СИСТЕМА КОНТРОЛЯ ЗАЩИЩЕННОСТИ И СООТВЕТСТВИЯ СТАНДАРТАМ

полное наименование объекта разработки

СКЗСС

сокращенное наименование объекта разработки

Пояснительная записка

наименование утверждаемого документа

Подп. и дата | Инв. № дубл. | Взам. инв. № | Подп. и дата | Инв. № подл.

Изм	Лист	№ докум.	Подп.	Дата

Лист 1

Копировал Формат А4

СОДЕРЖАНИЕ

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

ИБ	Информационная безопасность
КИС	Корпоративная информационная система
ОС	Операционная система
ПО	Программное обеспечение
СКЗСС	Система контроля защищенности и соответствия стандартам
СУБД	Система управления базами данных

1. НАЗНАЧЕНИЕ, ОБЛАСТЬ ИСПОЛЬЗОВАНИЯ И ЦЕЛЬ СОЗДАНИЯ СИСТЕМЫ ОБЩИЕ ПОЛОЖЕНИЯ

Основной целью создания СКЗСС является повышение уровня защищенности информационных ресурсов путем организации автоматизированного контроля возникновения и устранения технических уязвимостей и ошибок в конфигурации компонентов информационных автоматизированных систем и организации периодического автоматизированного контроля эффективности применяемых мер защиты.

СКЗСС предназначена для получения данных о параметрах конфигурации компонентов информационных автоматизированных систем, влияющих на информационную безопасность, а также справочной и вспомогательной информации о компонентах информационных автоматизированных систем.

2. ОПИСАНИЕ ПРОЦЕССА ДЕЯТЕЛЬНОСТИ

Основной целью создания СКЗСС является повышение уровня защищенности информационных ресурсов организации за счет предупреждения инцидентов информационной безопасности, связанных с использованием уязвимостей в компонентах информационных автоматизированных систем. Наличие подобных уязвимостей может быть обусловлено:

- использованием программного обеспечения, нарушающего требования политики информационной безопасности;
- наличием ошибок в используемом программном обеспечении и программно-аппаратных комплексах;
- несоответствием конфигурации программного обеспечения и программно-аппаратных комплексов требованиям информационной безопасности.

Предупреждение подобных инцидентов обеспечивается решением следующих задач:

- инвентаризацией аппаратного и программного обеспечения узлов вычислительной сети Заказчика;
- анализом защищенности узлов вычислительной сети;
- контролем соответствия конфигурации узлов вычислительной сети требованиям информационной безопасности;
- контролем изменений в конфигурации узлов вычислительной сети.

Для решения указанных задач средствами СКЗСС производится сканирование узлов вычислительной сети и формирование отчетов по результатам сканирования. Перечень узлов для сканирования определяется персоналом СКЗСС и задается в настройках сканирования.

СКЗСС обеспечивает сканирование узлов вычислительной сети в трех режимах: режим PenTest, режим Audit и режим Compliance.

Сканирование в режиме PenTest направлено на получение оценки защищенности контролируемого узла со стороны внешнего злоумышленника и отличается использованием минимальных привилегий в сканируемой системе. С помощью данного сканирования выявляются уязвимости программного обеспечения, проверка стойкости паролей и отсутствующие обновления ОС Microsoft Windows.

Сканирование в режиме Audit предполагает использование специальной учетной записи для более глубокой проверки безопасности операционной системы и приложений контролируемого узла.

При сканировании в режиме Compliance выполняется проверка контролируемого узла на соответствие различным стандартам безопасности.

Используемые режимы определяются настройками сканирования, при этом возможно одновременное использование нескольких режимов.

До начала сканирования Администратор СКЗСС создает задачу на сканирование, которая включает в себя одну или несколько подзадач. Каждая подзадача состоит из перечня сканируемых узлов и профиля, определяющего особенности сканирования узлов из этого перечня. Сканирование, определяемое параметрами задачи, может быть запущено вручную или автоматически в заданное время, в том числе многократно с заданной периодичностью. Результаты сканирования сохраняются в СУБД сервера управления СКЗСС и используются для создания отчетов.

Выходными данными СКЗСС являются отчеты, которые формируются в соответствии с заданными шаблонами.

2.1 Инвентаризация программного и аппаратного обеспечения контролируемых узлов

Инвентаризация программного и аппаратного обеспечения контролируемых узлов производится при сканировании в режиме Audit.

Для представления собранной инвентаризационной информации используется отчет об инвентаризации. Сведения, отображаемые в отчете об инвентаризации, определяются типом сканируемого узла.

2.2 Анализ защищенности контролируемых узлов

Анализ защищенности контролируемых узлов производится при сканировании в режимах PenTest и Audit. Результаты сканирования представляются в отчете о найденных уязвимостях.

При сканировании в режиме PenTest выявляются уязвимости, которые могут быть использованы внешним по отношению к контролируемому узлу нарушителем (т.е. нарушителем, который для реализации угрозы может использовать только взаимодействие с контролируемым узлом по доступным протоколам сетевого и транспортного уровней). Отчет об уязвимостях, выявленных в режиме PenTest, содержит перечень протоколов, доступных для взаимодействия с контролируемым узлом, и выявленные уязвимости в реализации данных протоколов.

При сканировании в режиме Audit выявляются уязвимости, которые могут эксплуатироваться как внешним нарушителем, так и нарушителем, имеющим полный или ограниченный доступ к операционной системе и прикладному ПО контролируемого узла. Отчет об уязвимостях,

выявленных в режиме Audit, содержит перечень программ, функционирующих на контролируемом узле, и выявленные в них уязвимости.

Независимо от режима сканирования, отчет об уязвимостях содержит следующую информацию:

- идентификатор уязвимости по каталогу Common Vulnerabilities and Exposures[1] (если уязвимость в нем зарегистрирована);
- краткое и подробное описания уязвимости;
- рекомендации, описывающие действия по устранению уязвимости (в явной форме или в форме ссылки на соответствующие документы);
- ссылки на публикации, содержащие дополнительную информацию об уязвимости;
- рейтинг и классификацию уязвимости в соответствии с методикой CVSS[2];
- уровень критичности (низкий, средний, высокий), присваиваемый уязвимости на основании ее рейтинга.

В зависимости от режима сканирования, отчет об уязвимостях может также содержать дополнительную информацию о просканированных узлах.

При сканировании в режиме PenTest допускается ошибочное выявление уязвимостей (false positive). Ошибочная идентификация уязвимости возможна в случаях, когда при сканировании были выявлены некоторые признаки наличия уязвимости, но совокупности выявленных признаков недостаточно для принятия однозначного решения о наличии уязвимости. Подобные уязвимости отмечаются в отчете как «подозрение на уязвимость».

2.3 Контроль соответствия требованиям безопасности

Контроль соответствия требованиями безопасности производится при сканировании в режиме Compliance. При этом результаты одного сканирования могут использоваться для оценки соответствия просканированных узлов нескольким техническим стандартам.

Отчет о соответствии техническому стандарту (стандартам) формируется в соответствии с заданными настройками шаблона и содержит:

- перечень узлов, для которых проверялись требования безопасности;
- перечень технических стандартов, применимых к данным узлам;

[1] Common Vulnerabilities and Exposures (CVE) — Справочник (база данных) уязвимостей — [Электронный ресурс] / MITRE Corp. — [Б. м.]: MITRE. — Корректируется ежедневно. — Режим доступа: http://cve.mitre.org/

[2] A Complete Guide to the Common Vulnerability Scoring System (CVSS) — Система оценки уязвимостей — [Электронный ресурс] / Peter Mell, Karen Scarfone, Sasha Romanosky). — Version 2.0. — [Б. м.]: National Institute of Standards and Technology, Carnegie Mellon University, June 2007

- диаграмму, отражающую соотношение выполненных и невыполненных требований;
- описание требований безопасности.

Описание каждого требования включает в себя:

- краткую и подробную характеристику требования;
- результаты проверки данного требования;
- рекомендации по приведению узла в соответствие с данным требованием.

3. ОСНОВНЫЕ ТЕХНИЧЕСКИЕ РЕШЕНИЯ

3.1 Функциональная структура системы

В состав СКЗСС входят следующие подсистемы:

- подсистема инвентаризации;
- подсистема анализа защищенности;
- подсистема контроля соответствия стандартам;
- подсистема отчетности;
- подсистема обновления;
- подсистемам управления.

Подсистема инвентаризации используется при сканировании узлов вычислительной сети, обеспечивая идентификацию доступных на момент сканирования сетевых узлов и сбор следующей инвентаризационной информации:

- сведений о составе аппаратного обеспечения узла;
- сведений о составе программных средств узла;
- сведений об отдельных настройках программного обеспечения, существенных для решения задач инвентаризации.

Подсистема анализа защищенности обеспечивает выявление уязвимостей на контролируемых узлах и обеспечивает сбор информации о настройках параметров безопасности контролируемых узлов, а также прочих конфигурационных параметров, некорректная настойка которых может привести к снижению защищенности контролируемых узлов.

Подсистема контроля соответствия стандартам обеспечивает анализ собранной инвентаризационной информации, конфигурационной информации и информации об уязвимостях. Результатом анализа являются данные о соответствии или несоответствии контролируемых узлов техническим стандартам безопасности.

Подсистема отчетности обеспечивает формирование отчетов о результатах сканирования (в том числе автоматическое по завершении задачи).

Подсистема обновления обеспечивает централизованное обновление компонентов системы. В качестве источника обновлений должен использоваться сервер организации – производителя программного обеспечения СКЗСС.

Подсистема управления обеспечивает централизованное управление Системой и выполняет следующие функции:

- управление задачами сканирования;

- управление автоматическим запуском задач сканирования;
- управление компонентами СКЗСС;
- управление доступом к компонентам и подсистемам СКЗСС (идентификация и аутентификация пользователей СКЗСС по имени и паролю, разграничение доступа пользователей к функциям СКЗСС).

Подсистемы инвентаризации, анализа защищенности, контроля конфигурации реализованы средствами программных компонентов СКЗСС, описанных ниже.

3.2 Описание компонентов системы

Система контроля защищенности и соответствия стандартам информационных ресурсов строится на базе ПО MaxPatrol производства компании ЗАО «Позитив Текнолоджиз». При помощи ПО MaxPatrol реализуются все описанные в разделе 3.1 подсистемы СКЗСС.

ПО MaxPatrol включает в себя следующие компоненты:

- сервер управления MaxPatrol Server;
- сканер MaxPatrol Scanner;
- консоль управления MaxPatrol Console.

Сервер управления MaxPatrol Server является основным модулем ПО MaxPatrol. В состав MaxPatrol Server входит база знаний, содержащая информацию о проверках, уязвимостях и стандартах, модуль управления и сканирующее ядро. Сервер управления MaxPatrol Server используется для проведения сканирования, построения отчетов и управления системой. Он содержит собственную локальную базу данных учетных записей и групп пользователей, которые используются для разграничения доступа к элементам ПО MaxPatrol (задачам, отчетам и т.д.).

Сканер MaxPatrol Scanner является дополнительным сканирующим модулем, подключаемым к серверу управления MaxPatrol Server. Вся информация о контролируемых узлах, собранная сканером MaxPatrol Scanner, передается серверу управления MaxPatrol Server.

Консоль управления MaxPatrol Console предоставляет графический интерфейс для взаимодействия с пользователями. С помощью консоли управления MaxPatrol Console пользователи подключаются к доступным для них компонентам ПО MaxPatrol, просматривают и изменяют конфигурацию данных компонентов, создают и модифицируют задачи на проведение сканирований, а также просматривают информацию о ходе выполнения задач и отчеты о результатах сканирований.

Контроль сегментов вычислительной сети осуществляется следующим образом:

- Сканирование рабочих станций, серверов и активного сетевого оборудования осуществляется при помощи Сервера управления СКЗСС.

– Все собранные в результате сканирования данные сохраняются в базе данных.

3.3 Обновление компонентов СКЗСС

Целью обновления компонентов ПО MaxPatrol является поддержание базы знаний и ПО MaxPatrol в актуальном состоянии, что позволяет получать достоверную информацию о текущем уровне защищенности контролируемых узлов.

Обновления ПО MaxPatrol отличаются по объему и частоте выхода. Политика обновлений продуктов линейки MaxPatrol приведена в Таблица 1.

Таблица 1. Политика обновлений ПО MaxPatrol

Тип обновления	Описание	Объем	Период
Оперативные обновления	Содержат информацию о срочных или критичных уязвимостях	0 – 2 МБ	По мере необходимости
Плановые обновления базы знаний	Содержат информацию о новых уязвимостях, ошибках и стандартах	1 – 10 МБ	Еженедельно
Новые выпуски ПО (релизы)	Содержат новые версии ПО MaxPatrol	~100 МБ	Ежемесячно, по мере выхода
Оперативное исправление ошибок ПО	Содержат исправления ошибок ПО MaxPatrol	1 – 100 МБ	В случае обнаружение критических ошибок

В качестве источника обновлений используется сервер организации-производителя программного обеспечения СКЗСС, расположенный по адресу update.maxpatrol.com. Узел update.maxpatrol.com передает данные с использованием протокола SSL/TLS по портам 443/TCP или 2002/TCP.

3.4 Режимы функционирования

Система контроля защищенности и соответствия стандартам информационных ресурсов может функционировать в следующих режимах:

– штатный (нормальный) режим;

– технологический режим;

– аварийный режим.

3.4.1 Штатный режим

В данном режиме СКЗСС обеспечивает решение своих функциональных задач в полном объеме.

3.4.2 Технологический режим

Технологический режим функционирования применяется для проведения работ по обслуживанию программно-аппаратных средств СКЗСС. В технологическом режиме работы допускается недоступность основного функционала системы.

3.4.3 Аварийный режим

Аварийный режим функционирования применяется при обнаружении сбоев и отказов в работе компонентов СКЗСС. Аварийный режим характеризуются полной или частичной потерей работоспособности СКЗСС. Классификация подобных отказов и описание связанных с ними потерь функциональности СКЗСС приведены в Таблица 2.

Таблица 2. Классификация сбоев СКЗСС

Описание сбоя	Последствия сбоя	Особенности эксплуатации СКЗСС до устранения сбоя
Выход из строя Сервера управления СКЗСС	Невозможность сканирования узлов	До устранения сбоя сканирование не производится
Выход из строя Сервера СУБД	Невозможность сканирования узлов Невозможность сканирования узлов Недоступность данных, накопленных в процессе эксплуатации СКЗСС	До устранения сбоя сканирование не производится

3.5 Численность, квалификация и функции персонала

СКЗСС предусматривает следующие роли персонала, осуществляющего эксплуатацию системы:

- Администратор СКЗСС, выполняющий функции административного управления системой;
- Пользователь СКЗСС, выполняющий функции анализа отчетов и устранения обнаруженных уязвимостей.

В состав обслуживающего персонала СКЗСС входят:

- Администратор СКЗСС, обеспечивающий функционирование прикладного ПО СКЗСС;
- Системный администратор, обеспечивающий бесперебойную работу технических средств и системного ПО СКЗСС;

- Администратор СУБД, обеспечивающий бесперебойную работу СУБД СКЗСС.

Пользователями СКЗСС являются сотрудники отдела ИТ, при этом Администратор СКЗСС наделяет пользователя различными привилегиями в системе в зависимости от его должностных обязанностей.

Администрирование и резервное копирование ОС СКЗСС осуществляют специалисты отдела ИТ (роль – Системный администратор).

Администрирование и резервное копирование базы данных СКЗСС осуществляют специалисты отдела ИТ (роль – Администратор СУБД).

Описание функций персонала, требований к квалификации, разграничения ответственности, а также порядка обслуживания и эксплуатации СКЗСС приведено в следующих документах:

- Система контроля защищенности и соответствия стандартам. Регламент эксплуатации системы;
- Система контроля защищенности и соответствия стандартам. Руководство администратора;
- Система контроля защищенности и соответствия стандартам. Руководство пользователя.

ПРИЛОЖЕНИЕ А. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Контролируемый узел – сервер, рабочая станция или единица активного сетевого оборудования вычислительной системы. Контролируемый узел идентифицируется своим сетевым именем или IP-адресом.

Задача на сканирование – совокупность настроек, определяющих параметры сканирования узлов из задаваемого пользователем перечня.

Технический стандарт – совокупность требований безопасности, предъявляемых к определенному программному обеспечению или программно-аппаратному комплексу.