ЗАО «Инфосистемы Джет»

Информационная система управления инцидентами информационной безопасности «Джет Сигнал»

Описание функциональных характеристик

Москва
2016

Аннотация

Документ содержит описание применения информационной системы управления инцидентами информационной безопасности «Джет Сигнал» (далее – Система).

В разделе «Общие сведения» описана конфигурация Системы, среда её функционирования и средства разработки.

В разделе «Назначение Системы» описаны назначение программного решения и цели его использования, а также возможности, предоставляемые им для решения целевых задач. Областью применения Системы являются процессы регистрации, анализа, информирования о состоянии информационной безопасности объектов ИТ-инфраструктуры.

В разделе «Условия применения» описаны требования к программным и техническим средствам, которые необходимы для работы Системы.

В разделе «Описание задачи» указаны задачи, выполняемые в Системе.

В разделе «Входные и выходные данные» приведены сведения об информации, поступающей на вход Системы, и выходная информация.

Содержание

1 Общие сведения

1.1 Обозначение и наименование программы

Полное наименование программы: Информационная система управления инцидентами информационной безопасности «Джет Сигнал».

Сокращенное наименование: Система, Система «Джет Сигнал».

1.2 Инструментальные средства разработки

Для разработки Системы были использованы следующие языки программирования:

– PHP 5.4.4 (Yii framework 2.0);

– JavaScript (Backbone 1.3.*, jQuery 2.*).

2 Назначение программы

Система предназначена для повышения эффективности обработки инцидентов информационной безопасности (далее – ИБ), за счет автоматизации следующих процессов:

- планирование, учет и контроль работы дежурных смен;
- сбор, регистрация и обработка информации об инцидентах ИБ;
- контроль исполнения поручений в рамках решения задач по устранению причин и последствий инцидентов ИБ, а также по обеспечению защиты объектов и активов ИБ;
- доведение информационно-распорядительных документов до подразделений;
- управление жизненным циклом инцидентов ИБ;
- ведение базы знаний;
- обмен формализованной информацией об инцидентах между подразделениями организации;
- обмен быстрыми сообщениями между операторами Системы.

Система «Джет Сигнал» поддерживает схемы развёртывания:

- для приложения, которое установлено в виде одного автономного узла;
- распределённой информационной системы при развёртывании двух и более экземпляров приложения с обеспечением обмена информацией между ними.

В Системе реализовано взаимодействие узлов, функционирующих в разных сегментах информационной безопасности:

- двунаправленное взаимодействие при одинаковом классе защиты сегментов. Например, обмен данными между закрытыми сегментами;
- однонаправленное взаимодействие при разных классах защиты сегментов. Например, передача данных от интернет-сегмента к закрытому сегменту.

Система «Джет Сигнал» поддерживает работу с мандатной моделью управления доступом Astra Linux Special Edition 1.5. При этом в зависимости от назначения установки приложения мандатная модель управления доступом может быть как задействована, так и отключена в момент установки приложения.

В состав Системы входят подсистемы:

- управления дежурными сменами;
- управления инцидентами;
- управления поручениями;
- ведения Базы знаний;

– взаимодействия;
– администрирования;
– новостная лента;
– обмена сообщениями (веб-чат).

Функциональная архитектура Системы приведена на Рис. 1.

Рис. 1 – Функциональная архитектура Системы «Джет Сигнал»

Подсистема управления дежурными сменами предназначена для планирования, учета и контроля дежурных смен.

Подсистема управления инцидентами предназначена для информационного и процессного обеспечения работы подразделений по обнаружению и предотвращению компьютерных атак, а также расследования компьютерных инцидентов.

Подсистема поддерживает процессы:

– обеспечения жизненного цикла инцидентов;
– классификации и приоритизации инцидентов;
– принятия решений на базе планов мероприятий;
– организации оперативного реагирования;
– устранения инцидентов и их последствий.

Подсистема управления поручениями предназначена для:

- ведения и контроля исполнения поручений в рамках задач по обеспечению защиты объектов и активов ИБ;
- ведения и контроля исполнения распорядительных документов.

Подсистема ведения базы знаний предназначена для ведения информации об инцидентах, угрозах, уязвимостях активов ИБ и т.п.

Подсистема взаимодействия предназначена для обмена сообщениями в условиях территориальной и сетевой распределенности ИТ-инфраструктуры.

Подсистема взаимодействия предоставляет единый интерфейс обмена данными.

В подсистеме реализованы следующие функции:

- первичный контроль входной информации, включающий проверку её состава и полноты.
- прием входящих E-mail сообщений с вложениями, передаваемых из внешней системы SIEM.
- взаимодействие узлов Системы, функционирующих в разных сегментах.

Схема обмена данными в разных сегментах действия Системы приведена в Приложение А.

Подсистема администрирования предназначена для управления учетными записями пользователей, ведения ролевой модели, регистрации действий пользователей и системных событий. В подсистеме также реализованы функции ведения справочной информации.

Подсистема Новостная лента предназначена для публикации новостей и сообщений, в том числе об актуальных угрозах информационной безопасности.

Подсистема обмена сообщениями (веб-чат) предназначена для обеспечения быстрого обмена сообщениями между пользователями.

Система работает в автоматическом и автоматизированном режимах.

В автоматическом режиме операции выполняются без участия пользователя. Например, выбор мероприятий по реагированию на инцидент зависит от типа инцидента и происходит автоматически.

В автоматизированном режиме операции выполняются с участием пользователя. Например, информацию о событиях ИБ, полученную по E-mail и по телефону, оператор дежурной смены вводит вручную.

3 Условия применения

Система функционирует на платформах Intel x86, Intel x86 и AMD64. Рекомендуемые характеристики аппаратного обеспечения сервера:

- процессор не менее 4 ядер с тактовой частотой не менее 3 ГГц;
- объем оперативной памяти не менее 3 ГБ;
- жесткий диск не менее 250 ГБ.

Сервер функционирует под управлением операционной системы Astra Linux Special Edition 1.5 и использует СУБД PostgreSQL 9.4, веб-сервер Apache 2.2.22, интерпретатор PHP 5.4.4, сервер очередей RabbitMQ.

Для управления работой Системы используется веб-интерфейс администратора безопасности и интерфейс командной строки (CLI) для системного администратора. Компьютер, используемый в качестве АРМ администратора безопасности и системного администратора, должен отвечать следующим требованиям:

- процессор не менее 4 ядер с тактовой частотой не менее 2,8 ГГц;
- объём оперативной памяти не менее 4 ГБ;
- объём жёсткого диска не менее 128 ГБ;
- разрешение экрана при работе с интерфейсом не менее 1024x768.

АРМ администратора безопасности и системного администратора должен быть оборудован сетевым адаптером Ethernet.

Для работы Системы требуется:

1) Серверная часть:

- операционная система ОС Astra Linux;
- СУБД PostgreSQL 9.4.

2) Клиентская часть:

- веб-браузер Mozilla Firefox 44.0.2 и выше.

Для обеспечения дополнительной защищённости передаваемых данных между узлами системы, между которыми не требуется двунаправленный обмен интеграционными сообщениями, возможна организация сетевого взаимодействия через специализированный однонаправленный шлюз СТРОМ-1000.

Шлюз должен соответствовать следующим характеристикам:

- обеспечить скорость передачи информации не менее 1 Гбит/с;
- иметь сетевые интерфейсы:

- внешний: RJ-45, медь, витая пара, Ethernet 100/1000BASE-T; SFP, оптика, Ethernet 1000BASE-X;
- внутренний: SC, многомодовая оптика, 850нм, 1000BASE-SX.

4 Описание задачи

Задачи Системы «Джет Сигнал»:

- ведение планов работы дежурных смен и их контроль;
- ведение планов мероприятий по реагированию на инциденты ИБ;
- создание и ведение карточек инцидентов в автоматическом режиме и вручную;
- автоматическое предоставление плана мероприятий в зависимости от типа инцидента для устранения последствий инцидента ИБ;
- обмен формализованной информацией об инцидентах между задействованными подразделениями;
- создание и ведение информационных кампаний;
- создание и ведение поручений;
- создание и ведение распорядительных документов;
- ведение базы знаний и базы угроз;
- публикация информации (ведение новостей);
- обмен быстрыми сообщениями между пользователями (веб-чат);
- ведение справочной информации;
- ведение профилей пользователей;
- ведение ролей и прав доступа;
- просмотр журнала системных событий.

4.1 Ведение планов работы дежурных смен и их контроль

Задачи решаются с помощью функций подсистемы **управления дежурными сменами.**

В подсистеме реализованы следующие функции:

- составление графика дежурных смен с учетом отсутствий сотрудников;
- назначение новой роли сотрудникам в дежурной смене;
- составление отчета для передачи дежурных смен;
- инициирование передачи дежурных смен руководителем;

4.2 Ведение планов мероприятий по реагированию на инциденты ИБ

Задача решается с помощью функций модуля **Планы мероприятий** подсистемы **управления инцидентами.**

В модуле реализованы следующие функции:

- создание карточки мероприятий с перечнем шагов по устранению инцидентов ИБ;

- редактирование карточки мероприятий;
- удаление (деактивация) карточки плана мероприятий;
- восстановление (активация) карточки плана мероприятий.

Плану мероприятия в автоматическом режиме присваиваются статусы в соответствии с этапами жизненного цикла:

- активный;
- неактивный.

4.3 Создание и ведение карточек инцидентов в автоматическом режиме и вручную

Задача решается с помощью функций модуля **Инциденты** подсистемы **управления инцидентами.**

Автоматическое формирование карточек выполняется на основании данных, поступающих из системы сбора данных о событиях и инцидентах (SIEM). Данные в подсистему управления инцидентами передаются с помощью подсистемы взаимодействия.

В модуле реализованы следующие функции:

- создание карточки инцидента;
- категоризация инцидента с помощью присвоения инциденту типа, уровня критичности, приоритета, источника получения;
- актуализация данных зарегистрированного инцидента;
- назначение исполнителя по расследованию инцидента;
- смена исполнителей;
- связывание инцидента и поручения – в рамках устранения причин и последствий инцидента;
- связывание инцидента и информационной кампании в ходе анализа инцидента;
- прикрепление файлов к карточке инцидента;
- атрибутивный поиск и фильтрация данных по инцидентам;
- закрытие инцидента.

Инциденту в автоматическом режиме присваиваются статусы в соответствии с этапами его жизненного цикла:

- новый;
- в работе;
- выполнен;
- отклонен;

- возвращен;
- анализ;
- на аудите;
- аудит;
- закрыт.

4.4 Автоматическое предоставление плана мероприятий в зависимости от типа инцидента для устранения последствий инцидента ИБ

Задача решается с помощью функций модуля **Инциденты** подсистемы **управления инцидентами.**

Модуль обеспечивает автоматическую привязку плана мероприятий по устранению инцидента к карточке инцидента в зависимости от его типа.

4.5 Обмен формализованной информацией об инцидентах между задействованными подразделениями

Задача решается с помощью функций модуля **Инциденты** подсистемы **управления инцидентами.**

Модуль поддерживает передачу карточки инцидента в другие подразделения.

4.6 Создание и ведение информационных кампаний

Задачи решаются с помощью функций модуля **Информационные кампании** (ИК) подсистемы **управления инцидентами.**

В модуле реализованы следующие функции:

- создание карточки ИК;
- редактирование карточки ИК;
- привязка нескольких инцидентов к карточке ИК;
- прикрепление файлов к карточке ИК;
- атрибутивный поиск и фильтрация данных по ИК;
- закрытие ИК.

Информационной кампании в автоматическом режиме присваиваются статусы в соответствии с этапами жизненного цикла:

- активная;
- неактивная.

4.7 Создание и ведение поручений

Задачи решаются с помощью функций модуля **Поручения** подсистемы **управления поручениями.**

В модуле реализованы следующие функции:

- создание карточки поручения;
- редактирование карточки поручения;
- установление сроков исполнения поручений;
- привязка нескольких инцидентов к карточке поручения;
- прикрепление файлов;
- атрибутивный поиск и фильтрация данных по поручениям;
- исполнение поручения;
- контроль исполнения поручений.

Поручению в автоматическом режиме присваиваются статусы в соответствии с этапами жизненного цикла:

- зарегистрировано;
- принято к исполнению;
- отклонено;
- исполнено.

4.8 Создание и ведение распорядительных документов

Задачи решаются с помощью функций модуля **Распорядительные документы** подсистемы **управления поручениями.**

В модуле реализованы следующие функции:

- создание карточки распорядительного документа;
- редактирование карточки распорядительного документа;
- контроль информации о просмотре распорядительного документа, включая отметки о ФИО пользователя, времени первого и последнего просмотра, количестве просмотров.

В модуле реализованы механизмы защиты прикрепленного документа от скачивания и копирования.

4.9 Ведение базы знаний

Задачи решаются с помощью функций подсистемы **Ведения базы знаний.**

Подсистема обеспечивает возможности создания, редактирования и удаления информации в структуре Wiki.

4.10 Публикация информации (ведение новостей)

Задача решаются с помощью функций подсистемы **Новостная лента.**

Новостная лента обеспечивает выполнение следующих операций с новостями:

- создание;
- публикация;
- редактирование;
- удаление;
- просмотр;
- помещение новости в раздел «Избранное»;
- поиск новости по дате, периоду публикации, по фрагменту текста.

При добавлении и редактировании новости реализована возможность работы с текстом в формате Markdown. Формат позволяет редактировать текст, используя специальный синтаксис. Пользователь может выделять текст жирным шрифтом, создавать многоуровневые заголовки, создавать списки и т. п.

4.11 Обмен быстрыми сообщениями между пользователями (веб-чат)

Задача решаются с помощью функций подсистемы **обмена сообщениями (веб-чат).**

Веб-чат обеспечивает выполнение следующих операций:

- ввод сообщений;
- просмотр сообщений;
- создание групп чат;
- удаление групп чат;
- выход из групп.

4.12 Ведение справочной информации

Задачи решаются с помощью функций модуля **Справочники** подсистемы **администрирования.**

В модуле реализованы следующие функции:

- создание справочной информации;
- редактирование справочной информации;
- удаление (деактивация) справочной информации.

4.13 Ведение профилей пользователей

Задачи решаются с помощью функций модуля **Профили пользователей** подсистемы **администрирования.**

В модуле реализованы следующие функции:

- создание профиля пользователя;
- редактирование профиля пользователя;
- удаление (деактивация) профиля пользователя.

4.14 Ведение ролей и прав доступа

Задачи решаются с помощью функций модуля **Роли и права доступа** подсистемы **администрирования.**

В модуле реализованы следующие функции:

- создание роли;
- редактирование роли;
- удаление (деактивация) роли;
- назначение прав доступа к функциям для разных ролей;
- редактирование прав доступа;
- исключение права доступа к функции из ранее назначенного списка функций.

4.15 Просмотр журнала системных событий

Задачи решаются с помощью функций модуля **Журнал регистрации** подсистемы **администрирования.** Модуль обеспечивает ведение журнала регистрации системных событий.

В модуле реализованы следующие функции:

- просмотр событий в системе;
- атрибутивный поиск и фильтрация данных.

Журнал регистрации событий содержит следующую информацию:

- тип события;
- время возникновения события;
- описание события.

5 Входные и выходные данные

5.1 Входные данные

Система получает следующие входные данные:

– Данные инцидентов ИБ;

– Поручения;

– Распорядительные документы;

– Новостные данные;

– Данные для статей Базы знаний;

– Справочные данные (типы, категории инцидентов, подразделения, должности);

– Данные пользователей и их функции в Системе;

– Данные для составления графика выхода сотрудников в дежурные смены.

5.2 Выходные данные

Система создает следующие выходные данные:

– Зарегистрированные в БД инциденты, связанные с планами мероприятий, информационными кампаниями, поручениями и другими инцидентам.

– Зарегистрированные в БД информационные кампании, связанные с инцидентами.

– Зарегистрированные в БД поручения, связанные с инцидентами, назначенные на исполнителей и обработанные.

– Зарегистрированные в БД исходящие поручения, связанные с другими поручениями.

– График выхода сотрудников в дежурную смену с поддержкой функции предоставления полномочий в день выхода в смену в соответствии с ролью.

– Доставленные пользователям новости.

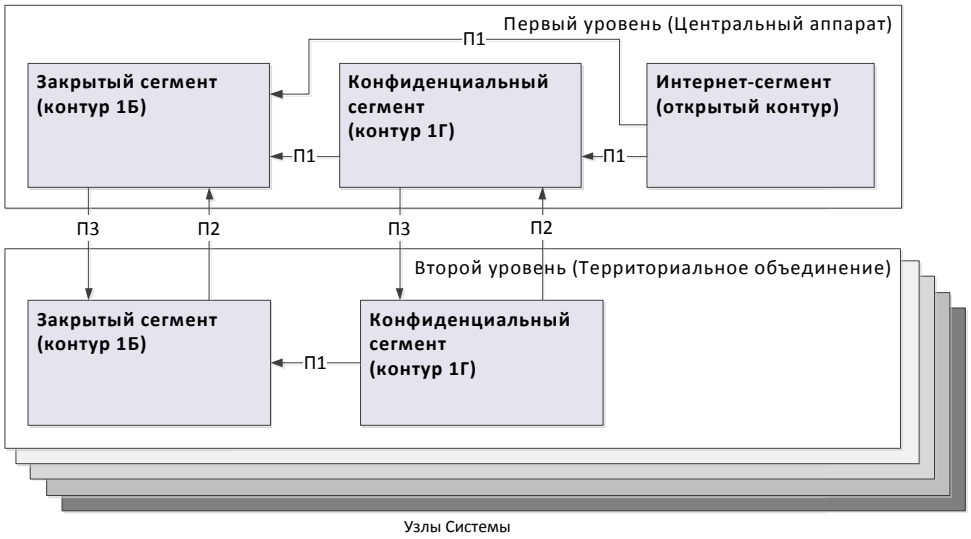
– Организованная по wiki-технологии База знаний.

6 Перечень принятых сокращений

SIEM	Security Information and Event Management – система управления информацией о безопасности и событиях безопасности
АРМ	Автоматизированное рабочее место
ИБ	Информационная безопасность
ИК	Информационная кампания
ОС	Операционная система
СУБД	Система управления базами данных
Узел Системы	Часть разворачиваемой Системы, в состав которой входит аппаратное обеспечение, операционная система, СУБД и база данных, сервер очередей и экземпляр приложения
Экземпляр приложения	Копия приложения, входящая в состав каждого узла Системы

Приложение А
Общая схема обмена данными

Общая схема обмена данными между узлами Системы «Джет Сигнал» в разных сегментах приведена на рисунке.



П1: Поток подъёма информации от узла с меньшим уровнем допуска к узлу Системы с более высоким уровнем

П2: Поток подъёма информации от окружного узла с тем же уровнем допуска к узлу центрального аппарата

П3: Поток спуска информации с тем же уровнем допуска от вышестоящего узла Системы к нижестоящему узлу

Система «Джет Сигнал» может функционировать как распределенное решение. Это сделано в целях обеспечения возможности автономной работы узлов Системы. Предполагается, что в каждом сегменте информационной безопасности каждого территориального объединения развёрнут свой узел Системы. Пользователи работают с экземпляром приложения в соответствующем узле Системы центрального аппарата или территориального объединения, или сегмента ИБ – в зависимости от расположения АРМ.

Каждый узел Системы включает в себя:

- базу данных PostgreSQL 9.4;
- веб-сервер Apache 2.2.22-13astra.se15;
- интерпретатор PHP 5.4.4-2astra2;
- сервер очередей RabbitMQ 2.8.4-1;
- приложение Системы «Джет Сигнал», содержащее: логику, настройки, хранилище файлов и файлов истории работы приложения и интеграционного модуля.

В существующей конфигурации система допускает до 4096 узлов Системы.