+7 (495) 786 34 93
info@itprotect.ru

Россия, 129110, г. Москва,
Дербеневская наб., 11 В

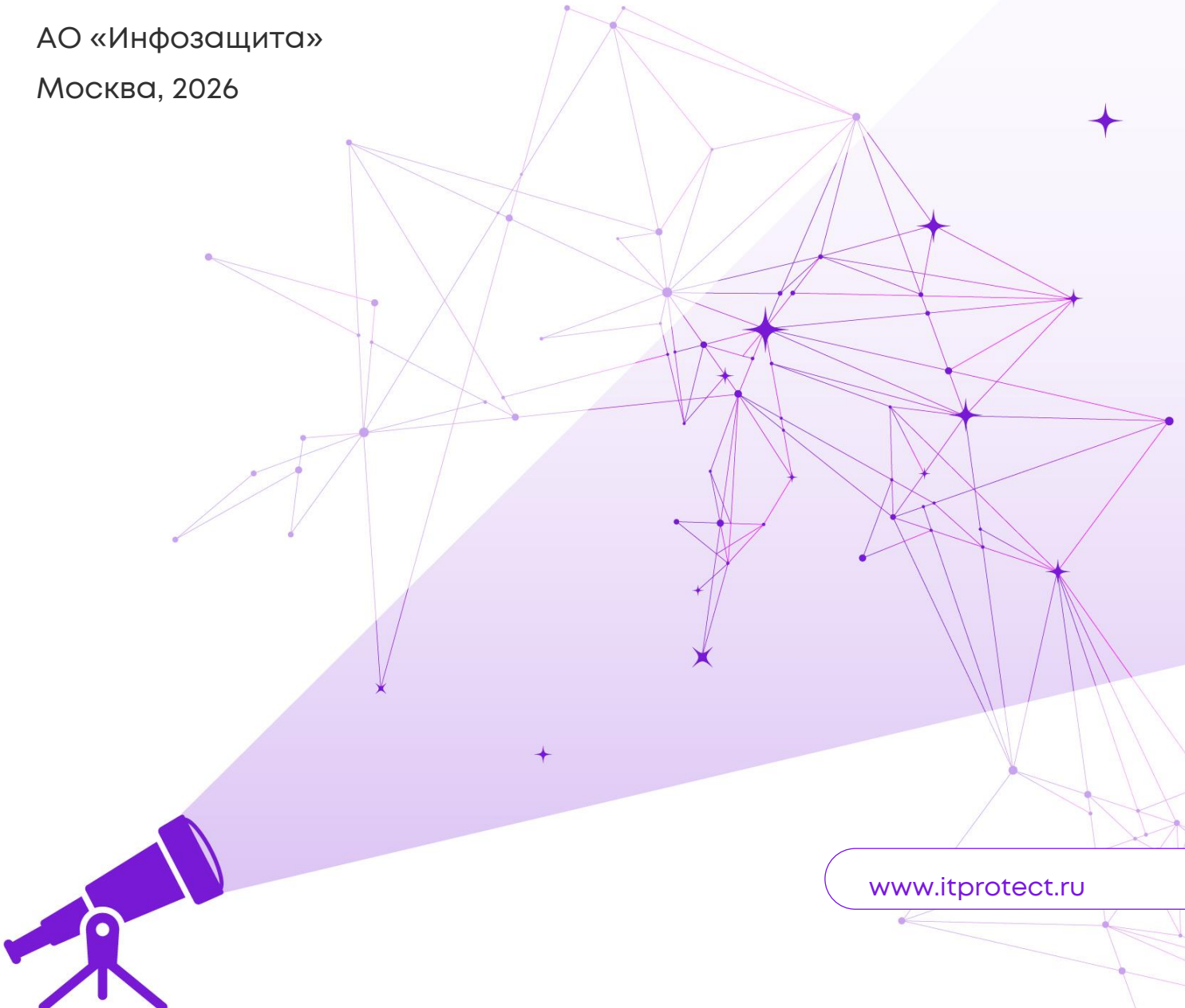
ОГРН 1087746313500,
ИНН КПП 7719672244 | 770201001

itprotect scout

ФУНКЦИОНАЛЬНЫЕ ХАРАКТЕРИСТИКИ

АО «Инфозащита»

Москва, 2026



Содержание

1 Введение

1.1 Назначение документа

Настоящий документ содержит описание функциональных характеристик программного обеспечения iTPROTECT Scout (далее — iTPROTECT Scout, Система), предназначенного для углублённой разведки киберугроз и оперативного анализа индикаторов компрометации в корпоративной инфраструктуре организаций.

Документ определяет состав функций системы, входные и выходные данные, условия выполнения функций и ожидаемые результаты согласно принятым требованиям к оформлению программной документации.

1.2 Область применения

iTPROTECT Scout представляет собой специализированную систему кибербразведки, ориентированную на профессиональное использование службами информационной безопасности организаций, внешними аудиторами и консультантами по кибербезопасности.

Система предназначена для решения следующих задач:

- глубокое профилирование внешней поверхности атаки с выявлением векторов проникновения;
- разведывательный анализ цифровых активов организации с картированием всех внешних точек входа;
- детальное профилирование сетевых служб с определением версий программного обеспечения и конфигураций;
- корреляция обнаруженных уязвимостей с известными эксплойтами и техниками атак;
- поиск цифровых следов организации в специализированных источниках кибербразведки;
- оперативное обнаружение модификаций в инфраструктуре для выявления подозрительной активности;

- формирование технических отчётов для служб безопасности с детализированными данными.

Ограничения области применения. iTPROTECT Scout является системой автоматизированной оценки внешней поверхности атаки (EASM) и принципиально отличается от средств тестирования на проникновение (пентеста). Различия фиксируются по следующим параметрам:

- Эксплуатация уязвимостей не выполняется. Цель системы — зафиксировать наличие технической возможности эксплуатации, а не доказать факт компрометации актива.
- Подбор паролей выполняется в ограниченном режиме password spraying — один-два популярных пароля на множество учётных записей. Классический перебор (bruteforce) — много паролей на одну учётную запись — не применяется.
- Покрытие — непрерывное по всей внешней поверхности Заказчика, а не разовая проверка согласованного сегмента инфраструктуры.

Активные проверки (например, сканирование портов в активном режиме, проверки на наличие уязвимостей по подтверждённым активам) выполняются только при наличии авторизационного письма Заказчика, фиксирующего согласие на их проведение. При выполнении исключительно пассивной разведки (OSINT) обращение к серверам Заказчика не происходит, и формальное наличие авторизационного письма не требуется.

Отсутствие обнаруженных уязвимостей в отчёте по результатам отдельного цикла сканирования не является гарантией их фактического отсутствия во внешнем периметре. Результат зависит от согласованного скоупа активов, выбранного профиля сканирования (см. раздел 2.1) и доступности активов на момент проверки.

Управление статусами обнаруженных проблем — «Без статуса», «В работе», «Исправлена», «Ложно-позитивная», «Игнорировать» — выполняется пользователем в личном кабинете и остаётся на стороне Заказчика. Изменение статусов не является обязательным для работы

сервиса; оно позволяет управлять отображением проблем и приоритизировать работу с ними.

1.3 Целевая аудитория

Основными пользователями iTPROTECT Scout являются:

Службы информационной безопасности организаций:

- Специалисты SOC (Security Operations Center);
- Аналитики по информационной безопасности;
- Администраторы безопасности корпоративных систем;
- Руководители подразделений ИБ.

Внешние аудиторы и консультанты:

- Специалисты по проведению аудита информационной безопасности;
- Консультанты по кибербезопасности;
- Эксперты по анализу защищённости;
- Специалисты по пентестингу и этичному хакингу.

Специализированные организации:

- Центры мониторинга информационной безопасности;
- Компании-интеграторы решений ИБ;
- Поставщики управляемых услуг безопасности (MSSP);
- Организации, проводящие расследования инцидентов безопасности.

2 Функциональные характеристики

Программное обеспечение iTPROTECT Scout реализует комплекс функций для углублённой разведки киберугроз и оперативного анализа индикаторов компрометации в корпоративной инфраструктуре. Система обеспечивает полный цикл работы с внешним периметром организации: обнаружение и

инвентаризацию активов, глубокий анализ уязвимостей, непрерывный мониторинг изменений и формирование технической отчётности.

Все функциональные возможности доступны через защищённый веб-интерфейс без необходимости установки локальных компонентов. Система работает в режиме SaaS (Software as a Service) и обеспечивает централизованное управление процессами сканирования и анализа результатов.

Далее представлено детальное описание реализованных функциональных возможностей в соответствии с требованиями технического задания.

2.1 Глубокое профилирование внешней поверхности атаки с выявлением векторов проникновения

В соответствии с требованиями к комплексному исследованию внешнего периметра организации, в системе iTPROTECT Scout реализованы следующие функциональные возможности:

2.1.1 Режимы запуска и профили сканирования

Система поддерживает два режима инициирования процесса профилирования:

- Ручной запуск сканирования выполняется оператором через веб-интерфейс. Администратор выбирает необходимый профиль сканирования, определяющий параметры и глубину анализа, после чего инициирует проверку активов проекта.
- Автоматическое сканирование по расписанию настраивается администратором для каждого проекта. Система позволяет добавить проект в расписание сканирований с заданной периодичностью выполнения проверок.

Система предусматривает следующие профили сканирования:

- Default — основной профиль для большинства сценариев мониторинга. Включает разведку и поиск уязвимостей по подтверждённым активам. Применяется в обычной ситуации для большинства проектов; стандартная регулярность — раз в неделю.
- OSINT — разведывательный профиль, выполняющий только сбор информации об активах Заказчика без проверки на уязвимости. Используется на этапе подготовки сделки, при подготовке пилота или в случаях, когда активные проверки ещё не согласованы. Результатом является перечень выявленных активов, требующих последующего подтверждения.
- Быстрая проверка — облегчённый профиль для оперативного отслеживания изменений внешнего периметра. Выполняется чаще (раз в день или раз в 6 часов); ограничивается проверкой открытых портов и предназначен для своевременного выявления кратковременно появляющихся точек входа.
- Enterprise — настраиваемый профиль под ресурсы конкретного Заказчика; параметры частоты, состава проверок и допустимой нагрузки согласуются индивидуально.

Настройка и поддержание актуальности профилей сканирования выполняются поставщиком услуги. Назначение и изменение профиля для конкретного проекта пользователя выполняется администратором сервиса.

2.1.2 Этапы автоматического сканирования

Автоматическое сканирование выполняется последовательно по трём этапам с разной периодичностью:

1. Разведка внешнего периметра (OSINT) — поиск доменов, поддоменов и связанных с организацией IP-адресов через анализ открытых источников. Выполняется без обращения к серверам Заказчика. Регулярность — раз в неделю.

2. Мониторинг утечек данных — ежедневная проверка опубликованных утечек, связанных с инфраструктурой организации, по нескольким источникам (см. раздел 2.5).
3. Проверка подтверждённых активов на наличие уязвимостей — детальное сканирование подтверждённых пользователем активов в соответствии с выбранным профилем (см. раздел 2.1.1). Регулярность — раз в неделю в профиле Default.

2.1.3 Процесс профилирования инфраструктуры

При выполнении сканирования система осуществляет комплексный анализ внешнего периметра организации.

Идентификация активов производится для всех подтверждённых доменов и IP-адресов организации. Каждый актив проходит проверку доступности, определение открытых портов и запущенных служб. Система фиксирует тип актива, его текущий статус и время обнаружения.

Анализ сетевых служб включает определение запущенных сервисов на открытых портах, извлечение баннеров и отпечатков служб, идентификацию используемых протоколов. Для каждой обнаруженной службы фиксируется порт, протокол (TCP/UDP) и дополнительная техническая информация.

2.1.4 Формирование карты поверхности атаки

По результатам сканирования система формирует комплексное представление внешней инфраструктуры организации.

Реестр активов представляет собой структурированный список всех цифровых активов организации. Каждый актив отображается с указанием уровня риска через цветовую индикацию (критический — красный, высокий — оранжевый, средний — жёлтый).

Для каждого актива указывается количество связанных проблем безопасности, дата первичного обнаружения и дата последней проверки.

Детальные карточки активов предоставляют исчерпывающую информацию о каждой точке входа в инфраструктуру. Карточка содержит общую

информацию об активе, DNS-записи для доменных имён, перечень всех связанных проблем безопасности и историю изменений. Интерфейс позволяет просматривать техническую информацию и отслеживать динамику изменений актива во времени.

2.1.5 Выявление уязвимых компонентов и векторов атак

Система автоматически анализирует собранную информацию для идентификации проблем безопасности и потенциальных векторов атак.

Обнаружение уязвимостей выполняется путём анализа версий программного обеспечения и конфигураций служб. Каждая выявленная уязвимость классифицируется по типу угрозы и получает числовую оценку риска. Система идентифицирует уязвимости через CVE-идентификаторы, определяет категорию проблемы и фиксирует технические параметры: затронутый IP-адрес, порт, протокол и службу.

Анализ векторов проникновения включает выявление всех потенциальных путей компрометации инфраструктуры. Система определяет реальные векторы атаки, где существуют подтверждённые уязвимости с доступными методами эксплуатации, и потенциальные векторы, представляющие теоретическую угрозу. Для каждого вектора формируется описание возможного сценария атаки.

Детализация проблем безопасности реализована через систему карточек проблем, содержащих техническое описание, уровень риска, категорию, затронутые компоненты, рекомендации по устранению и временные метрики.

2.1.6 Представление результатов профилирования

Результаты глубокого профилирования представляются в различных форматах для обеспечения полноты анализа состояния безопасности.

Дашборд системы отображает консолидированную информацию о состоянии защищённости. Общая оценка угроз представлена по шкале от 0 до 10, где визуально отображается текущий уровень риска. Статистика проблем разделена по уровням критичности с цветовой индикацией.

Отдельно выводится информация о скомпрометированных учётных данных и обнаруженных векторах атак с разделением на реальные и потенциальные угрозы.

Технические отчёты формируются в формате PDF и содержат полную информацию о результатах профилирования. Отчёты включают перечень всех обнаруженных активов, выявленные уязвимости с детальным описанием, анализ векторов атак и рекомендации по устранению проблем. Формат отчётов адаптирован для использования специалистами служб информационной безопасности.

2.2 Разведывательный анализ цифровых активов организации с картированием всех внешних точек входа

В соответствии с требованиями к ведению реестра цифровых активов и картированию инфраструктуры, в системе реализованы следующие функциональные возможности:

2.2.1 Организация активов в проектах

Активы в системе объединяются в проекты для проведения сканирования и формирования единой оценки состояния информационной безопасности. Проект является основной организационной единицей работы с системой: ключевые разделы личного кабинета — дашборд, список активов, список проблем — отображают данные применительно к выбранному проекту.

При регистрации пользователя в системе автоматически создаётся проект, в который пользователь добавляет активы. Как правило, у пользователя ведётся один проект; при необходимости пользователь может работать с несколькими проектами.

Для каждого проекта в системе фиксируются:

- Название проекта (длиной не менее 3 символов; пользователь может изменить его в любой момент);

- Дата последнего сканирования;
- Перечень добавленных активов с разделением по статусу подтверждения (подтверждённые, неподтверждённые, новые, исключённые).

Переключение между проектами, если у пользователя их несколько, выполняется через выпадающий список в верхней панели личного кабинета. Добавление активов в проект выполняется через интерфейс работы с проектом.

Удаление проектов в системе не предусмотрено.

2.2.2 Ведение реестра цифровых активов

Система обеспечивает полнофункциональное управление реестром цифровых активов организации через специализированный раздел «Активы».

Добавление активов в систему осуществляется пользователем или администратором сервиса вручную через веб-интерфейс. Поддерживается внесение доменных имён и IP-адресов, которые составляют внешний периметр организации.

Каждому пользователю при создании учётной записи назначается квота — базовый лимит в 50 активов, действующий на сумму подтверждённых активов во всех его проектах. Размер квоты задаётся целым числом не менее 0 и может быть изменён администратором сервиса.

Поведение системы при достижении лимита: пользователь не может самостоятельно добавить и подтвердить активы сверх установленной квоты. Администратор сервиса может подтвердить активы, добавленные сверх квоты, однако такие активы переводятся в категорию «Неподтверждённые» и не включаются в процесс сканирования до тех пор, пока остаток квоты пользователя не будет увеличен или количество подтверждённых активов не сократится. Уменьшение квоты ниже текущего количества подтверждённых активов не приводит к удалению существующих активов, но блокирует добавление новых.

Процесс подтверждения активов настраивается централизованно для сервиса и допускает два режима, описанных в подразделе 2.13.3: либо обязательное подтверждение администратором перед включением в сканирование, либо автоматическое подтверждение при добавлении пользователем. В обоих случаях процесс направлен на обеспечение контроля над областью сканирования.

Валидация активов выполняется системой автоматически при добавлении. Корректно введённые активы отображаются на вкладке «На проверку», где администратор может подтвердить их принадлежность организации. Система контролирует формат вводимых данных и предотвращает добавление некорректных записей.

2.2.3 Управление и категоризация активов

Реестр активов предоставляет расширенные возможности управления и анализа.

Статусы и состояния активов отображаются в едином интерфейсе с возможностью быстрой визуальной оценки. Каждый актив имеет индикацию уровня риска через цветовую схему (см. раздел 2.1.4). Система отображает количество связанных с активом проблем безопасности.

Фильтрация и поиск реализованы для эффективной работы с большими объёмами данных. Список активов поддерживает фильтрацию по следующим параметрам:

- Уровень риска — отображение активов в соответствии с одним или несколькими уровнями (критический, высокий, средний, низкий);
- DNS-записи (только для активов типа «домен»);
- TCP-порты (только для активов типа «IP-адрес»).

Поисковая система позволяет быстро находить конкретные активы по названию или части адреса.

Сортировка активов поддерживается по всем ключевым параметрам: названию актива, уровню риска, типу, дате последнего обнаружения, дате первичного обнаружения. Для доменов дополнительно доступна

сортировка по DNS-записям. Направление сортировки изменяется нажатием на заголовок соответствующего столбца.

2.2.4 Детальные карточки активов

Для каждого актива в системе формируется подробная карточка с исчерпывающей информацией.

Общая информация об активе включает основные характеристики: тип актива, текущий статус, уровень риска, даты первого и последнего обнаружения. Отображается принадлежность к проекту и общая статистика по связанным проблемам.

DNS-информация для доменов представлена на отдельной вкладке карточки. Система отображает все DNS-записи домена, включая A, AAAA, MX, TXT, NS и другие типы записей. Это позволяет получить полное представление о конфигурации DNS и выявить потенциальные проблемы настройки.

Связанные проблемы безопасности отображаются непосредственно в карточке актива. Каждая проблема представлена с указанием уровня риска, CVE-идентификатора (при наличии), категории угрозы. Из карточки актива можно перейти к детальному описанию любой связанной проблемы.

История изменений актива фиксирует все модификации, обнаруженные в процессе мониторинга. Система отслеживает изменения в DNS-записях, появление или исчезновение служб, изменение статуса доступности.

2.2.5 Картирование точек входа

Система выполняет комплексное картирование всех внешних точек входа в инфраструктуру организации.

Автоматическое обнаружение связей между активами реализовано на основе анализа DNS-записей, WHOIS-информации и сетевой топологии. Система выявляет взаимосвязи между доменами и IP-адресами, определяет принадлежность к единой инфраструктуре.

Визуализация инфраструктуры через интерфейс активов позволяет получить целостное представление о внешнем периметре. Группировка по уровню риска помогает приоритизировать работу с проблемными активами.

2.2.6 Интеграция с процессом сканирования

Реестр активов тесно интегрирован с подсистемой сканирования.

Автоматическое обновление информации происходит после каждого сканирования. Система обновляет статусы активов, уровни риска, списки обнаруженных проблем. Новая информация немедленно отображается в реестре и карточках активов.

Обнаружение новых активов в процессе сканирования приводит к их добавлению в реестр с пометкой о необходимости подтверждения. Администратор получает уведомление о появлении новых объектов и может принять решение о их включении в периметр мониторинга.

2.3 Детальное профилирование сетевых служб с определением версий ПО и конфигураций

В соответствии с требованиями к исследованию сетевых служб и идентификации технологического стека, в системе реализованы следующие функциональные возможности:

2.3.1 Обнаружение и идентификация сетевых служб

Система выполняет комплексное исследование всех доступных сетевых служб на обнаруженных активах.

Сканирование портов и протоколов осуществляется для каждого подтверждённого актива. Система идентифицирует открытые TCP и UDP порты, определяет запущенные на них службы. Для каждого обнаруженного порта фиксируется номер порта, используемый протокол транспортного уровня, тип и название службы.

Идентификация программного обеспечения выполняется через анализ баннеров служб и специфических откликов. Система определяет типы сервисов, включая веб-серверы (Apache, Nginx, IIS), почтовые серверы, базы данных, службы удалённого доступа. Для каждой службы, где это технически возможно, определяется версия программного обеспечения.

2.3.2 Анализ конфигураций и настроек безопасности

Система проводит детальный анализ конфигурационных параметров обнаруженных служб.

Выявление небезопасных конфигураций включает обнаружение служб с настройками по умолчанию, использование устаревших или небезопасных протоколов, отсутствие необходимых механизмов защиты. Каждая выявленная проблема конфигурации классифицируется по уровню риска.

Анализ криптографических параметров выполняется для служб, использующих шифрование. Система проверяет поддерживаемые алгоритмы шифрования, выявляет использование слабых криптографических алгоритмов (например, «Weak Encryption Algorithm(s) Supported (SSH)» или «Weak MAC Algorithm(s) Supported (SSH)»). Данные проблемы отображаются в общем реестре с указанием уровня риска.

2.3.3 Технологический стек и взаимосвязи

Определение технологического стека происходит через комплексный анализ всех обнаруженных компонентов. Система идентифицирует используемые технологии веб-приложений, определяет категории служб (например, «Web application abuses» для веб-приложений), выявляет специфические технологии защиты, такие как Anti-Scanner Defenses.

Категоризация служб реализована через систему классификации проблем. Каждая обнаруженная служба и связанная с ней проблема относится к определённой категории, что позволяет быстро оценить профиль технологических рисков организации.

2.3.4 Мониторинг состояния служб

Система отслеживает изменения в составе и конфигурации сетевых служб.

Фиксация времени обнаружения каждой службы и связанной проблемы позволяет отслеживать динамику изменений. Для каждой проблемы указывается дата первого обнаружения, дата последнего подтверждения, время жизни проблемы.

Отслеживание изменений в конфигурации служб происходит при каждом сканировании. Система фиксирует появление новых служб, изменение версий программного обеспечения, модификацию конфигурационных параметров.

2.3.5 Интеграция с оценкой рисков

Результаты профилирования сетевых служб интегрируются в общую систему оценки рисков.

Результаты профилирования сетевых служб интегрируются в общую систему оценки рисков, описанную в разделе 2.8.

Приоритизация проблем основана на совокупной оценке риска службы и связанных уязвимостей. Службы классифицируются по уровню риска согласно общей системе цветовой индикации (см. раздел 2.1.4).

2.4 Корреляция обнаруженных уязвимостей с известными эксплойтами и техниками атак

В соответствии с требованиями к сопоставлению выявленных уязвимостей с базами данных известных эксплойтов, в системе реализованы следующие функциональные возможности:

2.4.1 Идентификация уязвимостей через стандартизированные базы

Система выполняет автоматическое сопоставление обнаруженных проблем безопасности с международными базами уязвимостей по цепочке:

точная версия программного обеспечения (CPE) → база уязвимостей и метрик эксплуатации (NVD, EPSS, KEV) → список применимых CVE-идентификаторов → приоритизация.

Использование CVE-идентификаторов обеспечивает однозначную идентификацию известных уязвимостей. Каждая обнаруженная уязвимость, присутствующая в базе CVE, маркируется соответствующим идентификатором (например, CVE-2010-4755, CVE-2021-41617, CVE-2021-27065). Система предоставляет ссылки на базы CVE/NVD для получения детальной информации об эксплойтах и методах атаки.

Оценка применимости эксплойтов выполняется для каждой идентифицированной CVE-уязвимости с учётом следующих источников:

- NVD (National Vulnerability Database) — базовые характеристики уязвимости, описание, оценка по CVSS;
- EPSS (Exploit Prediction Scoring System) — вероятность реальной эксплуатации уязвимости в течение ближайшего периода;
- KEV (Known Exploited Vulnerabilities, CISA) — перечень уязвимостей, для которых зафиксированы факты активной эксплуатации в актуальных атаках.

Совместное использование этих источников позволяет выделить уязвимости, имеющие наибольший приоритет с точки зрения вероятности применения в реальной атаке.

Доступность результатов для пользователя. На текущем этапе развития продукта результаты корреляции CPE → CVE по баннерам сетевых служб включаются в технические отчёты (см. раздел 2.7). Их отображение непосредственно в личном кабинете отнесено к перспективным направлениям развития интеграционных возможностей системы. Система определяет, существуют ли публично доступные эксплойты для конкретной версии программного обеспечения и конфигурации службы.

2.4.2 Анализ техник атак

Категоризация по типам атак позволяет оценить характер угроз. Уязвимости классифицируются по категориям возможных атак, например «Web application abuses» для атак на веб-приложения, что помогает понять потенциальные векторы компрометации.

Оценка сложности эксплуатации отражается в числовой оценке риска. Уязвимости с простыми методами эксплуатации получают более высокую оценку риска, учитывая вероятность их использования злоумышленниками.

2.4.3 Определение критичности в контексте инфраструктуры

Расчёт уровня риска выполняется с учётом базовой оценки CVE и контекста инфраструктуры согласно методологии, описанной в разделе 2.8.

Приоритизация по вероятности эксплуатации обеспечивает фокус на наиболее опасных уязвимостях. Проблемы с известными эксплойтами и простыми методами атаки получают повышенный приоритет и выделяются соответствующей цветовой индикацией (см. раздел 2.1.4).

2.5 Поиск цифровых следов организации в специализированных источниках киберразведки

В соответствии с требованиями к мониторингу утечек данных и обнаружению признаков компрометации, в системе реализованы следующие функциональные возможности:

2.5.1 Источники мониторинга утечек

Утечки — это учётные данные (логины, пароли, адреса электронной почты, номера телефонов и персональные сведения), оказавшиеся доступными третьим лицам в результате преднамеренных действий или по случайным причинам.

Поиск утечек выполняется ежедневно на основе информации из открытых источников. В систему попадают все опубликованные утечки, связанные с активами организации. Утечки, связанные с инфраструктурой организации, разделяются по характеру источника:

Пользовательские — учётные данные сотрудников и иная чувствительная информация, обнаруженная во внешних публичных источниках.

- Клиентские — данные, связанные с публичными доменами организации, при этом сами учётные записи принадлежат внешним почтовым сервисам. Такие находки указывают на компрометацию клиентов или контрагентов, использующих сервисы организации, а не сотрудников.
- Стиллер-логи — данные, собранные вредоносным программным обеспечением типа stealer с заражённых рабочих станций, где зафиксировано взаимодействие с инфраструктурой организации.
- Стиллер-логи с мобильных устройств — данные, собранные стиллерами с Android-устройств, связанные с приложениями и сервисами организации.

Найденные утечки отображаются в личном кабинете в виде списка, сгруппированного по источникам. При раскрытии источника отображаются обнаруженные в нём учётные записи: e-mail, опубликованные поля учётной записи, а также пароль и телефон (если содержатся в утечке) — пароли и телефоны выводятся частично скрытыми.

Часть утечек может быть объединена в источник «Unknown» — это, как правило, данные, похищенные стиллерами. Такие случаи требуют отдельного внимания: помимо смены паролей, рекомендуется проверка рабочих станций на наличие вредоносного программного обеспечения.

2.5.2 Управление статусами утечек

Для каждой утечки и для каждого источника предусмотрено управление статусом:

- Актуальна — статус, присваиваемый системой автоматически всем вновь обнаруженным утечкам;

- Не актуальна — статус, который пользователь устанавливает вручную, отмечая утечку как обработанную.

Автоматическая смена статуса системой не предусмотрена. Статусы позволяют пользователю отмечать обработанные данные и одновременно влияют на отображение статистики: утечки со статусом «Не актуальна» не учитываются в отчётах и на дашборде.

Статус можно изменить как у отдельной записи, так и у источника целиком — в этом случае статус каскадно обновляется для всех входящих в источник утечек. Если все утечки источника помечены как «Не актуальна», источник также получает этот статус; если хотя бы одна утечка остаётся актуальной, источник считается актуальным.

Список утечек поддерживает фильтрацию по статусу: «Актуальные» (отображаются источники с хотя бы одной актуальной утечкой), «Не актуальные» (источники без актуальных утечек), «Все» (без фильтра).

2.5.3 Уведомления об утечках

При выявлении новых утечек сервис направляет пользователю уведомление по электронной почте. Письмо содержит информацию о факте обнаружения новых утечек и уточнение, присутствуют ли в них пароли; сами данные утечек по почте не передаются и доступны только в личном кабинете и отчётах.

Уведомления включены по умолчанию при активной подписке и могут быть отключены в период тестирования сервиса или при отсутствии оплаченной подписки.

Актуальные утечки отображаются на дашборде и включаются в отчёты как отдельный показатель состояния информационной безопасности организации. Утечки со статусом «Не актуальна» не учитываются в отчётах и на дашборде.

2.6 Оперативное обнаружение модификаций в инфраструктуре для выявления подозрительной активности

В соответствии с требованиями к выявлению изменений в инфраструктуре и идентификации признаков компрометации, в системе реализованы следующие функциональные возможности:

2.6.1 Отслеживание изменений между сканированиями

Система выполняет сравнительный анализ результатов последовательных сканирований для выявления изменений в инфраструктуре.

Фиксация новых объектов происходит при обнаружении ранее отсутствовавших элементов инфраструктуры. Система идентифицирует появление новых активов, открытие ранее закрытых портов, запуск новых служб. Все новые объекты требуют подтверждения администратором для включения в периметр мониторинга.

Мониторинг исчезновения элементов отслеживает прекращение доступности ранее обнаруженных компонентов. Система фиксирует закрытие портов, остановку служб, недоступность активов.

2.6.2 Временные метрики изменений

Фиксация временных характеристик обеспечивает понимание динамики изменений. Для каждого элемента инфраструктуры система сохраняет:

- Дату первого обнаружения объекта;
- Дату последнего подтверждения наличия;
- Время жизни проблемы или актива.

Классификация изменений по критичности выполняется автоматически на основе характера модификаций. Появление новых критических уязвимостей или высокорисковых служб получает повышенный приоритет и отражается в общей оценке угроз.

2.6.3 Индикация подозрительной активности

Выделение аномальных изменений происходит через систему цветовой индикации и уровней риска. Изменения, потенциально указывающие на компрометацию или подготовку к атаке, выделяются соответствующим уровнем угрозы.

Обновление статусов после сканирования обеспечивает актуализацию данных в системе. После завершения каждого сканирования все изменения отражаются в дашборде, реестре активов и связанных карточках.

2.7 Технические отчёты для служб безопасности с детализированными данными

В соответствии с требованиями к формированию подробных технических отчётов для специалистов ИБ, в системе реализованы следующие функциональные возможности:

2.7.1 Формирование отчётов в формате PDF

Система обеспечивает генерацию технических отчётов через специализированный раздел «Отчёты».

Создание отчётов выполняется на основе актуальных данных о состоянии инфраструктуры. Система формирует документ, содержащий результаты последнего сканирования, перечень обнаруженных проблем и рекомендации по устранению.

Скачивание документов реализовано в формате PDF, что обеспечивает универсальность использования и сохранение форматирования. Отчёты доступны для загрузки непосредственно из веб-интерфейса системы.

2.7.2 Управление отчётами

Раздел «Отчёты» предоставляет централизованный доступ к сформированным документам. Интерфейс позволяет просматривать

список доступных отчётов, выполнять их скачивание для дальнейшего использования.

Пагинация и настройка отображения обеспечивают удобную работу с большим количеством отчётов. Система поддерживает настройку количества отображаемых записей и навигацию по страницам.

2.8 Детализированная оценка критичности угроз на основе вероятности эксплуатации

В соответствии с требованиями к расчёту критичности угроз с учётом вероятности их эксплуатации, в системе реализованы следующие функциональные возможности:

2.8.1 Интегральная оценка уровня угроз

Общий показатель безопасности рассчитывается системой автоматически и отображается на дашборде по шкале от 0 до 10. Визуальное представление оценки позволяет мгновенно определить текущий уровень защищённости инфраструктуры, где 0 соответствует отсутствию угроз, а 10 — критическому уровню опасности.

По умолчанию общая оценка угроз проекта равна максимальному уровню риска среди всех его активов. Уровень риска отдельного актива, в свою очередь, определяется как наибольший уровень риска среди связанных с ним проблем. Расчёт риска отдельной проблемы выполняется по методологии CVSS (Common Vulnerability Scoring System).

Градация уровней риска по итоговому показателю:

- 0,1–4,9 — низкий риск: вероятность угроз минимальна, последствия незначительны;
- 5,0–6,9 — средний риск: возможны угрозы, требующие внимания;
- 7,0–8,9 — высокий риск: высокий уровень угроз, необходимы срочные меры;

- 9,0–10,0 — критический риск: чрезвычайная опасность, требующая немедленных действий, возможны катастрофические последствия.

2.8.2 Индивидуальная оценка каждой угрозы

Числовая оценка риска присваивается каждой обнаруженной проблеме индивидуально. Значения варьируются в зависимости от характеристик угрозы (например, «3.4» для проблем среднего уровня, «10.0» для критических уязвимостей).

Факторы оценки включают техническую сложность эксплуатации, доступность уязвимого компонента из интернета, потенциальное воздействие на инфраструктуру. Система учитывает контекст конкретной инфраструктуры при определении итогового уровня риска.

2.8.3 Распределение угроз по категориям критичности

Группировка по уровням опасности представлена на дашборде в виде счётчиков:

- Критические угрозы (красная индикация)
- Высокие угрозы (оранжевая индикация)
- Средние угрозы (жёлтая индикация)

Такое распределение позволяет быстро оценить профиль рисков и приоритизировать работу по устранению проблем.

2.9 Экспертные рекомендации по реагированию на сложные векторы атак

В соответствии с требованиями к предоставлению рекомендаций по устранению угроз, в системе реализованы следующие функциональные возможности:

2.9.1 Рекомендации в карточках проблем

Текстовые описания проблем содержатся в каждой карточке обнаруженной уязвимости. Система предоставляет техническое описание сути проблемы, объясняющее характер угрозы и потенциальные последствия её эксплуатации.

Решения по устранению включены в карточку каждой проблемы в специальном поле "Решение". Рекомендации содержат конкретные шаги по нейтрализации угрозы, адаптированные для технических специалистов служб информационной безопасности.

2.9.2 Техническая детализация рекомендаций

Привязка к конкретным компонентам обеспечивает точность рекомендаций. Каждое решение учитывает специфику затронутого актива, службы, порта и протокола, что позволяет применять рекомендации без дополнительной адаптации.

2.10 Углублённый анализ нестандартных угроз силами экспертов

В дополнение к автоматическому сканированию (см. разделы 2.1–2.6) в составе услуги предусмотрены экспертные проверки внешней инфраструктуры Заказчика, выполняемые специалистами по кибербезопасности. Эти проверки дополняют результаты автоматического сканирования и направлены на находки, требующие ручной интерпретации, специфичных техник или проверки в нестандартных сценариях.

2.10.1 Состав экспертных проверок

Состав регулярных экспертных проверок включает:

- Поиск служебных и конфигурационных файлов в публичном доступе — обнаружение открытых логов, файлов системы контроля версий (например, .git), оставленных конфигурационных файлов через механизмы поисковой выдачи (Google Dorks);

- Ручная обработка утечек, не закрытых автоматическим контуром (см. раздел 2.5);
- Поиск форм входа в публичных приложениях Заказчика с последующей проверкой устойчивости к ограниченной атаке методом password spraying (1–2 попытки на учётную запись; см. раздел 1.2 «Ограничения области применения»);
- Фаззинг и перебор путей на веб-серверах с использованием инструментов уровня ffuf и dirsearch и расширенных словарей путей;
- Ручной разбор отдельных открытых портов — служб SNMP, SSH и других — на предмет небезопасных конфигураций;
- Расширенная проверка параметров SSL/TLS на портах за пределами стандартных веб-сервисов (IMAP, POP3 и иные) по рекомендациям Mozilla Foundation (Intermediate / Modern);
- Дополнительные проверки веб-приложений с использованием шаблонов сканера Nuclei (формы входа, шаблоны под распространённые платформы Bitrix, WordPress, собственные шаблоны команды);
- Сверка IP-адресов Заказчика с публичными списками скомпрометированной инфраструктуры (в том числе списками известных ботнет-узлов).

2.10.2 Применимость и взаимодействие с автоматическим сканированием

Результаты экспертных проверок передаются Заказчику в составе технической отчётности (см. раздел 2.7). Решение о реагировании на каждую находку остаётся за службой информационной безопасности Заказчика. Параметры регулярности, объёма и сроков выполнения экспертных проверок фиксируются в спецификации услуги.

2.11 Расширенные настройки для профессиональных пользователей

В соответствии с требованиями к реализации расширенных возможностей настройки для профессиональных пользователей, в системе реализованы следующие функциональные возможности:

2.11.1 Управление профилем и безопасностью

Раздел настроек личного кабинета предоставляет пользователю доступ к управлению параметрами собственной учётной записи и безопасности доступа.

Доступные возможности включают:

- Редактирование профиля пользователя (имя и фамилия, телефон, должность, информация об организации)
- Изменение пароля учётной записи
- Настройку двухфакторной аутентификации (2FA)
- Управление активными сессиями с возможностью их завершения

Детальное описание двухфакторной аутентификации и управления сессиями приведено в подразделах 2.11.2 и 2.11.3.

2.11.2 Двухфакторная аутентификация

Активация 2FA выполняется через приложение-аутентификатор на мобильном устройстве. Система генерирует QR-код для связывания учётной записи с приложением. После сканирования кода пользователь вводит 6-значный код из приложения для подтверждения привязки.

Процесс аутентификации после активации 2FA требует ввода дополнительного кода при каждом входе в систему. При включении двухфакторной аутентификации система отправляет пользователю уведомление по электронной почте.

Отключение 2FA доступно в настройках безопасности. Для отключения необходимо ввести актуальный код из приложения-аутентификатора.

2.11.3 Управление сессиями

Контроль активных сессий отображает все открытые подключения к учётной записи с информацией о времени и месте входа. Пользователь может завершить любую подозрительную сессию, обеспечивая дополнительный уровень контроля доступа.

2.12 Защищённый веб-доступ с расширенными настройками безопасности для работы с конфиденциальными данными

В соответствии с требованиями к обеспечению безопасного доступа к системе без установки локальных компонентов, реализованы следующие функциональные возможности:

2.12.1 Веб-интерфейс системы

Доступ через браузер обеспечивает работу с системой без необходимости установки дополнительного программного обеспечения. Система функционирует в режиме SaaS (Software as a Service) и доступна через защищенное соединение.

Поддержка современных браузеров гарантирует совместимость с актуальными версиями Chrome/Chromium, Safari, Firefox, Microsoft Edge. Интерфейс адаптирован для корректного отображения во всех поддерживаемых браузерах.

2.12.2 Механизмы защиты доступа

Защищенное соединение реализовано через использование протокола HTTPS для всех взаимодействий с системой. Это обеспечивает шифрование передаваемых данных между браузером пользователя и серверами системы.

Контроль доступа к данным обеспечивается через систему авторизации с уникальными учётными записями для каждого пользователя. Разграничение прав доступа гарантирует, что пользователи имеют доступ только к данным своей организации.

2.13 Управление учётными записями пользователей и квотами

Система обеспечивает централизованное управление учётными записями пользователей и количественными ограничениями на работу с системой. Управление выполняется на стороне правообладателя в режиме SaaS и не требует развёртывания административных компонентов в инфраструктуре Заказчика.

2.13.1 Способы создания учётных записей

Поддерживаются два способа создания учётных записей:

- Создание администратором. Учётная запись формируется администратором с заданием параметров профиля пользователя (контактные данные, организация, отрасль, должность, адрес сайта, название проекта по умолчанию). При создании может быть включена опция отправки приглашения по электронной почте, по ссылке из которого пользователь устанавливает пароль; в этом случае указывать пароль администратору не требуется. Дополнительно может быть включено требование смены пароля при первом входе. Учётные записи, созданные администратором, готовы к работе сразу и не требуют отдельной процедуры активации.
- Самостоятельная регистрация пользователя. Пользователь регистрируется через публичную форму. Регистрация ограничена чёрным списком доменов, исключающим публичные почтовые сервисы (например, Gmail, Yahoo, Outlook) и временные почтовые сервисы (например, Mailinator, TempMail), что обеспечивает регистрацию только

с корпоративных адресов. До завершения процедуры активации администратором пользователь не имеет доступа к сервису.

Требования к паролю: длина не менее 12 символов, обязательное наличие латинских символов в верхнем и нижнем регистре, цифр и специальных символов.

2.13.2 Процедура самостоятельной регистрации и активации

Пользователь, регистрирующийся самостоятельно, последовательно проходит следующие этапы с использованием пошагового помощника:

a. Создание учётной записи;
b. Подтверждение адреса электронной почты — в штатном режиме выполняется пользователем по ссылке из письма; при необходимости может быть выполнено администратором вручную;
c. Заполнение профиля организации;
d. Создание проекта;
e. Добавление активов в проект.

После прохождения этих этапов учётная запись поступает на рассмотрение администратору. Заявка на активацию отображается у администратора в одном из статусов: «Не заполнен», «Готов к проверке», «Ожидает проверки», «Активирован».

Активация выполняется администратором с возможностью предварительного анализа добавленных пользователем активов — недопустимые активы могут быть помечены как несканируемые, а попадающие под критерии чёрного списка могут быть включены в него до активации.

2.13.3 Подтверждение активов

Режим подтверждения активов настраивается централизованно для всего сервиса и допускает два варианта:

- Активы, добавленные пользователем, требуют подтверждения администратором — на каждое добавление формируется заявка со статусом «Pending» (не обработана) или «Processed» (обработана);
- Активы автоматически подтверждаются при добавлении пользователем без участия администратора.

В режиме подтверждения администратор может обрабатывать активы индивидуально или группами в рамках одной заявки. При отклонении актива администратор указывает причину.

Если суммарное количество активов в заявке превышает остаток квоты пользователя, администратор по-прежнему может подтвердить активы — однако в этом случае они переводятся в категорию «Неподтверждённые» и не включаются в процесс сканирования до увеличения квоты.

2.13.4 Изменение параметров учётной записи

Администратору доступны следующие операции с учётной записью пользователя:

- Редактирование параметров профиля — контактные данные, информация об организации и должности;
- Изменение пароля напрямую администратором либо установка требования смены пароля пользователем при следующем входе. Для немедленного применения требования смены пароля могут быть принудительно завершены активные сессии пользователя;
- Сброс настроек двухфакторной аутентификации — применяется в ситуации, когда пользователь утратил доступ к приложению-аутентификатору;
- Завершение активных сессий — администратор видит список открытых сессий пользователя (токен, IP-адрес, идентификатор браузера, время создания, время последней активности, время истечения) и может завершить выбранные сессии;
- Блокировка учётной записи с обязательным указанием причины. Заблокированный пользователь видит соответствующее уведомление

при попытке авторизации. Разблокировка выполняется с указанием причины. История блокировок и разблокировок сохраняется в карточке пользователя;

- Отключение уведомлений заблокированного пользователя — выполняется отдельно при необходимости.

Удаление учётной записи как операция в системе не предусмотрено: для прекращения доступа пользователя к сервису используется блокировка.

2.13.5 Управление квотами пользователей

Квота определяет максимальное количество активов, которое пользователь может одновременно держать в категории «Подтверждённые» суммарно по всем своим проектам. Квота задаётся целым числом не менее 0.

Значение квоты 0 фактически блокирует возможность пользователя добавлять и подтверждать новые активы. Если администратор уменьшает квоту до значения ниже текущего количества подтверждённых активов пользователя — существующие активы сохраняются без изменений, но добавление или подтверждение новых блокируется до увеличения квоты или сокращения количества подтверждённых активов.

Создание квоты выполняется одним из двух способов:

- Автоматическое — при создании учётной записи или при активации самостоятельно зарегистрированного пользователя система устанавливает базовую квоту 50 активов;
- Ручное — администратор может задать квоту индивидуально через интерфейс управления.

Изменение размера квоты выполняется администратором в любой момент.

2.14 Уведомления пользователей

Система направляет пользователю уведомления о значимых событиях по электронной почте на адрес, привязанный к учётной записи. Перечень событий, по которым предусмотрены уведомления:

- События регистрации — подтверждение адреса электронной почты, активация учётной записи и другие сопутствующие события. Уведомления этой группы отправляются только пользователям, прошедшим самостоятельную регистрацию.
- Блокировка и разблокировка учётной записи.
- Изменение пароля учётной записи.
- Установка требования сменить пароль при следующем входе.
- Включение и отключение двухфакторной аутентификации.
- Авторизация в сервисе.
- Завершение сканирования активов проекта.
- Загрузка отчёта в раздел «Отчёты» личного кабинета.
- Обнаружение новых утечек — подробное описание содержания уведомления приведено в подразделе 2.5.3.

Адрес электронной почты, на который направляются уведомления, соответствует адресу учётной записи и не настраивается отдельно. Часть уведомлений может быть отключена администратором сервиса индивидуально для конкретного пользователя — например, на период тестирования сервиса или при отсутствии оплаченной подписки.

Для уведомлений поддерживается выбор языка.

3 Системные требования

3.1 Требования к серверной части

Поскольку iTPROTECT Scout функционирует в режиме SaaS, серверная инфраструктура полностью обеспечивается правообладателем. Система развёрнута в облачной инфраструктуре и не требует установки серверных компонентов на стороне пользователя.

3.2 Требования к клиентской части

3.2.1 Минимальные аппаратные требования

Компонент	Требования
Процессор	64-разрядный процессор с тактовой частотой 2,1 ГГц или выше, количество ядер — 2 или более
Оперативная память	4 ГБ или более
Свободное дисковое пространство	10 ГБ или более
Разрешение экрана	1280×1024 пикселей или выше
Сетевой адаптер	Ethernet-адаптер с поддержкой скорости 100 Мбит/с или выше

3.2.2 Минимальные программные требования

Компонент	Требования
Операционная система	Windows 10 (версия 1909 или новее), Windows 11 macOS 10.14 (Mojave) или новее Linux (Ubuntu 20.04 LTS или новее, RHEL 8 или новее)
Веб-браузер	Google Chrome версии 90 или новее Mozilla Firefox версии 88 или новее Microsoft Edge версии 90 или новее

Компонент	Требования
	Safari версии 14 или новее Opera версии 76 или новее

3.2.3 Сетевые требования

Параметр	Требования
Скорость подключения к сети Интернет	100 Мбит/с или выше
Протоколы	HTTPS (TLS 1.2 или выше)
Порты	TCP 443 (HTTPS)
Стабильность соединения	Постоянное подключение к сети Интернет

4 Входные и выходные данные

4.1 Типы входных данных

Система iTPROTECT Scout принимает и обрабатывает следующие типы входных данных для анализа внешней инфраструктуры организации:

4.1.1 Доменные имена

Система поддерживает добавление доменных имён различных уровней для включения в периметр сканирования. Поддерживаются домены второго и последующих уровней. Для каждого домена система автоматически выполняет:

- Валидацию корректности формата доменного имени;
- Разрешение DNS-записей;

- Определение связанных IP-адресов;
- Выявление поддоменов.

4.1.2 IP-адреса

Система принимает как отдельные IP-адреса, так и диапазоны адресов для сканирования:

- IPv4-адреса в стандартном формате;
- IPv6-адреса;
- Валидация корректности формата IP-адресов при вводе.

4.1.3 Ограничения и валидация

При добавлении активов в систему действуют следующие правила:

- Базовый лимит — 50 активов на пользователя (квота, действует суммарно на все проекты пользователя; может быть изменена администратором сервиса);
- Все активы проходят процедуру валидации формата при добавлении;
- Перед включением в сканирование актив должен пройти подтверждение в соответствии с настройками сервиса: обязательное подтверждение администратором либо автоматическое подтверждение при добавлении пользователем (см. раздел 2.13.3);
- Некорректные записи автоматически отклоняются системой.

4.2 Форматы выходных данных

4.2.1 Технические отчёты

Основным форматом экспорта результатов анализа являются технические отчёты в формате PDF, которые формируются системой на основе актуальных данных о состоянии инфраструктуры. Отчёты содержат результаты последнего выполненного сканирования, включая полный

перечень обнаруженных проблем безопасности с их детальным описанием и экспертными рекомендациями по устранению выявленных уязвимостей.

Доступ к сформированным отчётам осуществляется через специализированный раздел «Отчёты» веб-интерфейса системы, откуда документы могут быть загружены для дальнейшего использования. Формат PDF обеспечивает универсальность использования и сохранение форматирования при передаче между различными системами. Отчёты предназначены для документирования текущего состояния безопасности инфраструктуры и адаптированы для использования специалистами служб информационной безопасности.

4.2.2 Веб-интерфейс

Интерактивное представление данных через веб-интерфейс включает:

- Дашборд с визуализацией общей оценки угроз (0—10) и статистикой по уровням критичности;
- Таблицы активов с возможностью фильтрации, сортировки и пагинации;
- Карточки активов с детальной информацией, DNS-записями, связанными проблемами;
- Карточки проблем с техническим описанием, CVE-идентификаторами, рекомендациями;
- Визуальные индикаторы уровней риска через цветовую схему.

4.2.3 Структурированные данные

Система обеспечивает представление данных в структурированном виде:

- Перечень активов с атрибутами (тип, риск, статус, проблемы);
- Список проблем с техническими параметрами (CVE, CVSS, категория, порт, протокол);
- Временные метрики (даты обнаружения, время жизни проблем);
- Статистика по категориям угроз и векторам атак.

4.3 Интеграционные возможности

4.3.1 Веб-доступ

Система функционирует в режиме SaaS и предоставляет:

- Защищённый доступ через HTTPS-протокол;
- Поддержку современных браузеров (Chrome/Chromium, Safari, Firefox, Microsoft Edge);
- Работу без установки локальных компонентов;
- Централизованное управление через веб-интерфейс.

4.3.2 Экспорт данных

На текущий момент реализованы следующие возможности экспорта результатов работы системы:

- Выгрузка результатов сканирования в формате CSV. Система автоматически формирует CSV-файл по результатам очередного сканирования. О готовности новой выгрузки пользователь получает уведомление по электронной почте; сам файл доступен для скачивания из личного кабинета. CSV-выгрузка содержит результаты сканирования в структурированном виде и предназначена для дальнейшей обработки во внешних системах Заказчика.
- Скачивание технических отчётов в формате PDF через раздел «Отчёты» личного кабинета. Каждый отчёт содержит результаты последнего выполненного сканирования и доступен для загрузки отдельным файлом;
- Пакетная загрузка нескольких отчётов одним ZIP-архивом — для случаев, когда требуется получить несколько отчётов за один шаг;

Структура отчёта включает краткую сводку, ориентированную на восприятие за несколько минут (векторы атак, таблица изменений: новые и исправленные уязвимости), а также детальную часть, описывающую каждую обнаруженную находку (где, что, как устранить). Краткая сводка

предназначена для руководящего состава Заказчика, детальная часть — для специалистов служб информационной безопасности.

Развитие интеграционных возможностей — в частности, программный доступ к данным через REST API — отнесено к перспективным направлениям развития продукта и реализуется по согласованию с Заказчиком в рамках отдельной технической проработки.

5 Используемые технологические инструменты

Для функционирования программного обеспечения «iTPROTECT Scout» используются современные технологические решения, обеспечивающие масштабируемость, надёжность и соответствие требованиям информационной безопасности.

Архитектура системы построена на принципах микросервисного взаимодействия с использованием контейнеризации и оркестрации, что обеспечивает гибкость развёртывания, отказоустойчивость и независимое масштабирование компонентов.

5.1 Языки программирования

- **PHP** — серверная бизнес-логика, REST-шлюз и микросервисы прикладного уровня;
- **Go** — высокопроизводительные сервисные компоненты и инструменты киберразведки;
- **JavaScript / TypeScript** — клиентский интерфейс и фронтенд-приложение.

5.2 Программное обеспечение и платформы

- **Kubernetes** — оркестрация контейнеров и автоматическое управление жизненным циклом сервисов;

- **Docker** — контейнеризация приложений и унификация сред развёртывания;
- **PostgreSQL** — основное реляционное хранилище данных системы;
- **Apache Kafka** — брокер сообщений и событийно-ориентированное взаимодействие сервисов;
- **S3-совместимое объектное хранилище** — хранение файлов, отчётов и артефактов сканирования;
- **Temporal** — оркестрация длительных рабочих процессов киберразведки;
- **Centrifugo** — сервер WebSocket для обмена сообщениями в реальном времени;
- **RoadRunner** — высокопроизводительный сервер приложений для PHP-сервисов;
- **Gotenberg** — генерация технических отчётов в формате PDF;
- **Prometheus, Grafana** — системы сбора и визуализации метрик для мониторинга и наблюдаемости;
- **Российские облачные платформы** — размещение компонентов системы и динамическое масштабирование вычислительных ресурсов при ресурсоёмких операциях сканирования.

5.3 Фреймворки и библиотеки

- **Laravel, Spiral Framework** — серверные компоненты, REST-шлюз и микросервисы прикладного уровня;
- **Vue.js** — одностраничное веб-приложение (SPA) для клиентского интерфейса.

5.4 Протоколы и интерфейсы взаимодействия

- **HTTP/HTTPS (REST)** — внешние и внутренние API, защищённый веб-доступ для пользователей;
- **gRPC** — высокопроизводительное синхронное взаимодействие между микросервисами;

- **WebSocket** — двунаправленный обмен данными и обновление информации в реальном времени в пользовательском интерфейсе.

5.5 Инструменты кибербразведки и анализа защищённости

Для решения задач углублённого профилирования внешней поверхности атаки и поиска индикаторов компрометации в системе задействован комплекс специализированных инструментов следующих типов:

- сетевые сканеры портов и идентификации сетевых служб;
- сканеры уязвимостей с поддержкой стандартизированных баз CVE и NVD;
- сканеры безопасности веб-приложений для анализа конфигураций и поиска проблем в HTTP/HTTPS-сервисах;
- инструменты разведки DNS (поиск поддоменов, фильтрация wildcard-записей, запросы WHOIS);
- инструменты обнаружения и определения межсетевых экранов уровня веб-приложений (WAF);
- HTTP-фаззеры для выявления скрытых директорий и файлов;
- инструменты проверки риска перехвата поддоменов (subdomain takeover);
- OSINT-инструменты для мониторинга Dark/Deep Web и поиска цифровых следов организации в открытых и закрытых источниках.

Перечисленные классы инструментов интегрированы в единый процесс сканирования и анализа под управлением сервисов оркестрации кибербразведки iTPROTECT Scout.