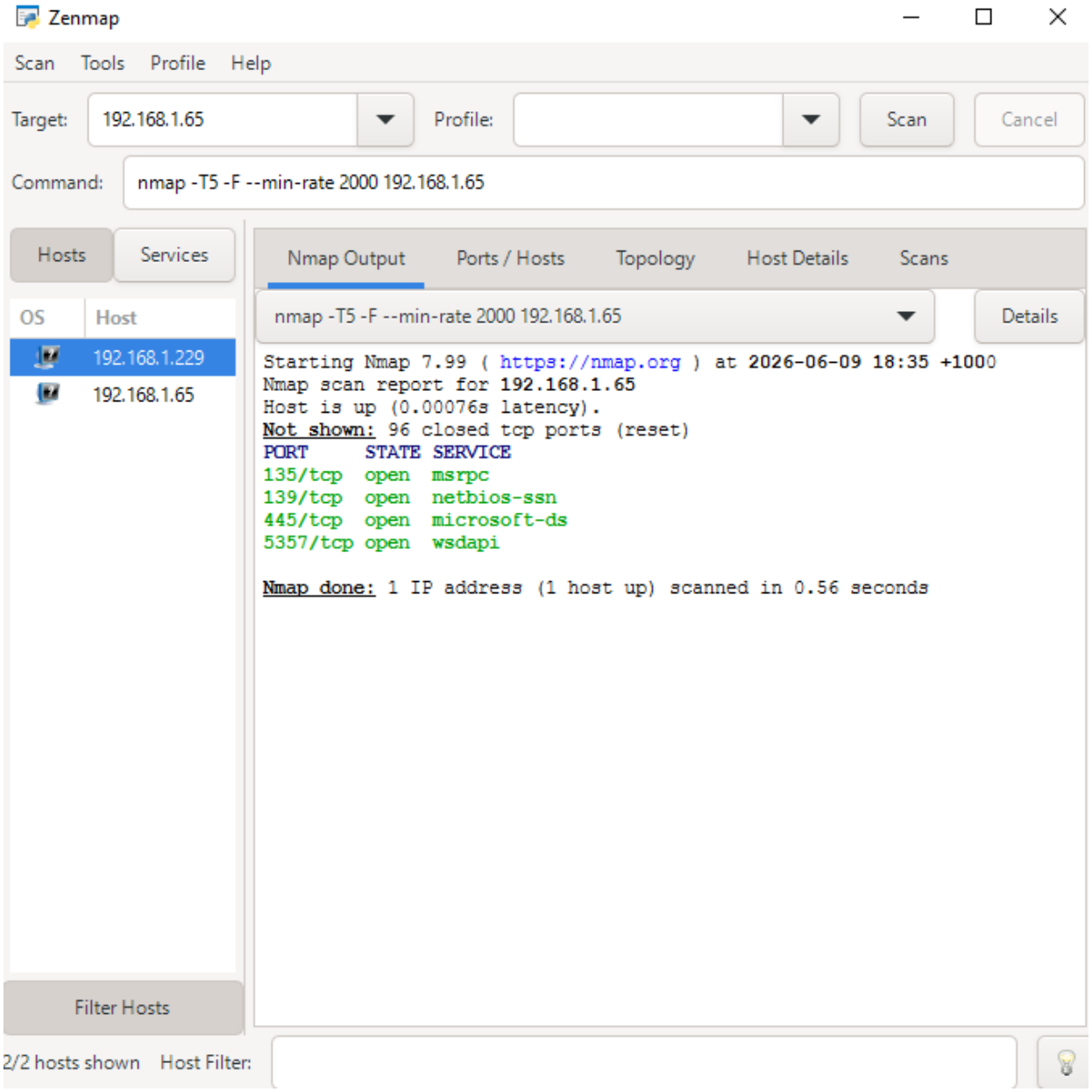

Рисунок Д.1 – Использование команды для поиска сетевых уязвимостей.