Описание процессов
«CrossTech Database Security»

Версия 0.2.0 © ООО «Кросстех Солюшнс Групп», 2025.06

СОДЕРЖАНИЕ

1. Общая информация 4
1.1. Информация о Системе 4
1.2. Описание Системы 5
2. Жизненный цикл системы 6
2.1. Общая информация 6
2.2. Поддержка версий и доработка 7
2.3. Процессы, обеспечивающие поддержание ЖЦ 8
2.4. Технические процессы 9
2.4.1. Разработка и совершенствование 9
2.4.2. Внедрение 10
2.4.3. Документирование 11
2.4.4. Управление развертыванием 11
2.5. Поддержка и сопровождение 12
2.5.1. Обеспечение гарантии качества 12
2.5.2. Тестирование 13
2.5.3. Аудит 13
2.5.4. Устранение неисправностей, выявленных в ходе эксплуатации 14
2.5.5. Устранение сбойных ситуаций 14
2.5.6. Эксплуатация 15
2.5.7. Приобретение и поставка 15
2.6. Информация о персонале 17
2.6.1. Обучение и квалификация персонала 17
2.6.2. Информация о необходимом персонале для обеспечения поддержки 17
2.6.3. Размещение персонала Вендора 18

АННОТАЦИЯ

В данном документе содержится описание процессов, обеспечивающих поддержание жизненного цикла программного обеспечения «CrossTech Database Security» (далее – Система), в том числе описание устранения неисправностей, выявленных в ходе эксплуатации, совершенствования программного обеспечения (далее – ПО), а также информация о персонале, необходимом для обеспечения такой поддержки.

Настоящий документ носит описательный характер.

1. ОБЩАЯ ИНФОРМАЦИЯ

1.1. Информация о Системе

«CrossTech Database Security» – система для отслеживания и анализа активности в базах данных (далее – БД), обеспечения защиты БД от несанкционированного доступа, атак и утечек данных.

Система способна обнаруживать необычные или потенциально вредоносные действия, такие как: несанкционированный доступ, изменение данных или попытки вторжения.

Система в режиме реального времени обеспечивает контроль доступа, мониторинг активности пользователей и другие меры для обеспечения безопасности данных в БД. Агенты позволяют осуществлять мониторинг обращений к БД.

Система способствует защите конфиденциальной информации, хранимой в таблицах БД, протоколирует действия пользователей в БД, а также действия пользователей в соответствии с заданными параметрами (политиками) и информирует о выполнении подозрительных операций.

Интерфейс Системы основан на высокоуровневой Java-платформе JMIX (ранее известной как CUBA Platform) с открытым исходным кодом, используемой для создания корпоративных информационных систем. В составе платформы используется компонентный фреймворк пользовательского интерфейса Vaadin.

1.2. Описание Системы

Система обеспечивает выполнение следующих функций:

- выявление подозрительных запросов пользователей БД в реальном времени;
- выявление и предотвращение нарушений политик безопасности или превышения прав пользователей;
- управление правами доступа пользователей.

Особенности и возможности Системы:

- современный быстрый web-интерфейс;
- возможность авторизации под доменными учетными данными;
- интеграционные API;
- возможность отправки уведомлений о любых событиях.

Система поддерживает серверные Linux-подобные операционные системы из реестра российского ПО с возможностью установки OpenJDK 17.

Система поддерживает популярные браузеры, такие как «Google Chrome».

2. ЖИЗНЕННЫЙ ЦИКЛ СИСТЕМЫ

2.1. Общая информация

Жизненный цикл (далее – ЖЦ) Системы – это процесс ее развития, начинающийся со стадии замысла и заканчивающийся прекращением применения.

Внедрение Системы имеет ряд преимуществ:

- предотвращение несанкционированного доступа к данным;
- ограничение распространения конфиденциальных материалов;
- классификация запросов к БД по различным критериям (пользователям, временным интервалам, типу запроса и т.д.);
- анализ операций с БД (позволяет отслеживать аномалии и подозрительные действия в запросах пользователей);
- создание отчетов по выбранному трафику (полезны для оптимизации производительности и оценки уровня нагрузки на инфраструктуру);
- оперативное реагирование на инциденты (за счет быстрого обнаружения отклонений в трафике и своевременного уведомления специалистов ускоряется выявление проблем и сбоев, связанных с трафиком);
- сокращение административных расходов (автоматизация процессов сбора, анализа и предоставления отчетов по трафику снижает нагрузку на администратора и инженеров, высвобождая их время для выполнения более значимых задач).

Внедрение Системы может значительно улучшить безопасность, производительность и эффективность организации, а также помочь в соблюдении регуляторных требований.

2.2. Поддержка версий и доработка

Система является развивающейся, поэтому ее ЖЦ носит циклический характер, т.е. является последовательностью ЖЦ отдельных версий Системы – ее релизов.

Версия Системы – цифровое или цифробуквенное обозначение конкретного образа Системы, получаемого в процессе ее разработки. В рамках настоящего документа существенными в версии Системы считаются два первых числа.

Версии Системы имеют следующий общий вид:

<Мажорная версия>.<Минорная версия>.<Хотфикс>
Например: 0.2.0

1. Мажорная версия
   Основной номер версии или поколение Системы. Одно поколение от другого может существенно отличаться по функциональным и нефункциональным возможностям.
2. Минорная версия
   Вспомогательный номер версии Системы. Используется для различения версий Системы внутри одного поколения при несущественном изменении функциональности или исправление несущественных недостатков.
3. Хотфикс
   Вспомогательный номер версии Системы. Используется для различения версий Системы внутри одного поколения при исправлении выявленных дефектов (hotfix).

К каждому новому релизу в рамках доработки привязывается список историй (story) и исправленных дефектов в аналитической системе Jira. При выпуске релиза к новой версии прикладывается документ «Release Notes», в котором описан состав релиза с указанной версией Системы.

2.3. Процессы, обеспечивающие поддержание ЖЦ

ЖЦ Системы рассматривается с точки зрения ГОСТ Р ИСО/МЭК 12207-2010 «Процессы ЖЦ программных средств (Information technology. System and software engineering. Software lifecycle processes)». Процессы ЖЦ реализуются под управлением сторон, вовлеченных в ЖЦ. Под стороной понимают одну из тех организаций, которые инициируют или выполняют разработку, эксплуатацию или сопровождение Системы.

Основными сторонами являются:

- Заказчик (конечный пользователь, эксплуатирующий Систему);
- Вендор (разработчик, обеспечивающий разработку, внедрение, модернизацию и сопровождение Системы).

2.4. Технические процессы

2.4.1. Разработка и совершенствование

Процесс разработки и совершенствования – технический процесс, посредством которого потребности пользователей преобразуются в программный продукт.

Для Системы определена долгосрочная стратегия развития (roadmap), в рамках которой составляется план на год. Новые версии Системы (релизы) выпускаются, как правило, каждые три месяца. Годовой план детализируется и корректируется для каждой выпускаемой версии Системы.

Стратегическое видение развития Системы формируется руководством Дирекции по технической деятельности Вендора и дополняется рекомендациями от службы эксплуатации, отдела развития продуктов и пожеланиями от конечных пользователей Системы, которые фиксируются службой клиентской поддержки в специализированной аналитической системе «Jira».

Функциональные и нефункциональные требования к Системе формируют план каждого релиза. Задачи записываются в бэклог, который ведется в аналитической системе «Jira» и приоритезируются владельцем продукта.

Процесс разработки и совершенствования Системы строится на базе методологии «Scrum» по принципам «Agile» с управлением задачами в учетной системе «Jira». Требования к Системе описываются в «Confluence» и декомпозируются таким образом, чтобы обеспечить возможность реализации каждой отдельной функции Системы в виде отдельного «merge request» в «Gitlab».

При реализации каждая разрабатываемая функция проходит полный жизненный цикл: анализ, проектирование, разработка, код ревью, тестирование, приемка.

Результат каждой итерации анализируется и корректирует план следующей итерации. Каждый компонент Системы разрабатывается силами отдельных команд. Это означает, что команды укомплектованы специалистами, которые гарантируют полный цикл реализации требований к компоненту без привлечения внешних специалистов: владелец продукта как источник знания о бизнес-требованиях, разработчики, тестировщики и системные аналитики необходимой квалификации.

Бизнес-требования создаются в системе «Confluence» в виде описания. Исходя из описания, производится декомпозиция на истории (story), а затем на отдельные задачи (issues) в «Jira» для программирования, и определяются сроки их выполнения.

Каждая задача разрабатывается в отдельной ветке «Git». После проведения функционального тестирования и стабилизации, соответствующая ветка проходит «pipeline» со сборкой, unit-тестами и т.д., и, в случае успеха, сливается с веткой

основной разработки «develop». В конце каждой итерации основная ветка разработки проходит регресс-тестирование для подтверждения общей работоспособности Системы.

Перед релизом все компоненты Системы развертываются совместно для релизного оценочного и интеграционного тестирования Системы. На базе результатов тестирования в соответствии с критериями качества принимается решение о выпуске релиза или возвращении Системы на доработку. В случае принятия решения о выпуске релиза в «Git» создается отдельная ветка с префиксом «-rc» (release candidate), после чего специалистами отдела автоматизации она сливается с веткой со стабильным кодом «master».

Инсталляция Системы осуществляется Вендором или Заказчиком самостоятельно. Инструкция по инсталляции и дистрибутив предоставляется Заказчику Вендором.

2.4.2. Внедрение

Заказчик, получив дистрибутив от Вендора, организует развертывание Системы в своей инфраструктуре.

Процесс внедрения и доработки функционала под требования Заказчика, а также процесс функционирования, сопровождения и устранения возникающих ошибок производится в соответствии с договором на внедрение. При необходимости Вендор оказывает требуемую помощь и устраняет возникающие ошибки.

Основные цели и задачи внедрения:

- развертывание Системы в инфраструктуре Заказчика;
- подключение пользователей Заказчика к Системе;
- подключение Системы к полигонам и базам данных Заказчика;
- передача и разработка всей необходимой документации;
- обучение персонала Заказчика использованию и поддержке Системы.

В процессе внедрения также может быть выполнено:

- настройка любой части решения под бизнес-процессы Заказчика;
- изменение / расширение модели бизнес-данных необходимыми объектами, изменение атрибутного состава;
- изменение / расширение экранов, форм, интерфейса;
- изменение / расширение любой логики, связанной с особенностями бизнес-процессов Заказчика;
- проведение интеграции с любой существующей Системой Заказчика для получения или передачи данных;

– разработка необходимых отчетов, виджетов, дашбордов;
– иное, в зависимости от пожеланий Заказчика.

2.4.3. Документирование

Процесс управления документацией является неотъемлемой частью всех стадий и этапов ЖЦ Системы. Документирование происходит одновременно с процессами проектирования и разработки каждого из релизов Системы или после них.

Заказчику в составе дистрибутивов предоставляется документация в составе:

– настоящий документ;
– документация на Систему.

После внедрения Системы Заказчику предоставляется отчетная документация по проекту, в составе которой могут быть:

– организационно-техническое архитектурное решение;
– пояснительная записка к техническому заданию;
– инструкция пользователя;
– инструкция администратора;
– программа и методика испытаний.

2.4.4. Управление развертыванием

Развертывание и сборка исходных кодов Системы поддерживается системой управления версиями «Gitlab». Система запускается как набор docker-контейнеров, взаимодействующих между собой. Агенты запускаются на отдельных хостах, на которых установлены отслеживаемые БД. Для сборки компонентов на основе исходных кодов используется сервер непрерывной интеграции и доставки (CI / CD) «Gitlab», позволяющий быстро выявлять проблемы интеграции, немедленно прогонять тесты для свежих изменений, а также вместе с текущей стабильной версией иметь другие версии сборок для тестирования, демонстрации, и др.

После каждого релиза Система со всем окружением разработки развертывается на независимом сервере, расположенном в devops-инфраструктуре.

Каждый релиз Системы выпускается системой управления версиями «Gitlab» в виде отдельного дистрибутива, который представляет собой .tgz-архив. В архиве содержится файл Системы, запускаемый на серверах Заказчика со всеми необходимыми зависимостями.

2.5. Поддержка и сопровождение

Гарантийная поддержка Системы осуществляется Вендором. Срок гарантийной поддержки определяется договором на внедрение.

Плановое техническое сопровождение внедренной Системы осуществляется специалистами Заказчика. При необходимости Заказчик может обратиться за поддержкой к Вендору.

2.5.1. Обеспечение гарантии качества

Обеспечение качества программного обеспечения (Software quality assurance, SQA) – набор процедур мониторинга разработки программного обеспечения и методов, используемых для обеспечения его качества.

Руководство по качеству при разработке Вендора основано на требованиях стандартов системы менеджмента качества ГОСТ Р ИСО 9000-2015, 9001-2015, 9004-2010, 19011-2003, 10005-2007.

Управление качеством разрабатываемой Системы обеспечивается условиями договорных отношений с Заказчиками в соответствии с требованиями ГОСТ Р ИСО 9001-2015 и контролируется соответствующими службами и структурными подразделениями Вендора.

Процесс проверки качества Системы осуществляется в соответствии с запланированными мероприятиями, чтобы удостовериться, что получаемые в результате разработки Системы результаты соответствуют поставленным целям и задачам. Проверка завершается до официального выпуска релиза Системы.

Процедуры обеспечения качества у Вендора охватывают весь цикл разработки Системы, включая такие процессы как: определение требований, проектирование, разработка, контроль исходного кода, анализ кода, конфигурационное управление, тестирование, управление релизами и интеграция продуктов.

Процедуры обеспечения качества включают:

- цели;
- возможности;
- процедуры;
- измерения;
- проверки.

2.5.2. Тестирование

Для определения полноты соответствия установленных функциональных требований и созданного релиза у Вендора организованы следующие процессы тестирования:

- функциональное тестирование (functional testing);
- системное тестирование (system testing);
- тестирование производительности (performance testing);
- регрессионное тестирование (regression testing);
- модульное тестирование (unit testing);
- тестирование безопасности (security testing).

В случае выявления на этапе тестирования дефектов или несоответствий реализованного функционала функциональным требованиям задача переводится обратно в разработку, а затем, после доработки, – снова в тестирование. Цикл повторяется до тех пор, пока указанная функциональность не будет полностью соответствовать заявленным требованиям.

Перед слиянием кода, исправляющего дефект, проводится код ревью, а также функциональное и регресс-тестирование на отдельно развернутом под данный дефект стенде.

2.5.3. Аудит

Вендор проводит регулярные аудиты (проверки) своей системы менеджмента качества, процессов ЖЦ и самих разрабатываемых систем.

Назначением аудита Системы является независимая оценка Системы и процессов на предмет их соответствия применимым регулирующим документам, стандартам, руководящим указаниям, планам и процедурам.

Аудит является формально организованной деятельностью, участники которой выполняют определенные роли, такие как: главный аудитор (lead auditor), второй аудитор (another auditor), регистратор (recorder) и инициатор (initiator). В аудите принимает участие представитель Вендора.

В результате аудита идентифицируются случаи несоответствия и формируется отчет, необходимый команде разработки для принятия корректирующих действий, а также формируется конкретный план мероприятий. После реализации плана осуществляется верификация выполненных работ. Проводится как внутренний аудит, так и аудит с привлечением сторонних организаций.

2.5.4. Устранение неисправностей, выявленных в ходе эксплуатации

Проблемы, возникающие в процессе эксплуатации, регистрируются в специализированной аналитической системе Вендора «Jira». Данная система используется не только службой поддержки, но и другими структурными подразделениями. В данную систему также поступают все типы замечаний и пожеланий, независимо от их источника возникновения.

Собранные проблемы категоризируются по критичности для использования Системы и по распространенности данной проблемы. Категоризированные проблемы анализируются на предмет возможных действий. Вновь выявленные типовые проблемы, которые можно решить силами службы поддержки Вендора, добавляются в базу знаний.

Для вновь выявленных проблем, которые не могут быть решены силами службы поддержки, формируется заявка на разработку. Данная заявка на разработке привязывается к ошибке в «Jira» и контролируется до момента устранения в следующем релизе.

В некоторых случаях может быть разработано временное решение, реализуемое службой поддержки и смягчающее остроту проблемы (hotfix), но не решающее проблему в полном объеме, тогда это временное решение добавляется в базу знаний службы поддержки.

2.5.5. Устранение сбойных ситуаций

Сбойные ситуации регистрируются в специализированной аналитической системе Вендора «Jira». После фиксации сбойной ситуации Вендором производится классификация и приоритезация обращения.

Устранение сбойной ситуации в работе, возникшей по причине ошибочного поведения Системы, выполняется сотрудниками Вендора в соответствии с SLA, определенным на этапе подписания договора на внедрение Заказчику.

Устранение сбоев может осуществляться как в удаленном формате, так и с выездом на объект, если удаленное подключение по каким-либо причинам невозможно. Особо критичные сбои держатся на контроле непосредственно у руководителя управления разработки и развития информационных систем со стороны Вендора.

После устранения сбойной ситуации Вендором проводится работа по выявлению причин сбоя и минимизации рисков повторения подобной ситуации в будущем.

2.5.6. Эксплуатация

Эксплуатация Системы заключается в исполнении, функционировании ее на электронных вычислительных машинах (далее – ЭВМ) для обработки информации и в получении результатов, являющихся целью ее создания, а также в обеспечении достоверности и надежности выдаваемых данных.

Процесс эксплуатации состоит из работ и задач организации, эксплуатирующей Систему. Процесс охватывает эксплуатацию Системы и поддержку пользователей в процессе эксплуатации.

Оператор выполняет следующее:

- управляет процессом эксплуатации на проектном уровне в соответствии с процессом управления;
- определяет инфраструктуру для данного процесса в соответствии с процессом создания инфраструктуры;
- адаптирует данный процесс к условиям проекта в соответствии с процессом адаптации;
- управляет процессом эксплуатации на организационном уровне в соответствии с процессами усовершенствования и обучения.

Если оператор является поставщиком программной услуги, то оператор выполняет также процесс поставки.

Процесс эксплуатации Системы состоит из следующих работ и задач:

- подготовка процесса;
- эксплуатационные испытания;
- эксплуатация системы;
- поддержка пользователя.

2.5.7. Приобретение и поставка

Приобретение Заказчиком Системы осуществляется в рамках договора на поставку. В поставке Заказчику передается экземпляр Системы в виде .tgz-архива с дистрибутивом и документацией в его составе.

Дистрибутив представляет собой .tgz-архив, который содержит в себе пакеты, файлы конфигурации и скрипты запуска установки Системы.

По договору поставки Заказчику передается в собственность экземпляр Системы, который рассматривается в качестве вещи. Покупатель может свободно владеть и распоряжаться (в т.ч. передавать) таким носителем с экземпляром Системы (ст. 1270 ГК РФ), однако саму Систему он может использовать только путем записи в память ЭВМ и применения пределах объявленных функциональных возможностей (ст. 1280 ГК РФ).

Поставка Системы может осуществляться в коробочной версии на физических носителях информации в комплекте с документацией. Возможна поставка Системы путем передачи ее экземпляра по сети связи. Существуют варианты поставки Системы с ее установкой на оборудовании Заказчика непосредственно сотрудником поставщика на объекте Заказчика или в удаленном режиме.

Условия договора поставки Системы зависят от коммерческих и финансовых договоренностей сторон.

2.6. Информация о персонале

2.6.1. Обучение и квалификация персонала

Вендор обладает высококвалифицированной командой с опытом разработки программных продуктов и утилит на языке «Java». Все специалисты компании проходят обучение и внутреннюю сертификацию, а также постоянно совершенствуют свои навыки и квалификацию.

Вендор уделяет значительное внимание повышению квалификации своих сотрудников. Необходимый уровень знаний, умений и навыков, как требование к каждой должности, определяется моделью профессиональных и личных компетенций, принятой для соответствующей позиции в компании (hard / soft skills' model). Все сотрудники активно участвуют в реальных проектах разработки, получая опыт и нарабатывая практику.

Цель повышения квалификации персонала – поддержание и повышение уровня квалификации с учетом требований компании к определенной должности, роли.

2.6.2. Информация о необходимом персонале для обеспечения поддержки

Для работы с Системой необходимы следующие специалисты.

1. Пользователь Системы – специалист (служащий организации) Заказчика, использующий Систему для осуществления собственных ежедневных трудовых функций.
2. Администратор Системы – специалист IT-подразделения Заказчика, ответственный за корректную работу прикладных сервисов внутри организации, а также оказывающий внутреннюю поддержку пользователей при работе с Системой.
3. Инженер – инженер IT-подразделения Заказчика, осуществляющий работы по технической поддержке Системы на территории Заказчика.
4. Администратор операционной системы (системный администратор) – специалист IT-подразделения Заказчика, ответственный за корректную работу базовых сервисов внутри организации (операционные системы, сетевая инфраструктура, политики безопасности).

Общая численность персонала, относящегося к перечисленным категориям, зависит от специфики решаемых прикладных задач, масштаба Системы и количества одновременно работающих пользователей.

Обучение персонала Заказчика возможностям и методикам настройки Системы может выполняться Вендором в рамках проекта по внедрению Системы на

завершающих этапах и обычно занимает от одного до нескольких дней (в зависимости от категории пользователя).

Первичный инструктаж пользователей по работе с Системой осуществляется в форме демонстрации ключевых особенностей Системы и ее использования на рабочем месте пользователя. Инструктаж может быть проведен в дистанционной (вебинар) или очной формах. Длительность инструктажа около 120 минут. Обучение администраторов и инженеров работе с Системой и ее развертыванию осуществляется в рамках проекта внедрения или на специальных вендорских курсах.

В ходе обучения слушатели знакомятся с возможностями поддержки и настройки Системы и выполняют практические (лабораторные) работы. Обучение может быть проведено в очной и дистанционной (вебинар) формах. В зависимости от уровня подготовки слушателя, длительность курса может быть скорректирована в соответствии с программой обучения, утвержденной Вендором.

2.6.3. Размещение персонала Вендора

Персонал Вендора, задействованный в разработке и совершенствовании ПО, устранении сбойных ситуаций и техподдержки, включает сотрудников следующих отделов:

- отдела разработки;
- отдела автоматизации;
- отдела развития продуктов;
- отдела технической поддержки.

Фактический адрес размещения инфраструктуры разработки: Российская Федерация, г. Москва, вн.тер.г. муниципальный округ Солнцево, ш. Киевское, км 22-й, д. 6А, стр. 1., корпус В2, 108811.

Фактический адрес размещения разработчиков: Российская Федерация, г. Москва, вн.тер.г. муниципальный округ Солнцево, ш. Киевское, км 22-й, д. 6А, стр. 1., корпус В2, 108811.

Фактический адрес размещения службы поддержки: Российская Федерация, г. Москва, вн.тер.г. муниципальный округ Солнцево, ш. Киевское, км 22-й, д. 6А, стр. 1., корпус В2, 108811.