ООО «Гефест Технолоджиз»
ИНН: 7100029285; ОГРН: 1227100014195; КПП: 710001001.

Программный комплекс автоматизации ситуационного центра информационной безопасности "Эгида"

Описание функциональных характеристик экземпляра программного обеспечения

(для проведения экспертной оценки в Экспертном совете при Минцифры России)

ПРИНЯТЫЕ ТЕРМИНЫ, ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

Термин	**Расшифровка, пояснение или определение**
ИБ	Информационная безопасность
Исходное событие	Данные, полученные из источника событий
Нормализация	Создание структурированного экземпляра события и заполнение его полей данными исходного события на основе сопоставлений, заданных в источнике события
Обогащение	Расширение контекста нормализованного события дополнительными данными на основе правил обогащения, справочников и данных из внешних справочных систем
Справочник	Объект, содержащий данные для совместного и/или многоразового использования модулями и пользователями программного комплекса
Подготовленное событие	Событие, прошедшее нормализацию и обогащение
Корреляция	Производимый в реальном времени анализ подготовленных событий на наличие признаков угроз ИБ
Процессная модель	Описывает последовательность процессов обработки событий и инцидентов ИБ организации (действия и исполнителей)
Сценарий реагирования (playbook)	Набор действий по устранению конкретного типа инцидента ИБ
Карточка события/инцидента ИБ	Содержит детальную информацию о событии/инциденте ИБ: данные расширенного контекста с идентификаторами угроз и иную вспомогательную информацию, инструменты анализа связанных данных и обработки события/инцидента ИБ

Оглавление

1. ОБЩИЕ СВЕДЕНИЯ

«Эгида» – автоматизированный программный комплекс обеспечения работы ситуационного центра ИБ, объединяющий в себе функции систем кибербезопасности разных типов и назначений, позволяющий:

- выполнять сбор, хранение и обработку, в том числе автоматическую, событий;
- упрощать, ускорять и автоматизировать процессы обработки и расследования событий и инцидентов ИБ;
- осуществлять мониторинг, оперативно выявлять инциденты ИБ;
- поддерживать процессы управления инцидентами ИБ посредством постоянного расширения контекстов оценки событий с использованием инструментов автоматизации;
- производить автоматическое реагирование, формировать отчетность;
- поддерживать процессы повышения зрелости ситуационного центра.

2. ОПИСАНИЕ ФУНКЦИОНАЛЬНЫХ ХАРАКТЕРИСТИК

Программный комплекс автоматизации ситуационного центра информационной безопасности "Эгида" обеспечивает выполнение следующих функций:

- сбор, подготовка и хранение событий;
- мониторинг и корреляция событий;
- управление и выполнение сценариев реагирования;
- управление событиями и инцидентами ИБ;
- визуализация метрик ИБ;
- формирование отчетности.

2.1. Функция сбора, подготовки и хранения событий

Функция позволяет управлять подключением к различным источникам событий с целью извлечения или приема данных из них. Функция позволяет настроить параметры подключения в зависимости от типа источника и его местоположения.

Функция осуществляет подготовку (нормализацию и обогащение) собранных событий на основе создаваемых пользователями правил. Функция предоставляет возможность настройки правил (критерии их применения, производимые ими преобразования данных и т.п.).

Функция осуществляет передачу данных исходных и подготовленных событий в хранилище программного комплекса для дальнейшей обработки и анализа.

2.2. Функция мониторинга и корреляции событий

Функция производит анализ подготовленных и исходных событий на наличие угроз ИБ в автоматическом и ручном режимах.

В автоматическом режиме анализ осуществляется на основе создаваемых пользователями правил корреляции. Функция позволяет настроить параметры правил, включая критерии поиска событий и производимые с найденными событиями действия и преобразования данных. По результатам анализа функция автоматически регистрирует события и инциденты ИБ для их последующей обработки.

В ручном режиме функция обеспечивает возможность поиска событий, удовлетворяющих критериям выявления угроз. Функция позволяет связать найденные события с уже зарегистрированными событиями и инцидентами ИБ или зарегистрировать новые.

2.3. Функция управления и выполнения сценариев реагирования

Функция обеспечивает создание и настройку сценариев реагирования для автоматизации и ускорения реагирования на события и инциденты ИБ, повышения эффективности их обработки.

Функция обеспечивает выполнение шагов сценариев реагирования в автоматическом и полуавтоматическом режимах.

2.4. Функция управления событиями и инцидентами ИБ

Функция формирует карточки событий и инцидентов ИБ для фиксации связанной с ними информации. Функция выполняет управляющие действия с зарегистрированными событиями и инцидентами ИБ на основе заданной пользователями процессной модели.

Возможно связывание правил корреляции с созданными сценариями реагирования. При срабатывании правила корреляции функция осуществляет управление взаимодействием с пользователем на основе шагов связанного сценария.

2.5. Функция визуализации метрик ИБ

Функция отображает статистические и аналитические данные о работе ситуационного центра с возможностью их манипуляции для детального анализа трендов и проблем.

2.6. Функция формирования отчетности

Функция осуществляет сохранение в формат CSV данных подготовленных событий, зарегистрированных событий и инцидентов ИБ, справочников.

3. ЮРИДИЧЕСКАЯ ИНФОРМАЦИЯ

3.1. Авторские права

Материалы, приведенные в настоящем документе, являются собственностью ООО «Гефест Технолоджиз» и могут быть использованы только для целей экспертной проверки Системы в рамках процедуры включения в Единый реестр российских программ для электронных вычислительных машин и баз данных, а также для личных целей приобретателей программного комплекса автоматизации ситуационного центра информационной безопасности "Эгида".

Запрещается воспроизведение отдельных частей документа, внесение правок в него, размещение на сетевых ресурсах, распространение в любой форме (в том числе в переводе) на бумажных и электронных носителях, посредством каналов связи и средств массовой информации или каким-либо другим способом без специального письменного разрешения ООО «Гефест Технолоджиз» и ссылки на источник.

Программный комплекс автоматизации ситуационного центра информационной безопасности "Эгида" зарегистрирован ООО «Гефест Технолоджиз» и охраняется законом.

3.2. Содержание документа

Содержание данного документа может изменяться без предварительного уведомления. ООО «Гефест Технолоджиз» не несет ответственности за неточности и/или ошибки, допущенные в данном документе, и возможный ущерб, связанный с этим.