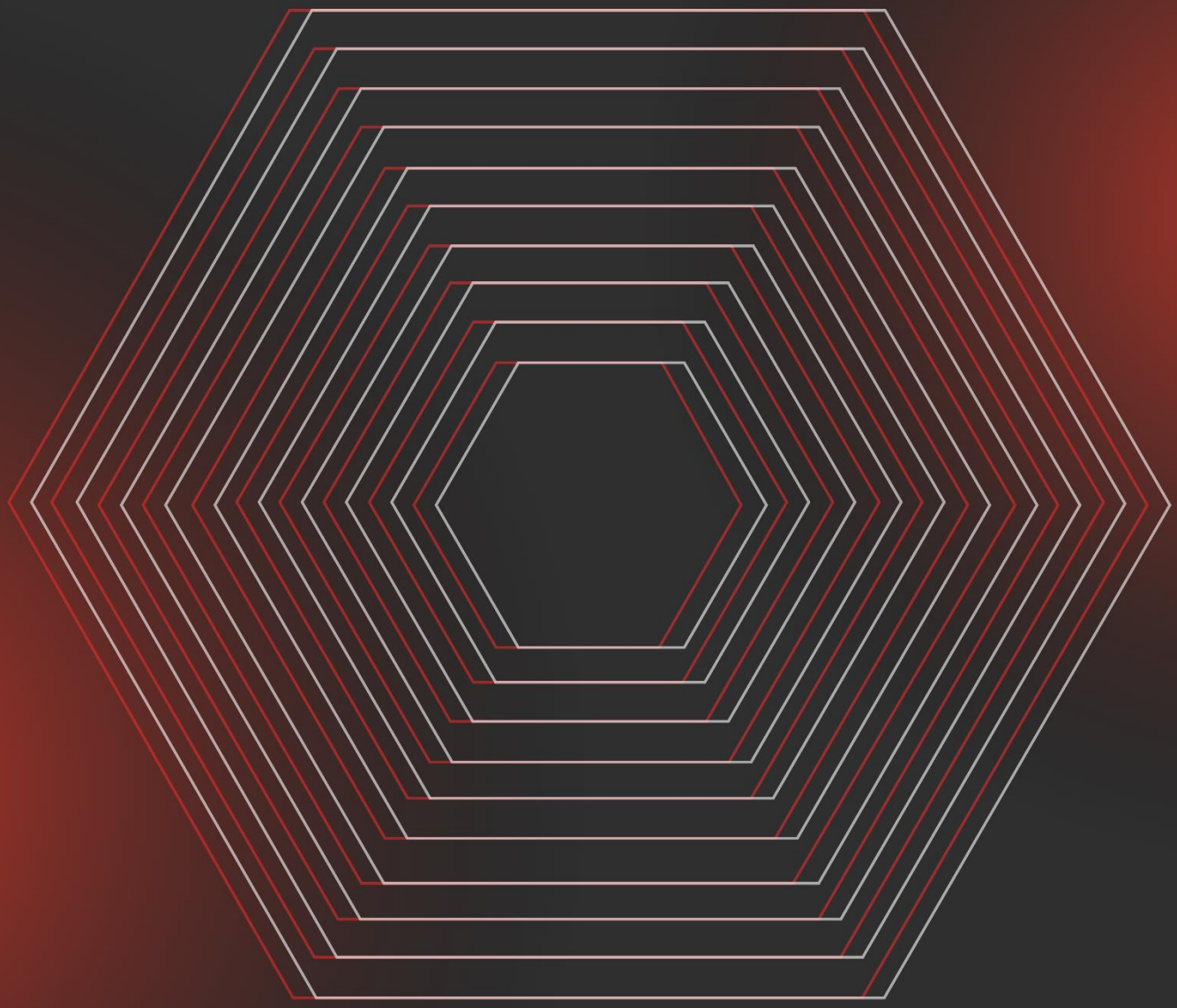
itprotect | scout



Описание процессов, обеспечивающих поддержание жизненного цикла ПО

Для компании: АО «Инфозащита»

Дата: Москва, 2025 год

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

Содержание

1 Общие сведения

1.1 Назначение документа

Настоящий документ содержит описание процессов, обеспечивающих поддержание жизненного цикла программного обеспечения ITProtect Scout (далее — ITProtect Scout, Система), в том числе устранение неисправностей, выявленных в ходе эксплуатации программного обеспечения, совершенствование программного обеспечения, а также информацию о персонале, необходимом для обеспечения такой поддержки.

Документ предназначен для ознакомления заинтересованных сторон с процедурами разработки, сопровождения и технической поддержки Системы.

1.2 Описание программного обеспечения

ITProtect Scout представляет собой специализированную систему киберразведки, предназначенную для углублённой разведки киберугроз и оперативного анализа индикаторов компрометации в корпоративной инфраструктуре организаций.

Система функционирует в режиме SaaS (Software as a Service) и обеспечивает:

- глубокое профилирование внешней поверхности атаки с выявлением векторов проникновения;
- детальное профилирование сетевых служб с определением версий программного обеспечения и конфигураций;
- корреляцию обнаруженных уязвимостей с известными эксплойтами и техниками атак;

- оперативное обнаружение модификаций в инфраструктуре для выявления подозрительной активности;
- формирование технических отчётов для служб безопасности с детализированными данными.

Правообладателем программного обеспечения ITProtect Scout является Акционерное общество «Инфозащита» (далее — Правообладатель).

1.3 Область применения

ITProtect Scout ориентирован на профессиональное использование:

- службами информационной безопасности организаций (специалисты SOC, аналитики ИБ, администраторы безопасности);
- внешними аудиторами и консультантами по кибербезопасности;
- центрами мониторинга информационной безопасности;
- поставщиками управляемых услуг безопасности (MSSP).

Система применяется для решения задач оперативного анализа защищённости внешнего периметра, выявления критических уязвимостей и векторов атак, мониторинга изменений в инфраструктуре и поддержки принятия решений по обеспечению информационной безопасности.

2 Модель жизненного цикла системы

Жизненный цикл ITProtect Scout представляет собой непрерывную модель развития, характерную для программного обеспечения, функционирующего в режиме SaaS. Система находится в стадии промышленной эксплуатации с постоянным циклом обновлений и улучшений.

2.1 Стадии жизненного цикла

Для ITProtect Scout как облачного сервиса характерна итеративная модель, в которой циклически повторяются следующие стадии:

- Планирование итерации — определение целей и содержания очередного обновления системы на основе анализа обратной связи пользователей, новых требований рынка, изменений в ландшафте киберугроз и обнаруженных недостатков. Длительность стадии составляет от одной до двух недель в зависимости от масштаба планируемых изменений.
- Разработка обновления — реализация запланированной функциональности, исправление обнаруженных дефектов, оптимизация алгоритмов обнаружения угроз. Стадия выполняется в соответствии с принципами agile-разработки с ежедневным контролем прогресса и оперативной корректировкой задач.
- Тестирование и валидация — комплексная проверка реализованных изменений, включающая функциональное тестирование, проверку совместимости, валидацию точности обнаружения угроз и оценку влияния на производительность системы. Автоматизированные тесты дополняются экспертной оценкой критических изменений.
- Развёртывание в продуктивной среде — поэтапный выпуск обновления в облачной инфраструктуре с контролем ключевых метрик и возможностью оперативного отката. Критические обновления безопасности могут развёртываться в ускоренном режиме.

Мониторинг и стабилизация — контроль работы обновлённой версии в продуктивной среде, сбор телеметрии, анализ обратной связи от пользователей и при необходимости выпуск корректирующих обновлений.

Данные стадии повторяются с периодичностью от двух до четырёх недель, обеспечивая регулярное обновление функциональности системы и оперативное реагирование на новые киберугрозы.

2.2 Особенности модели жизненного цикла

Модель жизненного цикла ITProtect Scout имеет ряд характерных особенностей, обусловленных спецификой функционирования системы как облачного сервиса киберразведки:

- Непрерывность и цикличность — в отличие от традиционного программного обеспечения с линейной последовательностью стадий от разработки до вывода из эксплуатации, ITProtect Scout находится в состоянии постоянной эволюции. Стадии жизненного цикла повторяются итеративно, обеспечивая регулярное обновление функциональности каждые 2—4 недели. При этом система никогда не выводится из эксплуатации полностью — обновления развёртываются без прерывания сервиса для пользователей.
- Приоритизация на основе критичности угроз — планирование каждой итерации определяется не только бизнес-требованиями, но и актуальным ландшафтом киберугроз. При обнаружении новых критических уязвимостей или активных кампаний злоумышленников стандартный цикл разработки может быть прерван для экстренного выпуска обновлений. Это обеспечивает способность системы оперативно реагировать на изменения в области информационной безопасности.
- Автоматизация процессов развёртывания — облачная архитектура позволяет полностью автоматизировать процесс развёртывания обновлений. Новые версии системы проходят через конвейер непрерывной интеграции и доставки (CI/CD), включающий

автоматическое тестирование, поэтапное развёртывание и мониторинг ключевых метрик. Это минимизирует риски при обновлениях и позволяет быстро откатить изменения при обнаружении проблем.

- Обратная связь как драйвер развития — телеметрия системы и обратная связь от пользователей непрерывно анализируются и напрямую влияют на приоритеты развития. Данные о ложных срабатываниях, пропущенных угрозах, производительности сканирования собираются автоматически и используются для улучшения алгоритмов обнаружения. Запросы службы технической поддержки систематизируются и преобразуются в требования для будущих итераций.
- Синхронизация с экосистемой безопасности — жизненный цикл системы синхронизирован с внешними процессами в области кибербезопасности: публикацией CVE-уязвимостей, выпуском обновлений безопасности вендорами, появлением новых исследований в области киберугроз. Система должна оперативно интегрировать эту информацию, что требует гибкости в планировании и способности быстро адаптировать приоритеты разработки.

Такая организация жизненного цикла обеспечивает баланс между стабильностью сервиса и способностью оперативно реагировать на изменения, что критически важно для системы киберразведки, функционирующей в динамично меняющейся среде угроз.

3 Процессы поддержания жизненного цикла

3.1 Совершенствование ПО

Процесс совершенствования программного обеспечения ITProtect Scout обеспечивает непрерывное развитие функциональности системы в соответствии с эволюцией киберугроз и требованиями пользователей. Данный процесс является ключевым для поддержания конкурентоспособности системы и её эффективности в обнаружении актуальных угроз информационной безопасности.

3.1.1 Планирование развития функциональности

Планирование совершенствования системы представляет собой структурированный процесс, основанный на анализе множественных источников информации и требований.

Основным источником требований является обратная связь от пользователей, поступающая через различные каналы. Служба технической поддержки систематизирует запросы клиентов, выявляя наиболее востребованные функции и типовые сценарии использования, которые требуют улучшения. Анализ обращений позволяет идентифицировать проблемные области в текущей функциональности, такие как недостаточная детализация отчётов, необходимость расширения типов сканируемых активов или потребность в дополнительных фильтрах и группировках данных. Каждое обращение категоризируется по типу (запрос новой функции, улучшение существующей, проблема производительности) и оценивается по критериям частоты возникновения и влияния на работу пользователей.

Вторым критически важным источником является мониторинг ландшафта киберугроз. Команда разработки отслеживает публикации исследователей безопасности, анализирует отчёты об инцидентах, изучает новые техники и тактики злоумышленников, описанные в матрице MITRE ATT&CK. Особое внимание уделяется появлению новых классов уязвимостей, изменениям в методах эксплуатации известных проблем, возникновению новых векторов атак на облачную инфраструктуру и контейнерные среды. Эта информация трансформируется в технические требования к расширению возможностей сканирования и улучшению алгоритмов обнаружения.

Третьим источником являются изменения в нормативно-правовой базе и индустриальных стандартах. Регулярно анализируются обновления требований регуляторов, изменения в стандартах ISO 27001, PCI DSS, требованиях ФСТЭК России. Выявленные изменения преобразуются в функциональные требования к системе, обеспечивающие соответствие актуальным нормам.

Формирование плана развития происходит в рамках квартального планирования с возможностью оперативной корректировки. Все собранные требования проходят через процесс приоритизации, учитывающий критичность для безопасности (устранение возможности пропуска критических уязвимостей), охват пользовательской базы (количество клиентов, которым необходима функция), техническую сложность реализации и совместимость с текущей архитектурой системы. Результатом является дорожная карта развития продукта, разбитая на двухнедельные спринты с чётко определёнными целями и измеримыми результатами.

3.1.2 Категории обновлений системы

Система обновлений ITProtect Scout организована по трём основным категориям, каждая из которых имеет свой цикл выпуска и процедуры развёртывания:

- Плановые функциональные обновления выпускаются с периодичностью 2—4 недели и представляют собой основной механизм эволюции системы. Эти обновления включают реализацию новых модулей анализа (например, добавление проверок безопасности Kubernetes-кластеров или анализа конфигураций облачных сервисов), расширение поддержки протоколов и сервисов (добавление распознавания новых версий веб-серверов, баз данных, сервисов очередей), улучшения пользовательского интерфейса (новые виды визуализации данных, расширенные возможности фильтрации и поиска), оптимизацию производительности сканирования. Каждое такое обновление проходит полный цикл тестирования, включающий функциональные тесты, тесты производительности и регрессионное тестирование.
- Обновления баз данных угроз представляют собой наиболее частый тип обновлений, происходящий ежедневно, а для критических угроз — несколько раз в день. Эти обновления включают добавление новых записей CVE с детальным описанием уязвимостей и методов их эксплуатации, обновление CVSS-оценок на основе актуальной информации от NIST, добавление новых сигнатур для обнаружения уязвимых версий программного обеспечения, интеграцию индикаторов компрометации из threat intelligence feeds, обновление правил корреляции для выявления сложных векторов атак. Процесс обновления баз полностью автоматизирован и включает валидацию данных на непротиворечивость и полноту перед развёртыванием.

- Критические обновления безопасности представляют собой экстренные релизы, выпускаемые вне планового расписания при обнаружении активно эксплуатируемых zero-day уязвимостей или новых кампаний массовых атак. Такие обновления разрабатываются и тестируются в ускоренном режиме, при этом приоритет отдаётся скорости реакции над полнотой функциональности. После развёртывания критического обновления в последующие плановые релизы включаются дополнительные улучшения и оптимизации.

3.1.3 Процедура развёртывания обновлений

Развёртывание обновлений в облачной инфраструктуре ITProtect Scout реализовано через структурированный процесс, обеспечивающий стабильность работы системы и минимизацию рисков для пользователей.

Процесс начинается с подготовки новой версии системы, которая проходит обязательный цикл внутреннего тестирования. На этом этапе проверяется корректность работы всех модулей системы, валидируется правильность обнаружения известных уязвимостей на эталонных наборах данных, оценивается влияние изменений на производительность сканирования. Особое внимание уделяется проверке совместимости новой версии с существующими данными пользователей, чтобы исключить потерю или искажение накопленной информации о результатах предыдущих сканирований.

Развёртывание в производственной среде выполняется поэтапно для минимизации потенциального влияния на пользователей. Сначала обновление применяется к предпродуктивному экземпляру системы, где проводится финальная проверка работоспособности в условиях, максимально приближенных к реальным. После подтверждения корректности функционирования начинается процесс обновления

основной системы, который планируется на период минимальной активности пользователей для сокращения возможных неудобств.

Архитектура системы позволяет выполнять обновления без полной остановки сервиса. Пользователи могут продолжать работу с системой, при этом новая функциональность становится доступна после завершения процесса развёртывания. В случае обнаружения критических проблем предусмотрена возможность оперативного восстановления предыдущей версии из резервной копии, что обеспечивает непрерывность предоставления услуги.

После каждого обновления проводится мониторинг ключевых показателей работы системы в течение первых 24 часов. Отслеживаются такие параметры как стабильность работы модулей сканирования, корректность формирования отчётов, время выполнения типовых операций. При выявлении отклонений от нормальных показателей инициируется процедура анализа и при необходимости выпускается корректирующее обновление.

Для критических обновлений безопасности, связанных с необходимостью оперативного добавления обнаружения новых угроз, применяется ускоренная процедура развёртывания. В таких случаях обновление может быть развёрнуто в течение нескольких часов после обнаружения угрозы, при этом тестирование фокусируется на проверке корректности новых правил обнаружения без полного регрессионного тестирования всей системы.

3.1.4 Развитие возможностей обнаружения угроз

Совершенствование механизмов обнаружения угроз является приоритетным направлением развития системы и реализуется через несколько взаимосвязанных процессов.

Расширение покрытия сканирования происходит через добавление поддержки новых технологий и сервисов, наиболее востребованных пользователями системы. Приоритет отдаётся технологиям с широким распространением в корпоративных средах и высоким уровнем риска с точки зрения информационной безопасности. При добавлении поддержки новых сервисов обеспечивается их корректная идентификация, определение версий и интеграция соответствующей информации об известных уязвимостях.

Повышение точности обнаружения достигается через постоянный анализ результатов работы системы и обратной связи от пользователей. Все зарегистрированные случаи ложных срабатываний анализируются для выявления системных проблем и корректировки алгоритмов обнаружения. Подтверждённые пользователями находки используются для валидации и улучшения механизмов оценки критичности обнаруженных проблем. Регулярно проводится актуализация баз данных уязвимостей и сигнатур обнаружения на основе информации из открытых источников и специализированных баз данных.

Оптимизация производительности сканирования направлена на обеспечение приемлемого времени получения результатов при сохранении полноты и качества анализа. Применяются методы оптимизации последовательности проверок, рационального использования сетевых ресурсов и минимизации воздействия на сканируемую инфраструктуру. Для часто сканируемых активов реализованы механизмы инкрементального анализа, позволяющие фокусироваться на изменениях с момента последнего сканирования.

Эффективность процесса совершенствования оценивается через анализ ключевых показателей работы системы. Отслеживается оперативность добавления новых уязвимостей в базу данных системы после их публичного

раскрытия, полнота покрытия известных уязвимостей для поддерживаемых типов инфраструктур, время выполнения типовых сценариев сканирования, соотношение подтверждённых и ложных срабатываний. Данные показатели регулярно анализируются для выявления областей, требующих улучшения, и корректировки приоритетов развития системы.

Результаты процесса совершенствования отражаются в регулярных обновлениях системы, расширении перечня обнаруживаемых угроз и повышении качества предоставляемой информации о состоянии безопасности инфраструктуры пользователей.

3.2 Устранение неисправностей

Процесс устранения неисправностей в системе ITProtect Scout обеспечивает оперативное выявление и исправление ошибок, возникающих в ходе эксплуатации системы. Данный процесс критически важен для поддержания высокого уровня доступности сервиса и доверия пользователей к результатам работы системы киберразведки.

3.2.1 Выявление и регистрация неисправностей

Выявление неисправностей в системе происходит через несколько взаимодополняющих каналов, обеспечивающих максимально быстрое обнаружение проблем различного характера.

Основным источником информации о неисправностях являются обращения пользователей через службу технической поддержки. Пользователи сообщают о различных типах проблем: некорректном отображении данных в интерфейсе, ошибках при выполнении сканирования, несоответствии результатов ожиданиям, проблемах с производительностью системы. Каждое обращение регистрируется в системе учёта с фиксацией подробного описания проблемы, условий её возникновения, данных об

окружении пользователя и, при возможности, скриншотов или другой диагностической информации.

Система автоматического мониторинга представляет второй важный канал обнаружения проблем. Мониторинг охватывает ключевые компоненты системы и отслеживает такие параметры как доступность сервиса, время отклика на запросы пользователей, успешность выполнения задач сканирования, уровень использования системных ресурсов, наличие ошибок в журналах работы системы. При превышении пороговых значений или обнаружении аномалий система мониторинга автоматически создаёт инцидент и оповещает ответственных специалистов.

Внутреннее тестирование и контроль качества обеспечивают проактивное выявление проблем до их обнаружения пользователями. Регулярные проверки включают выполнение тестовых сканирований эталонной инфраструктуры, анализ консистентности данных в базе, проверку корректности работы алгоритмов обнаружения на известных наборах уязвимостей. Выявленные в ходе внутренних проверок несоответствия документируются и включаются в план исправлений.

3.2.2 Классификация и приоритизация неисправностей

Все выявленные неисправности проходят процедуру классификации для определения приоритета и срочности их устранения. Классификация основывается на нескольких критериях, позволяющих объективно оценить влияние проблемы на работу системы и пользователей.

По степени критичности неисправности разделяются на четыре категории:

- Критические неисправности приводят к полной неработоспособности системы или её ключевых функций, влияют на всех или большинство

пользователей, могут привести к потере данных или предоставлению некорректной информации о критических уязвимостях.

- Высокий приоритет присваивается проблемам, существенно затрудняющим работу с системой, влияющим на точность обнаружения угроз или приводящим к значительной деградации производительности.
- Средний приоритет получают неисправности, влияющие на отдельные функции системы без критического воздействия на основной функционал.
- Низкий приоритет назначается косметическим дефектам интерфейса и незначительным неудобствам, не влияющим на результаты работы системы.

Дополнительными факторами при определении приоритета являются количество затронутых пользователей, частота возникновения проблемы, наличие обходных путей решения, потенциальные репутационные риски при длительном сохранении проблемы. На основе комплексной оценки формируется очередь задач по устранению неисправностей с чёткими сроками исполнения для каждой категории.

3.2.3 Процедура устранения неисправностей

Процесс устранения неисправностей следует структурированной процедуре, обеспечивающей систематический подход к решению проблем и минимизацию риска внесения новых ошибок.

Анализ и диагностика проблемы начинается с воспроизведения ошибки в контролируемой среде. Специалисты технической поддержки совместно с командой разработки анализируют условия возникновения проблемы, изучают журналы работы системы, при необходимости запрашивают дополнительную информацию у пользователей. Для сложных или трудновоспроизводимых проблем может применяться расширенная

диагностика с использованием специальных инструментов отладки и профилирования.

Разработка исправления выполняется после точной локализации причины проблемы. В зависимости от характера неисправности исправление может включать корректировку программного кода, обновление конфигурации системы, исправление данных в базе или комбинацию этих действий. Для критических проблем разработка исправления ведётся в приоритетном режиме с привлечением наиболее квалифицированных специалистов.

Тестирование исправления проводится в несколько этапов. Сначала проверяется устранение исходной проблемы в условиях, максимально приближенных к тем, в которых она была обнаружена. Затем выполняется регрессионное тестирование для подтверждения отсутствия негативного влияния на другие функции системы. Для критических исправлений дополнительно проводится нагрузочное тестирование для оценки влияния на производительность.

3.2.4 Развёртывание исправлений и контроль результатов

Развёртывание исправлений в производственной среде выполняется в соответствии с их приоритетом и характером устраняемой проблемы:

- Критические исправления, устраняющие проблемы, влияющие на работоспособность системы или корректность обнаружения угроз, развёртываются в экстренном порядке. После минимального необходимого тестирования исправление применяется к производственной системе, при этом обеспечивается постоянный контроль со стороны технических специалистов. Пользователи,

затронутые проблемой, оперативно информируются об устранении неисправности.

- Плановые исправления некритических проблем группируются и включаются в очередное плановое обновление системы. Это позволяет минимизировать количество вмешательств в работу производственной системы и обеспечить комплексное тестирование всех изменений. В release notes обновления включается информация обо всех устранённых проблемах для информирования пользователей.

После развёртывания каждого исправления проводится мониторинг его эффективности. Отслеживается отсутствие повторных обращений по той же проблеме, контролируется стабильность работы системы, анализируется обратная связь от пользователей. При выявлении недостаточной эффективности исправления или возникновении побочных эффектов инициируется повторный цикл анализа и доработки.

3.2.5 Предотвращение повторного возникновения проблем

Важной составляющей процесса устранения неисправностей является анализ коренных причин и принятие мер по предотвращению аналогичных проблем в будущем.

После устранения каждой критической или часто встречающейся проблемы проводится ретроспективный анализ. Команда анализирует, почему проблема не была выявлена на этапе разработки или тестирования, какие процессы или инструменты могли бы предотвратить её появление, какие уроки можно извлечь из данного инцидента. На основе анализа формируются рекомендации по улучшению процессов разработки,

расширению тестового покрытия, усилению мониторинга критических компонентов.

Накопленный опыт устранения неисправностей систематизируется в виде базы знаний, доступной всем членам команды. База содержит описание типовых проблем, методы их диагностики и решения, что позволяет ускорить устранение похожих проблем в будущем и обеспечить преемственность знаний при изменении состава команды.

3.3 Техническая поддержка

Процесс технической поддержки пользователей ITProtect Scout обеспечивает оперативное решение возникающих вопросов и проблем при работе с системой, консультационную помощь по использованию функциональности и поддержание высокого уровня удовлетворённости пользователей сервисом киберразведки.

3.3.1 Организация службы технической поддержки

Служба технической поддержки ITProtect Scout организована по трехуровневой модели, обеспечивающей эффективное распределение запросов в соответствии с их сложностью и требуемой квалификацией специалистов.

Первая линия поддержки осуществляет прием и первичную обработку всех входящих обращений. Специалисты первой линии регистрируют запросы в системе учета, проводят первичную диагностику проблемы, предоставляют ответы на типовые вопросы по функциональности системы и помогают пользователям в решении стандартных задач. При необходимости более глубокой экспертизы запрос эскалируется на вторую линию поддержки.

Вторая линия поддержки состоит из специалистов с углубленными знаниями системы и экспертизой в области кибербезопасности. Они занимаются детальным анализом нестандартных ситуаций, расследованием инцидентов, связанных с некорректной работой системы, консультированием по сложным сценариям использования и интерпретации результатов сканирования. Специалисты второй линии также оказывают экспертную поддержку по вопросам анализа обнаруженных угроз и приоритизации их устранения.

Третья линия поддержки представлена командой разработки, которая привлекается при выявлении дефектов в программном обеспечении, требующих внесения изменений в код или архитектуру системы. Разработчики проводят глубокий анализ технических проблем, разрабатывают и тестируют исправления, а также консультируют по вопросам технических ограничений и возможностей системы.

3.3.2 Каналы обращения в службу поддержки

Для обеспечения удобства пользователей и оперативности реагирования на запросы служба технической поддержки предоставляет несколько каналов коммуникации.

Основным каналом обращения является веб-портал технической поддержки, интегрированный с системой ITProtect Scout. Через портал пользователи могут создавать заявки с детальным описанием проблемы, прикреплять скриншоты и диагностическую информацию, отслеживать статус обработки своих обращений, просматривать историю решённых вопросов. Портал обеспечивает структурированный сбор информации, что ускоряет диагностику и решение проблем.

Электронная почта используется для асинхронной коммуникации по некритичным вопросам и для получения развёрнутых консультаций. Все

письма, направленные на адрес службы поддержки, автоматически регистрируются в системе учёта заявок с присвоением уникального номера для отслеживания. Ответы на обращения по электронной почте предоставляются в течение установленного соглашением об уровне сервиса времени.

Телефонная линия поддержки доступна для срочных обращений и ситуаций, требующих оперативного взаимодействия. Телефонная поддержка предоставляется в рабочее время, при этом все обращения фиксируются в системе учёта для обеспечения полноты истории взаимодействия с клиентом. Для критических инцидентов, влияющих на работоспособность системы у ключевых клиентов, может быть организована расширенная доступность телефонной поддержки.

3.3.3 Регламент обработки обращений

Обработка обращений в службу технической поддержки осуществляется в соответствии с установленным регламентом, обеспечивающим предсказуемость и качество обслуживания.

Каждое поступившее обращение проходит процедуру категоризации по типу запроса, уровню критичности и требуемой экспертизе. Запросы разделяются на несколько категорий: инциденты, связанные с неработоспособностью или некорректной работой системы; запросы на консультацию по использованию функциональности; запросы на изменение конфигурации или настроек; предложения по улучшению системы. Для каждой категории определены целевые показатели времени реакции и решения.

Приоритизация обращений основывается на оценке влияния проблемы на бизнес-процессы пользователя. Наивысший приоритет получают инциденты, приводящие к полной неработоспособности системы или

невозможности получения критически важной информации о безопасности. Высокий приоритет назначается проблемам, существенно затрудняющим работу с системой или влияющим на достоверность результатов. Средний и низкий приоритеты присваиваются запросам на консультации и некритичным улучшениям соответственно.

Эскалация запросов происходит автоматически при приближении к установленным временным лимитам обработки или по инициативе специалиста при выявлении сложности, превышающей его компетенцию. Процедура эскалации обеспечивает своевременное привлечение необходимых ресурсов и экспертизы для решения сложных вопросов.

3.3.4 Соглашение об уровне сервиса

Уровень сервиса технической поддержки определяется индивидуально для каждого клиента на основе выбранного тарифного плана и масштаба использования системы. Соглашение об уровне сервиса (SLA) устанавливает измеримые показатели качества обслуживания и взаимные обязательства сторон.

Базовые параметры SLA включают время первичной реакции на обращение, максимальное время решения для различных категорий запросов, доступность каналов поддержки, процент решения запросов с первого обращения. Конкретные значения этих параметров определяются в зависимости от критичности системы для бизнес-процессов клиента, объёма обрабатываемой инфраструктуры и частоты использования сервиса.

Для организаций с повышенными требованиями к оперативности поддержки предусматриваются расширенные условия обслуживания. Они могут включать приоритетную обработку запросов, выделенного менеджера по работе с клиентом, расширенные часы поддержки,

проактивный мониторинг использования системы и регулярные консультации по оптимизации работы с сервисом.

Контроль соблюдения SLA осуществляется на постоянной основе с формированием регулярной отчётности для клиентов. В отчётах отражаются фактические показатели времени реакции и решения, статистика по типам обращений, информация о выполненных улучшениях системы на основе обратной связи. При выявлении отклонений от установленных показателей принимаются корректирующие меры для восстановления требуемого уровня сервиса.

3.3.5 Пользовательская документация и самообслуживание

Для повышения эффективности поддержки и обеспечения возможности самостоятельного решения типовых вопросов пользователями поддерживается полная пользовательская документация и ресурсы для самообслуживания.

Пользовательская база знаний, в отличие от внутренней технической базы знаний команды разработки, ориентирована на конечных пользователей системы и содержит материалы, адаптированные для специалистов по информационной безопасности без глубоких технических знаний о внутренней архитектуре системы. База включает подробные руководства по всем функциям системы, пошаговые инструкции по выполнению типовых операций, ответы на часто задаваемые вопросы, рекомендации по интерпретации результатов сканирования и лучшие практики использования системы для различных сценариев киберразведки.

Материалы пользовательской документации регулярно обновляются на основе анализа поступающих в поддержку вопросов и при выпуске новых

версий системы. Поисковая система позволяет быстро находить необходимую информацию по ключевым словам или навигировать по тематическим разделам. Для сложных тем предусмотрены видеоинструкции и вебинары, демонстрирующие практическое использование функциональности системы. Эффективность пользовательской документации оценивается через метрики использования и сокращение количества обращений по вопросам, покрытым документацией.

4 Информация о персонале

4.1 Структура команды и компетенции

Поддержание жизненного цикла ITProtect Scout обеспечивается квалифицированной командой специалистов правообладателя, обладающей всеми необходимыми компетенциями для полного цикла разработки, эксплуатации и поддержки системы.

4.1.1 Состав команды по направлениям:

Управление продуктом и проектами — 2 специалиста

- Стратегическое планирование развития продукта;
- Управление требованиями и приоритизация задач;
- Координация работы команд разработки;
- Взаимодействие с клиентами и партнёрами.

Разработка программного обеспечения — 8 специалистов

- Разработка серверной части системы;

- Разработка веб-интерфейса;
- Проектирование архитектуры решения;
- Интеграция с внешними системами и источниками данных.

Экспертиза в области кибербезопасности — 3 специалиста

- Анализ современных киберугроз и векторов атак;
- Разработка и валидация правил обнаружения;
- Адаптация данных об уязвимостях (CVE/NVD);
- Консультирование по вопросам интерпретации результатов.

Системный анализ — 2 специалиста

- Анализ и формализация требований;
- Проектирование функциональности системы;
- Подготовка технической документации.

Контроль качества и тестирование — 3 специалиста

- Функциональное тестирование;
- Автоматизация тестирования;
- Валидация корректности обнаружения угроз;
- Нагрузочное тестирование.

DevOps и эксплуатация инфраструктуры — 2 специалиста

- Администрирование облачной инфраструктуры;
- Автоматизация процессов развёртывания (CI/CD);
- Мониторинг доступности и производительности;
- Резервное копирование и восстановление.

Техническая поддержка — 5 специалистов

- Сервис-менеджер (1 специалист) — координация работы службы поддержки;
- Первая линия поддержки (2 специалиста) — приём и первичная обработка обращений;
- Вторая линия поддержки (2 специалиста) — решение сложных технических вопросов;
- Третья линия поддержки — привлечение специалистов из профильных технических направлений (разработка ПО, DevOps, системный анализ) для устранения дефектов, требующих изменения кода или архитектуры системы.

Все специалисты являются штатными сотрудниками правообладателя и обладают необходимой квалификацией в соответствии с занимаемыми позициями. Команда имеет опыт разработки и эксплуатации облачных систем в области информационной безопасности, что обеспечивает эффективное поддержание всех процессов жизненного цикла продукта.

4.2 Контактная информация службы поддержки

4.2.1 Основные каналы связи

Служба технической поддержки ITProtect Scout доступна через следующие каналы коммуникации:

- Электронная почта службы поддержки support@itprotect.ru используется для асинхронной коммуникации и отправки диагностической информации большого объёма. Все сообщения, направленные на данный адрес, автоматически регистрируются в системе учёта заявок.

- Телефонная линия поддержки +7(495)120-64-46 доступна для срочных обращений и консультаций, требующих интерактивного взаимодействия. Время работы телефонной линии соответствует установленному для конкретного клиента соглашению об уровне сервиса.

4.2.2 Режим работы службы поддержки

Базовый режим работы службы технической поддержки охватывает рабочие дни с 9:00 до 18:00 по московскому времени. В указанное время доступны все каналы коммуникации и обеспечивается полный цикл обработки обращений.

Для клиентов с расширенными соглашениями об уровне сервиса могут быть установлены индивидуальные условия доступности поддержки, включая расширенные часы работы, поддержку в выходные и праздничные дни, выделенную линию для критических инцидентов.

4.2.3 Контактная информация правообладателя

Акционерное общество «Инфозащита» Юридический адрес: 129110, г. Москва, вн. тер. г., муниципальный округ Мещанский, ул. Большая Переяславская, д. 46, стр. 2, этаж 4, помещ. I, ком. 8; Почтовый адрес: 115114, г. Москва, Дербеневская набережная, д. 11, этаж 15, офис В1503; Телефон: +7 (495) 120-64-46; Электронная почта: info@itprotect.ru; Веб-сайт: https://itprotect.ru/

Для вопросов, связанных с лицензированием, коммерческими условиями и партнёрством, следует обращаться в коммерческий отдел по адресу hr@itprotect.ru или телефону +7 (495) 120-64-46 (доб. 2101).