МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Самарский государственный технический университет»

Институт автоматики и информационных технологий

Кафедра Электронные системы и информационная безопасность

**ЗАДАНИЕ**
**НА ВЫПОЛНЕНИЕ ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ**
СамГТУ 100301.043.009.01 ТЗ

Обучающемуся Коновалову Александру Евгеньевичу, 4 курс, ИАИТ, 2 группа
*(фамилия, имя, отчество, курс, институт, группа)*

Тема Разработка подсистемы анализа инцидентов в информационной сети предприятия

Исходные данные (или цель работы) Система анализа событий безопасности в информационной сети предприятия

Перечень подлежащих исследованию, разработке, проектированию вопросов:

| Наименование вопроса | Результаты освоения ОПОП |
|---|---|
| 1. Постановка цели и задач для ВКР, обзор литературных источников | ОК-1, ОК-3, ОК-6 |
| 2. Анализ систем класса SIEM для мониторинга сетевой инфраструктуры | ОК-8, ОПК-1 |
| 3. Детальное изучение SIEM-систем, в частности PT MaxPatrol SIEM | ОПК-4, ПК-12 |
| 4. Описание части системы мониторинга, занимающейся сбором данных | ОК-4, ОК-5, ПК-5 |
| 5. Описание архитектуры аналитической части системы мониторинга | ОПК-2, ПК-10, ПК-11 |
| 6. Изучение методики написания правил корреляции | ОК-1, ОПК-4, ПК-2 |
| 7. Разработка подсистемы анализа инцидентов в информационной сети предприятия | ПК-2, ПК-3, ПК-6, ПК-14 |
| 8. Внедрение разработанной подсистемы анализа инцидентов в PT MaxPatrol SIEM | ОПК-3, ОПК-5, ПК-1, ПК-15 |
| 9. Расследование инцидентов информационной безопасности с помощью разработанной подсистемы | ОПК-7, ПК-4, ПК-13 |
| 10. Анализ экономической эффективности разработанной подсистемы, безопасности жизнедеятельности сотрудников при эксплуатации разработки | ОК-2, ОК-9, ОПК-6, ПК-7 |

Перечень презентационного материала:
1. Плакат с архитектурой SIEM
2. Плакат с интерфейсом PT MaxPatrol SIEM
3. Плакат со структурой PT MaxPatrol SIEM
4. Плакат с алгоритмом работы программного кода
5. Плакат с расследованием инцидента «Подбор пароля»
6. Плакат с внедрением разработанной подсистемы анализа инцидентов
7. Плакат с анализом эффективности разработанной подсистемы
8. Плакат об экономической эффективности разработки

9. Раздаточный материал_____

Нормоконтролер:

_старший преподаватель Н.В, Андреева_

*(должность, ф.и.о. нормоконтролера)*

Дата выдачи задания: « » _____ 20__г.

Задание согласовано и принято к исполнению.

| **Руководитель** | **Студент** |
|---|---|
| ___Н.Е. Карпова___ | ___А.Е. Коновалов_____ |
| *(И. О. фамилия,)* | *(И. О. фамилия)* |
| ___к.т.н., доцент___ | ___ИАИТ, 2 группа____ |
| *(должность, уч. степень, уч. звание)* | *(институт, группа)* |
| _____ | _____ |
| *(подпись, дата)* | *(подпись, дата)* |

Тема утверждена приказом по СамГТУ № _1/238-А_ от "_23_"__04__2021г.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Самарский государственный технический университет»

Институт автоматики и информационных технологий

Кафедра Электронные системы и информационная безопасность

**Календарный план**
выполнения выпускной квалификационной работы
Обучающегося Коновалова Александра Евгеньевича, 4 курс, ИАИТ, 2 группа
*(фамилия, имя, отчество, курс, институт, группа)*

Тема Разработка подсистемы анализа инцидентов в информационной сети предприятия

| | Этапы выполнения ВКР | Дата (срок) выполнения | | Отметка о выполнении |
|---|---|---|---|---|
| | | план | факт | |
| | Разработка структуры ВКР. Проведение литературного обзора | 01.12.2020-24.01.2021 | 01.12.2020-24.01.2021 | |
| | Сбор фактического материала (лабораторные, исследовательские работы и др.) | 25.01.2021-29.02.2021 | 25.01.2021-29.02.2021 | |
| | Подготовка рукописи ВКР | 02.03.2021-13.04.2021 | 02.03.2021-13.04.2021 | |
| | Доработка текста ВКР в соответствии с замечаниями научного руководителя | 14.04.2021-11.06.2021 | 14.04.2021-11.06.2021 | |
| | Предварительная защита квалификационной работы на кафедре | 02.06.2021 | 02.06.2021 | |
| | Ознакомление с отзывом научного руководителя | 05.06.2021 | 05.06.2021 | |
| | Подготовка доклада и презентационного материала | 15.06.2021-20.06.2021 | 15.06.2021-20.06.2021 | |

Студент А.Е. Коновалов
Руководитель к.т.н., доцент Н.Е. Карпова
Заведующий кафедрой П.О. Скобелев

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Самарский государственный технический университет»

Институт автоматики и информационных технологий

Кафедра Электронные системы и информационная безопасность

ДОПУСТИТЬ К ЗАЩИТЕ

Заведующий кафедрой_____Скобелев П.О.

«___» _____ 2021 г.

# Выпускная квалификационная работа
## СамГТУ 100301.043.009.02 ПЗ

Тема:__Разработка подсистемы анализа инцидентов в информационной сети предприятия____

Обучающийся_Коновалов Александр Евгеньевич, 4 курс, ИАИТ, 2 группа_____
*(фамилия, имя, отчество, курс, институт, группа)*

Руководитель работы _____к.т.н., доцент, Н.Е. Карпова
*(должность, подпись, дата, фамилия, инициалы)*

Нормоконтролер _____старший преподаватель Н.В. Андреева
*(подпись, дата, фамилия, инициалы)*

Консультант _____старший преподаватель Н.В. Андреева
*(подпись, дата, фамилия, инициал)*

Консультант _____к.т.н., профессор Н.Г. Яговкин
*(подпись, дата, фамилия, инициал)*

Самара 2021г.

Приложение 3

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Самарский государственный технический университет»
Институт автоматики и информационных технологий
Кафедра Электронные системы и информационная безопасность

# ОТЗЫВ
# руководителя выпускной квалификационной работы

на ВКР по теме «_Разработка подсистемы анализа инцидентов в информационной сети _предприятия_»

обучающегося___4____ курса ____2_____ гр., _Коновалова Александра Евгеньевича____

(Ф.И.О. обучающегося)

по направлению подготовки (специальности) _Информационная безопасность_

направленности (профилю) образования _Комплексная защита объектов информатизации (в промышленности)_

**Актуальность, практическая значимость и новизна ВКР**_____

_____

_____

_____

_____

**Соответствие структуры и содержания ВКР выданному заданию и теме**_____

_____

_____

**Уровень, полнота и качество поэтапной разработки темы**_____

_____

_____

**Логическая последовательность изложения материала**_____

_____

_____

**Умение обрабатывать и анализировать полученные результаты, обобщать, делать научные и практические выводы**_____

_____

_____

**Качество предоставления результатов и оформления работы**_____

_____

_____

**Умение работать с библиографическими источниками, справочниками**_____

**Степень самостоятельности обучающегося в процессе выполнения ВКР**_____

**Анализ отчета проверки ВКР на наличие заимствований**_____

**Достоинства работы, замечания (при наличии) и др.**_____

_____

**Вывод:** представленная ВКР *соответствует / не соответствует* основным требованиям, предъявляемым к ВКР и отраженным соответствующих локальных нормативных актах Университета и Программе государственной итоговой аттестации, и заслуживает оценки _____.

**Руководитель** _____ _к.т.н., доцент Карпова Н.Е._

(подпись) (должность, ученая степень, звание, Ф.И.О.)

«____»_____2021 г.

## РЕФЕРАТ

Пояснительная записка содержит ** страницы, ** иллюстрации, ** таблиц, 2 приложения, ** источника. Графический материал выполнен на 8 листах формата А1.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, УПРАВЛЕНИЕ СОБЫТИЯМИ БЕЗОПАСНОСТИ, СИСТЕМЫ МОНИТОРИНГА СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, КОРРЕЛЯЦИЯ, ФИЛЬТРАЦИЯ, АНАЛИЗ ИНЦИДЕНТОВ.

Объектом исследования является разработанная компанией Positive Technologies SIEM-система MaxPatrol.

Результатом проектирования является разработка и внедрение подсистемы анализа инцидентов в информационной сети предприятия.

В данной работе проведен анализ существующих на Российских и зарубежных рынках систем мониторинга событий информационной безопасности, определены наиболее эффективные архитектуры SIEM-систем. На основе статистики проведен анализ точности автоматического обнаружения инцидентов SIEM-системой. Разработаны правила корреляции, реализованные программным кодом, с целью снижения процента ложных срабатываний.

Приведено технико-экономическое обоснование проекта, а также рассмотрены вопросы обеспечения охраны труда.

В приложении приведены программные коды реализации подсистемы анализа инцидентов в информационной сети предприятия.

ГЛАВА 3. РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ ИБ С ПОМОЩЬЮ РАЗРАБОТАННОЙ ПОДСИСТЕМЫ

3.1. Разбор инцидента «Подбор пароля» в ручном режиме.

3.2. Разбор инцидента «Подбор пароля» после внедрения подсистемы.

ГЛАВА 4. ТЕХНИКО-ЭКОНОМИЧЕСКОЕ ОБОСНОВАНИЕ РАЗРАБОТКИ

4.1. Расчет затрат на реализацию проекта

4.2. Расчёт затрат на эксплуатацию проекта

4.3. Расчёт экономической эффективности проекта

ГЛАВА 5. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ЖИЗНЕДЕЯТЕЛЬНОСТИ

5.1. Анализ опасных и вредных производственных факторов при работе пользователей

5.1.1 Человек

5.1.1.1. Описание пользователей системы

5.1.1.2. Условия труда при работе с ВДТ и ПК

5.1.2. Машина

5.1.2.1. Характеристики

5.1.2.2. Шум

5.1.2.3. Электромагнитные излучения

5.1.2.4. Электробезопасность

5.1.3. Среда

5.1.3.1. Микроклимат

5.1.3.2. Естественное и искусственное освещение

5.1.3.3. Производственные здания и помещения

5.1.4. Организация и оборудование рабочих мест с ВДТ и ПЭВМ

5.1.5 Пожарная безопасность

5.2. Режим труда и отдыха при работе с ПК

ЗАКЛЮЧЕНИЕ

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

ПРИЛОЖЕНИЕ А

ПРИЛОЖЕНИЕ В

# ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

ИБ – информационная безопасность.

ИС – информационная система.

ЗИ – защита информации.

НСД – несанкционированный доступ.

SIM – управление информационной безопасностью.

SEM – управление события безопасности.

Событие ИБ – какое-либо распознанное явление в информационной системе или информационной сети.

Инцидент ИБ – Нарушение или возможность нарушения информационной безопасности предприятия или целой компании.

Угроза ИБ – теоретически реализуемое событие, действие или воздействие, а также процесс или явление, реализация которого приведет к возникновению инцидента ИБ.

Уязвимость ИС – слабое место в информационной системы, воспользовавшись которым злоумышленник способен целенаправленно реализовать угрозу ИБ.

Реагирование на инцидент ИБ – определенная совокупность действий, направленная на определение всех подробностей инцидента, минимизацию материального и репутационного ущерба от возникшего инцидента и предотвращение повторения инцидента ИБ

Управление рисками (risk management) – это практически постоянный процесс оценки рисков и последующей разработки возможных стратегий противодействия выявленным факторам риска.

SIEM (Security Information and Event Management) – система, которая обеспечивает анализ событий ИБ, исходящих от сетевых устройств и приложений, в режиме реального времени. Это позволяет провести реагирование на инцидент ИБ на ранней стадии, до ощутимого ущерба.

# ВВЕДЕНИЕ

ИТ-инфраструктура современных компаний очень сложна. В связи с этим главной проблемой построения защиты информационной структуры стала обработка поступающей информации. Число источников, обеспечивающих поступление актуальной информации по текущему состоянию защищенности непрерывно растет. Сегодня уже сложно найти корпоративное программное обеспечение, которое бы не вело запись в журнал и т.п. При этом вместе с увеличением объёма информации, администраторам ИБ всё сложнее отслеживать «общую картину». А ведь если своевременно не анализировать возникающие угрозы и не пытаться предотвратить их, любая система защиты окажется бесполезной.

В связи с этим крупные предприятия и государственные учреждения все чаще внедряют в свои информационные сети SIEM-системы. В течение последних лет спрос на технологию SIEM остается на высоком уровне. Однако исследование Positive Technologies 2020-го года показало, что рутинные операции всё ещё являются для специалистов самыми трудоемкими: больше половины респондентов тратят особенно много сил и времени на доработку правил корреляции с целью уменьшить число ложных срабатываний, а также на разбор поступающих уведомлений о возможных инцидентах. Поэтому автоматизация процессов обработки инцидентов для кардинального снижения числа ложных срабатываний SIEM-системы при работе с большими объемами данных является актуальной задачей.

Цель данной работы разработать подсистему анализа инцидентов в информационной сети предприятия.

Задачи:

1. Анализ работы SIEM-систем и аналитический разбор существующих Российских и зарубежных SIEM.
2. Разработка подсистемы анализа инцидентов в информационной сети предприятия

3. Расследование инцидентов ИБ с помощью разработанной подсистемы

# ГЛАВА 1. СИСТЕМЫ КЛАССА SIEM ДЛЯ МОНИТОРИНГА СЕТЕВОЙ ИНФРАСТРУКТУРЫ

## 1.1 Определение, общая информация

SIEM – аббревиатура, которая содержит в себе два других термина полностью характеризующих эту системы: SIM (Security Information Management) – управление информационной безопасностью и SEM (Security Event Management) – управление событиями безопасности. Так можно сделать вывод, что SIEM проводит анализ в режиме реального времени событий информационной безопасности, которые исходят от различных сетевых устройств и приложений, а также позволяет провести реагирование на инцидент ИБ на ранней стадии, до ощутимого ущерба.

Фундаментальный принцип SIEM-системы состоит в том, что данные о безопасности ИС собираются из самых различных источников данных, после чего результат обработки эти данных выводится в едином интерфейсе, доступном для операторов, администраторов, а также аналитиков и специалистов безопасности. Данный принцип работы системы ощутимо упрощает изучение и анализ тех или иных особенностей, соответствующих инцидентам ИБ. Такой сегмент, как SIM, преимущественно отвечает за анализ исторических данных, проведение ретроспективных проверок. SIM оптимизирует хранение данных и в целом улучшает долгосрочную эффективность используемой системы. Сегмент SEM в свою очередь делает особый акцент на выгрузке определенного объема данных, благодаря чему можно сразу же выявить инциденты ИБ, из имеющихся данных. При постоянном росте объема информации возникает необходимость в непрерывном расширении, а также дополнении функциональности таких продуктов.

Основная цель, для достижения которой и используются SIEM-системы – это повышение уровня информационной безопасности в имеющейся инфраструктуре предприятия за счет обеспечения возможности

манипулировать информацией о безопасности, а также осуществлять управление инцидентами и событиями безопасности на упреждение, в режиме максимально близком к реальному времени. Данный подход управления событиями ИБ позволяет реагировать на инциденты ИБ с запасом времени, до того, как ситуация уже станет критической. Управление можно автоматизировать с помощью специальных механизмов прогнозирования событий. Для этого берутся исторические данные и производятся автоматические донастройки параметров мониторинга в зависимости от состояния системы в текущий момент времени, а так с помощью корректировки различных параметров и правил корреляций в ручном режиме.

Комплекс SIEM используется как в рамках внутреннего SOC (Security Operations Center, центр управления безопасностью), так и в рамках услуг на аутсорсинге.

Само понятие SIEM было введено такими людьми, как Марк Николетто и Амрит Вильямс из компании Gartner в далёком 2005 г. Данное понятие подразумевает в себе следующие решаемые задачи: функциональность сбора, анализа и представления информации от сетевых устройств и устройств безопасности, приложений идентификации (управления учетными данными) и управления доступом, инструментов поддержания политики безопасности и отслеживания уязвимостей, операционных систем, баз данных и журналов приложений, а также сведений о внешних угрозах. Отдельное и большое внимание уделяется управлению привилегиями пользователей и служб, сервисам директорий и другим изменениям конфигурации, а также обеспечению аудита и обзора журналов, реакциям на инциденты.

Решаемые задачи:

1. Сбор, обработка и анализ событий безопасности, поступающих в систему из разнообразных источников;

2. Обнаружение в режиме реального времени инцидентов безопасности: как внешних, так и внутренних атак, нарушений критериев и политик безопасности;
3. Оперативная оценка защищенности информационных, телекоммуникационных и других критически важных ресурсов;
4. Анализ и управление рисками информационной безопасности;
5. Проведение расследования инцидентов информационной безопасности;
6. Принятие эффективных решений в рамках защиты информации;
7. Формирование оповещений и отчетов по проведенной работе.

Для того, чтобы вышеуказанные задачи успешно выполнялись в SIEM-системы заложен ряд принципов, описанных ниже:

1. Нормализация – приводит все данных от всех подключенных источников данных к единому внутреннему формату, который и используется для их хранения и последующей обработки. Пример такого «сырого» события от операционной системы Windows в формате «XML» представлен на рисунке 1, пример нормализованного события представлен на рисунке 2;

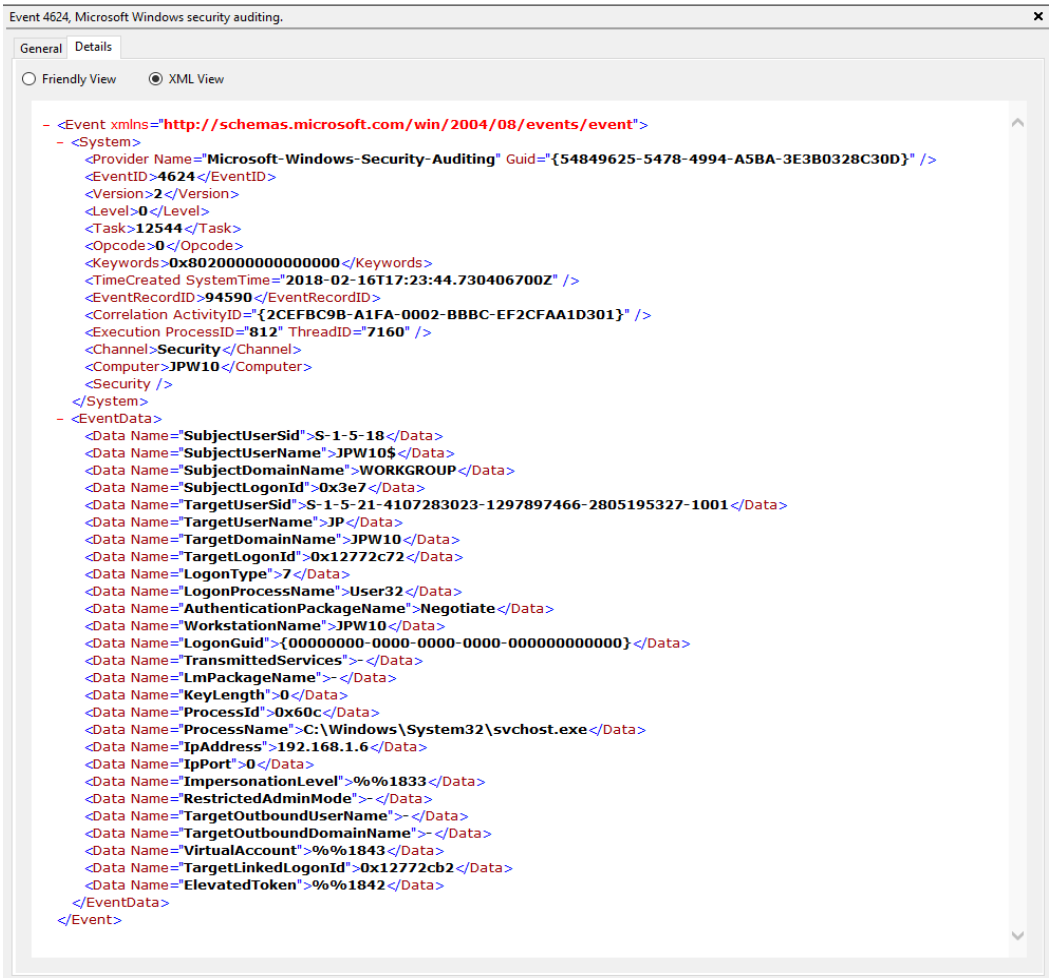



Рисунок 1 – Событие аутентификации Windows в формате XML

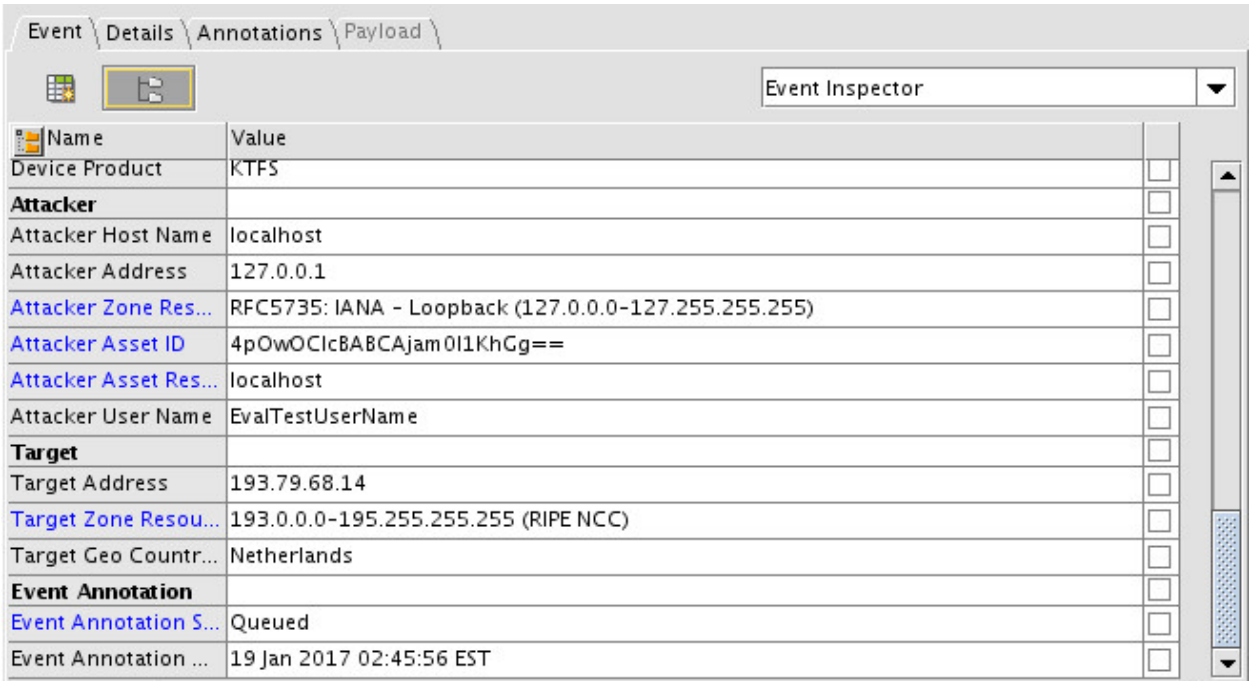



Рисунок 2 – Нормализованное событие

2. Фильтрация событий безопасности - это удалении избыточных событий;

3. Классификация нужна для определения принадлежности атрибутов событий безопасности определенным классам;
4. Агрегация объединяет те или иные события по схожим признакам;
5. Корреляция выявляет взаимосвязи между разнородными событиями;
6. Приоритезация выполняет функцию определения значимости и критичности событий ИБ на основании правил, которые определены в системе;
7. Анализ событий, инцидентов и их последствий подразумевает в себе моделирование событий, атак, а также их последствий, анализ уязвимостей и защищенности системы. Определяет конкретные параметры нарушителей, производит оценку риска, что позволяет в будущем выполнять прогнозирование событий ИБ и инцидентов;
8. Генерация отчетов и предупреждений – необходимая вещь для осуществления формирования, передачи, отображения или печати результатов функционирования и подробной отчетности по состоянию системы, выявленных событий ИБ;
9. Визуализация – для предоставления данных в удобном графическом виде, говорящих о результатах анализа событий ИБ, состоянии защищаемой системы и ее конечных элементов.

Функциональность SIEM:

1. Агрегация данных: управление журналами данных (логами), которые собираются с различных по своей сути источников, обеспечивается консолидация данных с целью поиска критических событий;
2. Корреляция: поиск общих атрибутов, связывание событий в значимые кластеры. Корреляция является типичной функцией компонента SEM (Security Event Management);
3. Оповещение: автоматизированный анализ корреляционных событий и генерация оповещений (инцидентов). Оповещение может быть выведено как в пользовательский интерфейс SIEM, так и в прочие

сторонние каналы: e-mail, различные платформы управления задачами и т.д.;

4. Средства отображения: отображение диаграмм, помогающих наглядно выявлять отклонения и аномалии в параметрах системы;
5. Совместимость (трансформируемость): применение приложений для автоматизации сбора данных, формированию отчетности для адаптации агрегируемых данных к существующим процессам управления информационной безопасностью и аудита;
6. Хранение данных: применение долговременных хранилищ данных в историческом порядке для обеспечения корреляции и трансформируемости. Хранение является необходимым для проведения ретроспективных экспертиз инцидентов информационной безопасности;
7. Экспертный анализ: возможность поиска по множеству журналов на различных узлах; может выполняться в рамках программно-технической экспертизы.

## 1.2 Архитектура SIEM

SIEM-систему внедряют в защищаемую информационную систему. Такая система имеет следующую архитектуру: «источники данных» — «хранилище данных» — «сервер приложений». SIEM-решения - интегрированные устройства (all-in-one) или комплексы из небольшого числа компонентов. Распределенная архитектура – это всегда большая производительность и лучшие возможности по масштабированию. Распределенная архитектура также позволяет произвести развертывание SIEM в IT-инфраструктурах, у которых организовано несколько площадок.

Для первоначальной обработки данных, сборов и фильтрации событий ИБ используются так называемые «Агенты».

Передача данных осуществляется двумя способами:

1. Источник данных самостоятельно производит инициацию передачи событий;
2. С источника данных события собираются в пассивном режиме.

Приведу практические примеры реализации данных способов. Первый пример для первого способа – на источнике указывается IP-адрес устройства, которое должно осуществлять сбор событий – то есть выполнять роль коллектора, а события отправляются адресату. Второй пример для второго способа – подразумевает в себе либо агентный, либо безагентный сбор информации. Для некоторых SIEM у некоторых источников могут быть доступны сразу оба способа. Безагентный способ предполагает использование настройки источника событий (Учетная запись, удаленный доступ, специальные протоколы). Агентный – реализуется с помощью специальной программы-агента.

После того, как данные о событиях безопасности будут собраны и отфильтрованы, они поступят в общее хранилище данных, где будут представлены во внутреннем формате для того, чтобы их можно было использовать в будущем, а также для анализа сервером приложений.

Реализацию основных функций защиты информации берет на себя «Сервер приложений», который производит анализ информации, которая хранится в соответствующем репозитории, после чего преобразует ее для выработки предупреждений или управленческих решений по ЗИ.

Пример архитектуры SIEM представлен на рисунке 3

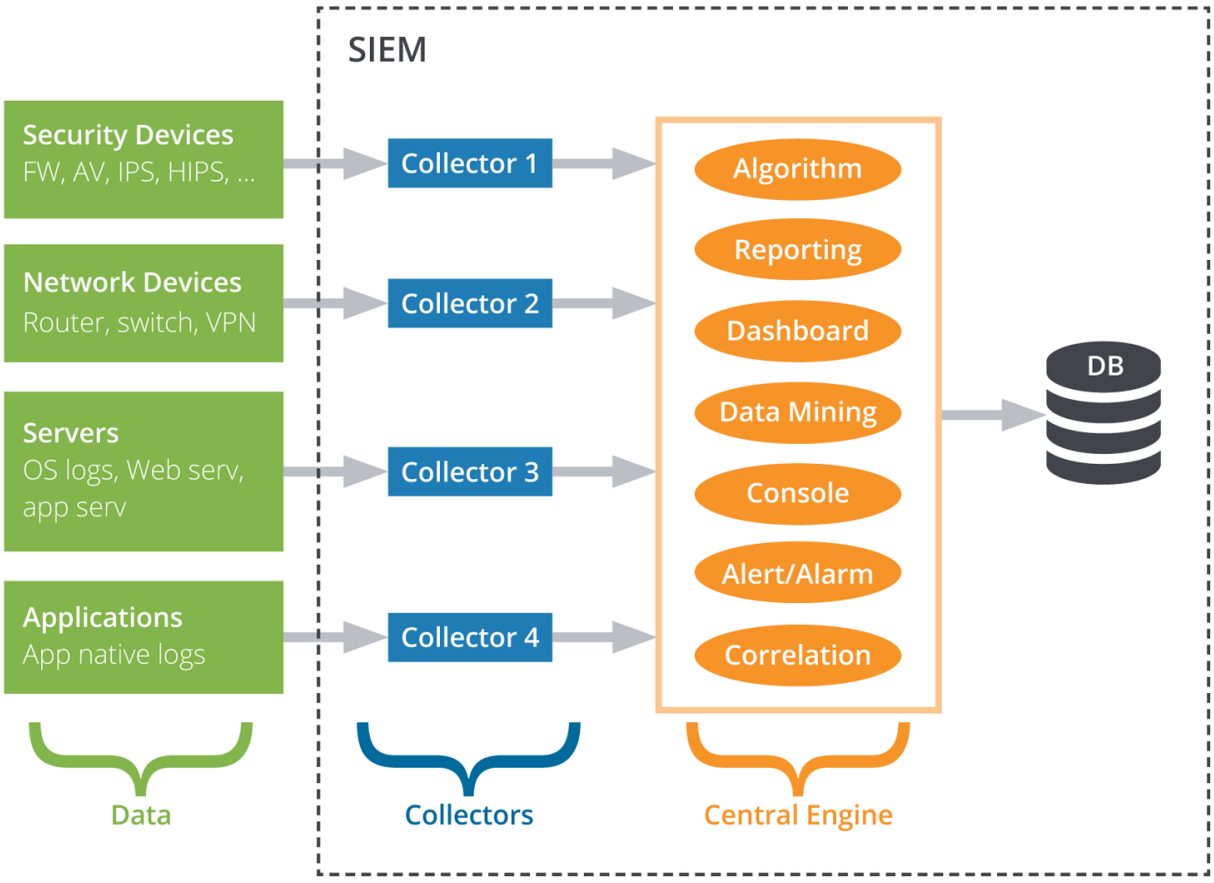



Рисунок 3 – Архитектура SIEM

Таким образом определяют три уровня построения SIEM-систем:

1. Сбор данных: осуществляется от источников различных типов, например, файловых серверов, межсетевых экранов, антивирусных программ;
2. Управление данными: данные, хранящиеся в репозитории, выдаются по запросам моделей анализа данных;

3. Анализ данных: результатом являются отчеты в предопределенной и произвольной форме, оперативная корреляция данных о событиях, а также выдаваемые предупреждения.

Источники данных:

1. Access Control, Authentication. Применяются для мониторинга контроля доступа к информационным системам и использования привилегий.
2. DLP-системы. Сведения о попытках инсайдерских утечек, нарушении прав доступа.
3. IDS/IPS-системы. Несут данные о сетевых атаках, изменениях конфигурации и доступа к устройствам.
4. Антивирусные приложения. Генерируют события о работоспособности ПО, базах данных, изменении конфигураций и политик, вредоносном коде.
5. Журналы событий серверов и рабочих станций. Применяются для контроля доступа, обеспечения непрерывности, соблюдения политик информационной безопасности.
6. Межсетевые экраны. Сведения об атаках, вредоносном ПО и прочем.
7. Сетевое активное оборудование. Используется для контроля доступа, учета сетевого трафика.
8. Сканеры уязвимостей. Данные об инвентаризации активов, сервисов, программного обеспечения, уязвимостей, поставка инвентаризационных данных и топологической структуры.
9. Системы инвентаризации и asset-management. Поставляют данные для контроля активов в инфраструктуре и выявления новых.
10. Системы веб-фильтрации. Предоставляют данные о посещении сотрудниками подозрительных или запрещенных веб-сайтов.

Внедрение SIEM трудозатратно. Необходимо учитывать такие факторы, как объёмные вычислительные ресурсы для эксплуатации, затраты на обслуживание SIEM-системы. Использование таких систем по большей

степени оправдано для организаций с распределённой информационной инфраструктурой при том условии, что она обязательно включает в себя большое разнообразие сетевых устройств и СЗИ, являющихся источниками событий ИБ, такие как: NGFW, IPS/IDS, различные АВПО, proxy-серверы и т.д.

Виды источников данных в виде схемы представлены на рисунке 4.

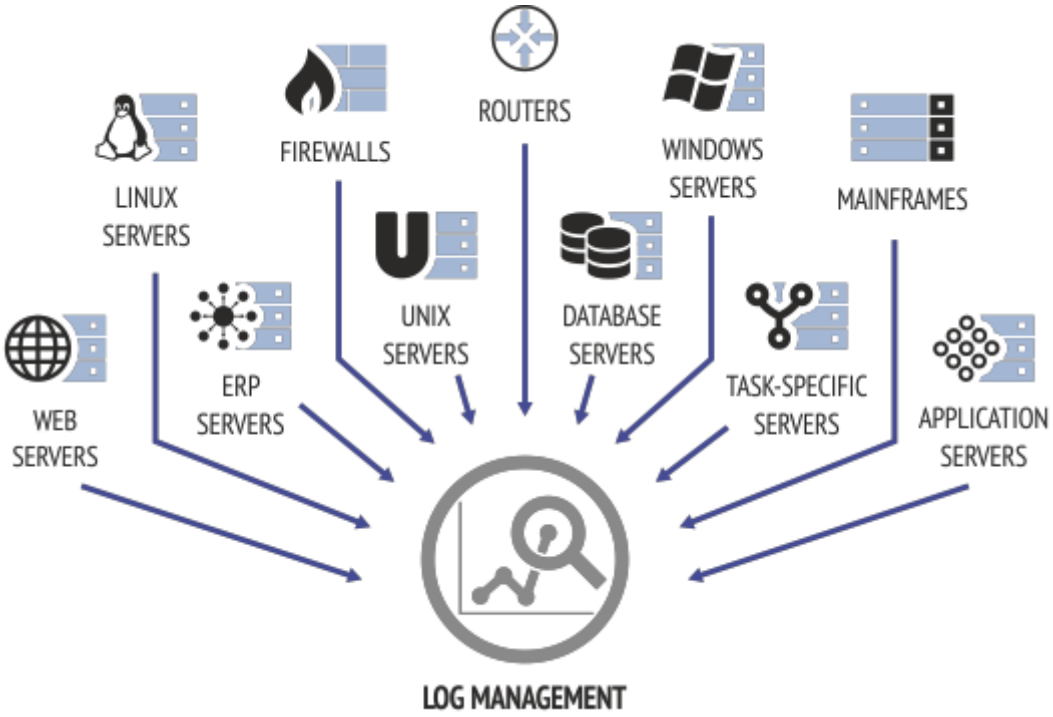



Рисунок 4 – Источники данных

### 1.3 Аналитический разбор существующих Российских и зарубежных SIEM-систем

В России государственные учреждения и крупный бизнес считается основным покупателем SIEM-систем. Крупные компании ищут продукты, которые могут отвечать их требованиям по следующим параметрам: производительность, масштабируемость, отказоустойчивость. Основным критерием в выборе системы остается соотношение «цена-качество». Государственные учреждения помимо критерия «цена-качество» обращают большое внимание на сертификаты соответствия требованиям регуляторов.

Основные задачи SIEM - консолидация событий из множества источников данных, последующих их анализ и оповещение специалистов ИБ о случившихся инцидентах ИБ. На отечественном рынке достаточно большой выбор SIEM-решений, как западных, так и Российских. Российские SIEM-решения в основном применяются на территории Российской Федерации. Поставкой и внедрением SIEM-систем занимаются бизнес-партнеры, аккредитованные производителями. В России таких компаний достаточно мало. Но крупные системные интеграторы, обладающие достаточным опытом, все же способны реализовать крупный SIEM-проект.

Ниже мною приводится более подробный анализ некоторых SIEM-систем.

**HPE ArcSight Hewlett Packard Enterprise (HPE)**

ArcSight — Одна из самых распространенных SIEM-систем как на зарубежном, так и на российском рынке. Данная система долгий промежуток времени считалась примером для других SIEM. С 2007 года реализовано огромное количество проектов по внедрению данной SIEM-системы. Важно отметить, что HPE ArcSight поддерживает интеграцию с ГосСОПКА.

Целевой сегмент HPE ArcSight – все секторы среднего и крупного бизнеса. Платформа имеет три варианта реализации:

- Платформа данных Arcsight Data Platform;

- Программное обеспечение Arcsight Enterprise Security Management (ESM);

- Программное-аппаратный комплекс Arcsight Express.

Платформа HPE ArcSight может быть развернута как устройство, как обычное ПО, так и виртуальное. HPE ArcSight поддерживает масштабируемую n–уровневую архитектуру с HPE ArcSight Management Center. HPE ArcSight Express доступен только в качестве устройства.

ArcSight Express - SIEM среднего уровня. HPE ArcSight ESM - SIEM для крупномасштабных развертываний и организаций, которые хотят построить свой «SOC».

В 2017 году вышел модуль ArcSight Investigate, который используется как усиление аналитических возможностей основной SIEM HPE ArcSight.

Преимущества HPE ArcSight:

- Arcsight ESM содержит в себе полный набор возможностей SIEM. Данный набор позволяет организовать свой собственный SOC с полным рабочим процессом.

- HPE User Behavior Analytics выявляет аномалии на основе анализа поведения пользователей и дополняет стандартную корреляцию.

- DNS Malware Analytics анализирует DNS–трафик и обеспечивает абсолютную видимость ИТ–инфраструктуры.

- Arcsight Threat Central содержит в себе базу знаний угроз.

- HPE Arcsight включает в себя широкий выбор уже подготовленных к использованию сторонних технологий и коннекторов.

ArcSight ESM имеет сертификат ФСТЭК России № 3605, подтверждающий выполнение требований руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) по 4 уровню контроля и Технических условий.

**IBM QRadar Security Intelligence Platform**

IBM QRadar Security Intelligence Platform содержит в себе следующие системы:

- Log Manager;

- SIEM;

- Flow Processor;

- Vulnerability Manager;
- Risk Manager;
- Network Insights;
- Watson Advisor for Cyber Security;
- Packet Capture and Incidents Forensics.

Все перечисленные компоненты являются платными. Данные платные компоненты дополняются бесплатным доступом к приложениям и репутационным базам из X-Force and App Exchange, UBA, интеграционные модули с другими системами безопасности от IBM.

QRadar может развертывается двумя вариантами: на физическом устройстве или виртуальном. Представляется как служба IaaS (Infrastructure-as-a-Service) в публичных или частных облачных сервиса, которая полностью управляется IBM вместе с дополнительным мониторингом событий IBM Managed Security Services. В недалеком прошлом, а именно в 2017 году, ряд российских компаний заключили партнерские соглашения с IBM на оказание услуг по мониторингу и реагированию на инциденты ИБ на решениях QRadar.

Платформа QRadar позволяет производить сбор и обработку данных о событиях ИБ из журналов аудита, проводить анализ сетевого трафика и передаваемой информации, строить топологию сети и эмулировать изменения в конфигурациях сетевого оборудования, выявлять уязвимости.

За последнее время IBM представила IBM Watson Advisor for Cyber Security и интеграцию с платформой IBM Resilient, что позволило снизить нагрузку на сотрудников SOC, систематизировать и автоматизировать процессы реагирования на инциденты.

Преимущества IBM QRadar Security Intelligence Platform:

- Единая платформа для создания SOC: включает в себя сканирование уязвимостей и выявление небезопасных конфигураций, сбор и анализ событий информационной безопасности, выявление аномальной сетевой активности,

интеграцию с ИИ IBM Watson, форензикой и процесс реагирования на инциденты в IBM Resilient.

- Гибкая архитектура QRadar Platform позволяет переопределять роль и функции модулей платформы и не ограничивает компании-клиентов жесткими рамками единожды выбранной схемы.

- Большое количество бесплатного контента и базы недоверенных IP от команды IBM X-Force.

- Множество реализованных проектов по всему миру, в том числе и России.

IBM Security QRadar SIEM имеет сертификат ФСТЭК России № 3354, подтверждающий выполнение функций мониторинга результатов регистрации событий безопасности и реагирования на них в соответствии с требованиями Технических условий.

**McAfee Enterprise Security Manager**

McAfee Enterprise Security Manager (ESM) поставляется в качестве ПО, физического и виртуального устройств. Данный SIEM имеет три основных компонента — ESM, Event Receiver и Enterprise Log Manager, вместе как один экземпляр или отдельно в случае крупномасштабных сред. Дополнительные компоненты – это Advanced Correlation Engine, Database Event Monitor, Application Data Monitor и Global Threat Intelligence.

Расширения, внедренные за последнее время, включают возможность динамического заполнения списков наблюдений из дополнительных внутренних или внешних источников, более глубокую двустороннюю интеграцию с Hadoop и поддержку дополнительного доступа к источникам информации об угрозах и управления ими. Интеграция ESM с McAfee Active Response обеспечивает большую видимость конечных точек.

Преимущества McAfee Enterprise Security Manager:

- Enterprise Security Manager большой охват промышленных систем управления (ICS) и устройств диспетчерского управления и сбора данных (SCADA).

- McAfee Data Exchange Layer (DXL) от Intel Security обеспечивает интеграцию с сторонними технологиями без использования API. Этот подход дает возможность для использования ESM в качестве платформы SIEM.

- McAfee Global Threat Intelligence позволяет расширить возможности SIEM-системы, путем добавления источника постоянно обновляемой информации об угрозах. Данное расширение позволяет быстро обнаруживать события, включающие в себя сессии с подозрительными или небезопасными IP-адресами.

McAfee SIEM имеет сертификат ФСТЭК России № 3353, подтверждающий выполнение требований руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) по 4 уровню контроля и Технических условий.

**Splunk Enterprise Security**

Splunk — это платформа со множеством функций, таких как сбор, обработка, анализ и хранение данных. В последние годы считается крайне популярной в США и в Европе. Особенность платформы в том, что она может работать с данными практически из любых источников. Это делает платформу очень универсальной и востребованной во множестве отраслях. SIEM-система имеет название Splunk Enterprise Security.

В состав данной SIEM входят следующие функциональные решения:

- Incident Review — гибкий инструмент обзора и управления инцидентами.

- Investigator — визуальный инструмент выявления Kill Chain.

- Glass Tables — наглядное построение логических схем защищаемых ресурсов со встроенным редактором.

- Security Intelligence — обширный набор преднастроенных интеграций с внешними источниками информации об угрозах, включая интеграцию с Facebook Threat Exchange.

Платформа Splunk разворачивается как на физических, так и на виртуальных серверах. Существует облачная версия. Лицензии делятся на два вида: постоянная лицензия и годовая подписка, стоимость каждый прямо пропорциональна объему обработанных данных в день в гигабайтах.

За последние годы Splunk разработал и интегрировал в свой продукт отдельный модуль – Splunk Machine Learning Toolkit, для расширеннуой аналитики в области прогнозирования, выявления аномалий, кластеризации.

Преимущества Splunk:

- Сбор, поиск, мониторинг и анализ по различным и большим объемам данных, выдавая быстрый результат и высокую интерактивность поисковых запросов на чрезвычайно больших объемах данных.

- Splunk - это Big Data платформа. Обеспечивает комплексный сбор данных, их обработку и анализ. Это повышает универсальность системы.

- Splunk использует технологию MapReduce, для быстрой горизонтальной масштабируемости.

**RuSIEM**

RuSIEM — разработка отечественной компании РУСИЕМ, резидента Сколково. Данная система производит централизованный и распределенный сбор событий с систем любого класса (включая СКУД). Также в данное системе присутствует автоматическое обнаружение инцидентов по правилам корреляции и с применением механизмов ИИ.

Развертывание может производиться как в виртуальной среде на гипервизорах, так и на физическом устройстве. Решение состоит из нескольких модулей и включает в себя:

- RuSIEM — коммерческое решение класса SIEM;

- RvSIEM free — полнофункциональное свободно распространяемое готовое решение класса LM (log management);

- RuSIEM Analytics — модуль аналитики, работающий в режиме реального времени;

- RuSIEM Network Sensor — сетевой сенсор для анализа трафика.

Здесь стоит обратить внимание на модуль RuSIEM Analytics. Данный модуль позволяет:

- выявлять инциденты с помощью ИИ и симптоматической модели;

- обнаруживать инциденты на основе статистического Baseline, управляемого пользовательскими правилами;

- уведомлять о совпадениях по фид-листам;

- автоматически строить активы инфраструктуры по данным из событий и трафика;

- оценивать Standard Compliance и Policy Compliance по техническим контролям, в том числе и по пользовательским стандартам;

- строить сложные аналитические отчеты с большим количеством расчетов.

RuSIEM имеет широкий набор визуализаций данных.

Симптоматическая модель помогает классифицировать и приоритизировать события, находить их без знания текста, строить комплексные отчеты.

Также SIEM-система поддерживает интеграцию с системами СКУД.

Преимущества RuSIEM:

- Применение новый аналитических методов дает возможность обнаружить угрозы без созданных для этого правил корреляции.

- Универсальные коннекторы делают масштабируемость быстрой.

- Гибкие правила корреляции.

- Возможность модульного развертывания допускает использование системы даже с минимальным бюджетом.

- Масштабирование во всех направлениях не имеет ограничения.

- Пользователи могут сами определять критичность событий.

- Распределенная корреляция.

- Встроенный инцидент–менеджмент по itil, включая постановку задач, ограничение видимости инцидентов, эскалацию инцидентов.

**НПО «Эшелон» КОМРАД**

КОМРАД — считается первой отечественной SIEM российской компании НПО «Эшелон».

КОМРАД – это централизованный мониторинг событий информационной безопасности. Данная система позволяет выявлять инциденты ИБ, производить своевременное реагирование, соблюдать требования регуляторов к защите ПДн, к обеспечению безопасности государственных ИС, АС военного назначения, АСУ ТП и т.д.

В 2016 году НПО «Эшелон» выпустило SIEM-систему КОМРАД 2.0. Новое решение стало поддерживать СЗИ отечественных производителей и получило возможность получения событий от любого источника с помощью универсального адаптера. Стоит отметить, что система КОМРАД поддерживает интеграцию с ГосСОПКА, что также является плюсом для отечественных компаний.

Преимущества КОМРАД:

- Высокая производительность.

- Гибкая настройка, подключение любых источников событий ИБ за счет универсального адаптера.

- Неограниченное масштабирование.

- Широкий спектр поддерживаемых отечественных СЗИ (СОВ и МЭ «Рубикон», САЗ «Сканер-ВС», СКУД АССОИ «МАТРИЦА», СЗИ от НСД «Страж NT», ОС Astra Linux, Dallas Lock, Страж NT и др.).

- Полнофункциональная подсистема визуализации.

- Конструктор различных директив корреляции представлен графически. Благодаря этому можно создавать любое количество уровней для правил корреляции и самих правил корреляции.

- Оперативное оповещение на почтовые сервисы и мессенджеры.

- Запросы по ненормализованным данным за счет полнотекстного поиска.

- Управление жизненным циклом инцидента ИБ, создание групп реагирования.

- Контроль соответствия требованиям ГОСТ Р ИСО/МЭК 27001-2006.

- Проверка доступности технических средств.

КОМРАД имеет следующие сертификаты соответствия:

- Минобороны России № 2315, подтверждающий выполнение требований руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) по 2 уровню контроля и выполнение требований по соответствию реальных и декларируемых в документации функциональных возможностей;

- ФСТЭК России № 3498, подтверждающий выполнение требований руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) по 4 уровню контроля и Технических условий при выполнении указаний по эксплуатации, приведенных в формуляре НПЭШ.60010–03 30.

КОМРАД включен в единый реестр российских программ для электронных вычислительных машин и баз данных (приказ Минкомсвязи России от 18.03.2016).

**Positive Technologies MaxPatrol SIEM**

MaxPatrol SIEM — также является отечественным продуктом от российской компании Positive Technologies. MaxPatrol SIEM тесно интегрирован с другими решениями этой компании. Данное решение может быть реализовано программно и программно-аппаратно. Продукт был выпущен на большой рынок в 2015 году.

MaxPatrol SIEM выделяет актив-ориентированный подход, благодаря чему достигается высокий уровень устойчивости работы SIEM-системы к различным изменениям в ИТ-инфраструктуре компаний. Правила корреляции могут спокойно назначаться на динамическую группу активов, состав которой способен постоянно меняться вместе с развитием сети.

Информация пополняется новыми данными об ИТ-инфраструктуре благодаря таким функциям, как поступление новых событий, результаты внутреннего сканирования, анализ сетевого трафика и агентов на конечных точках в сети. За счет этого создается полноценная IT-модель предприятия. Данный функционал позволяет оценивать инциденты с «линком» к конкретным узлам сети, что в свою очередь позволяет снизить число ложных срабатываний.

В MaxPatrol SIEM создан и активно поддерживается механизм передачи в продукт экспертизы исследовательского центра Positive Research, реализованный в модуле базы знаний Positive Technologies Knowledge Base (PT KB). Таким образом, когда в мире был зафиксирован рост атак WannaCry и NotPetya потребители продукта Positive Technologies в тот же день получили весь необходимый набор инструментов для выявления вышеперечисленных атак, а также рекомендации и инструкции по реагированию на полобного рода

инцидент. Используя PT KB удается снизить требования к экспертизе пользователей SIEM-системы.

В 2017 году компания Positive Technologies представила пользователям новую технологию проверки сетевой достижимости в MaxPatrol SIEM. Данная технология применяется для локализации очагов эпидемий и прогнозирования маршрутов атак. Также был разработан алгоритм распознавания активов, из-за чего правила корреляции эффективно работают даже после изменений IP-адресов и иных параметров сетевых узлов. В начале 2017 года были представлены новые собственные модули (Network Sensor и Endpoint Monitor.

MaxPatrol SIEM применяется для создания Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА). Это является большим преимуществом для отечественных компаний и предприятий.

Преимущества MaxPatrol SIEM:

- MaxPatrol SIEM имеет полный функциональный спектор систем управления активами (Asset Management). Это позволяет создавать и автоматически обновлять группы активов по организационным, территориальным, функциональным и любым другим признакам;

- MaxPatrol SIEM постоянно обновляет топологию сети и непрерывно обновляет эту топологию за счет данных от источников и по результатам сканирований;

- MaxPatrol SIEM приоритизирует инциденты в соответствии с важностью актива, что помогает реагировать на самые важные инциденты в первую очередь и тем самым снизить нагрузку на пользователей системы;

- MaxPatrol SIEM предлагает открытый API на языке Python. Благодаря этому можно быстро решить ряд практических задач, связанных с интеграцией.

- Подключение источников производится без дополнительных затрат со стороны заказчиков. А правила нормализации обновляются через базу знаний,

из-за чего события корректно интерпретируются после обновления источников данных;

- Решения Positive Technologies целиком спроектированы в России, с учетом специфики решаемых задач и требований регуляторов. В основе продукта лежит уникальная база знаний, накопленная за годы проведения масштабных тестов на проникновение, расследования сложных инцидентов и экспертного сопровождения знаковых мероприятий, таких как Универсиада в Казани и Олимпийские игры в Сочи.

MaxPatrol SIEM входит в реестр российского ПО №1143, имеет сертификат Минобороны РФ № 3044 и сертификат ФСТЭК России № 3734, подтверждающий выполнение требований руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) по 4 уровню контроля и Технических условий.

### 1.4 Подробный анализ MaxPatrol SIEM.

MaxPatrol SIEM – как было сказано выше, является отечественным продуктом от российской компании Positive Technologies. MaxPatrol SIEM тесно интегрирован с другими решениями этой компании. Компания целиком и полностью специализируется на разработке ПО в области ИБ, осуществляет услуги анализа защищенности и анализа управления в соответствии с требованиями БИ.

Ключевые особенности:

1. MP SIEM с помощью пассивного и активного сборы информации об активах постоянно обновляет и выстраивает модель сетевой инфраструктуры компании. Реализовывается данная функция за счет получения данных на конечных точках, узлах и от агентов для анализа трафика. Благодаря этому защищаемую инфраструктуру можно анализировать графически в режиме

«online» и производить анализ возможной реализации потенциальных атак. Это также позволяет оптимизировать расследование инцидентов ИБ. (реализация данной особенности представлена на рисунке 5);

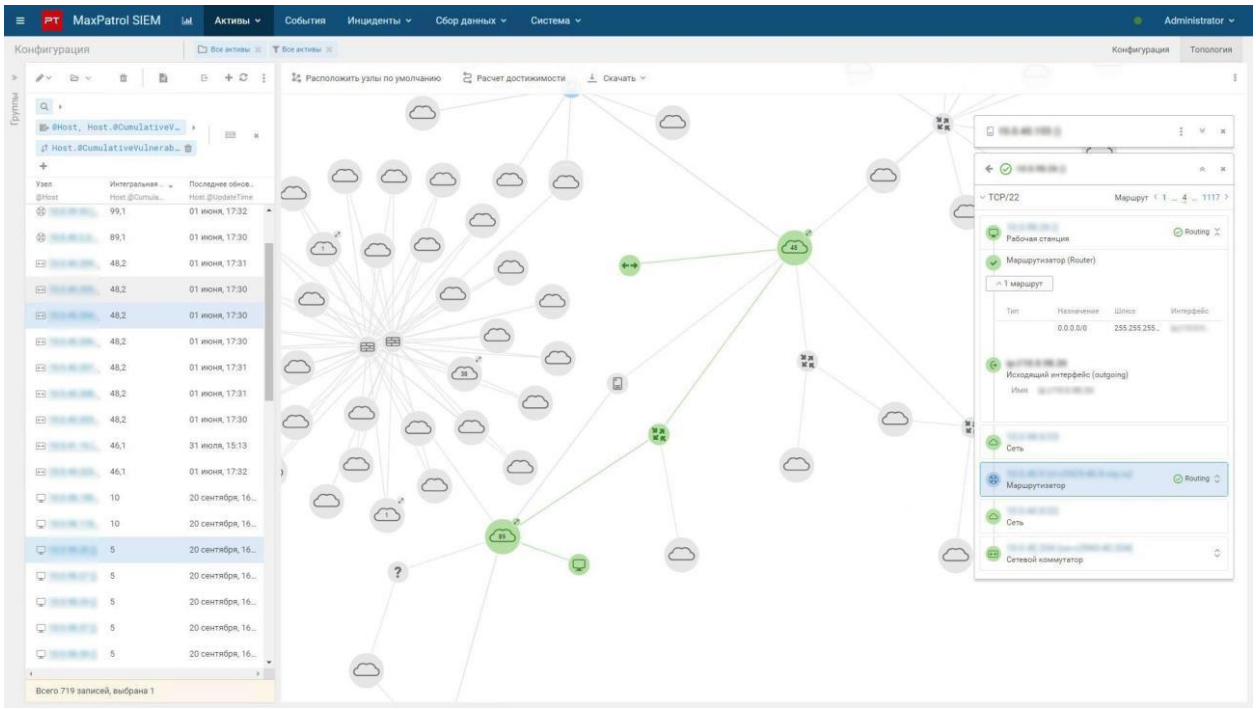



Рисунок 5 – Топология сети

2. Автоматическая сетевая инвентаризация с помощью адресов, сетевых имен хостов, групп активов позволяет производить автоматический контроль изменений в инфраструктуре предприятия;

3. Модуль PT Security Intelligence Portal позволяет производить оценку эффективности ИБ, отслеживать проблемы в информационной безопасности, проводить сводку по инцидентам. Реализация данного модуля представлена на рисунке 6;

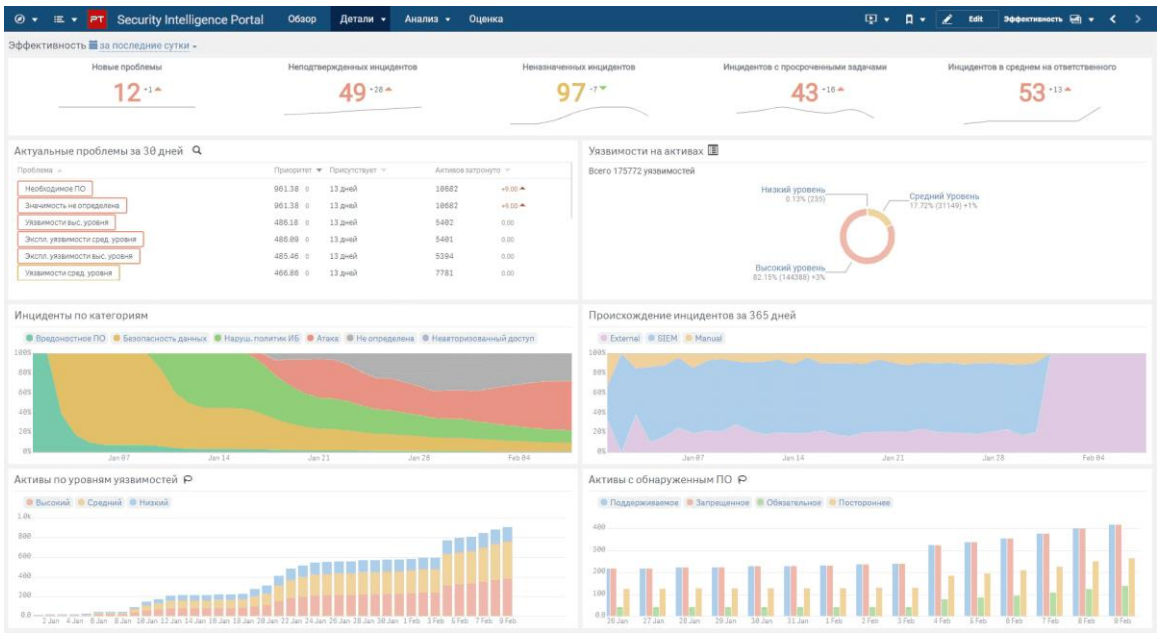



Рисунок 6 – Security Intelligence Portal (оценка эффективности ИБ)

4. Модуль PT Security Intelligence Portal – выполняет функцию оценки уровня защищенности, определяет общий уровень защиты организации с инфраструктурой, разделенной по большой территории, и помогает выявить проблемные участки, определить их причины (Пример представлен на рисунке 7).

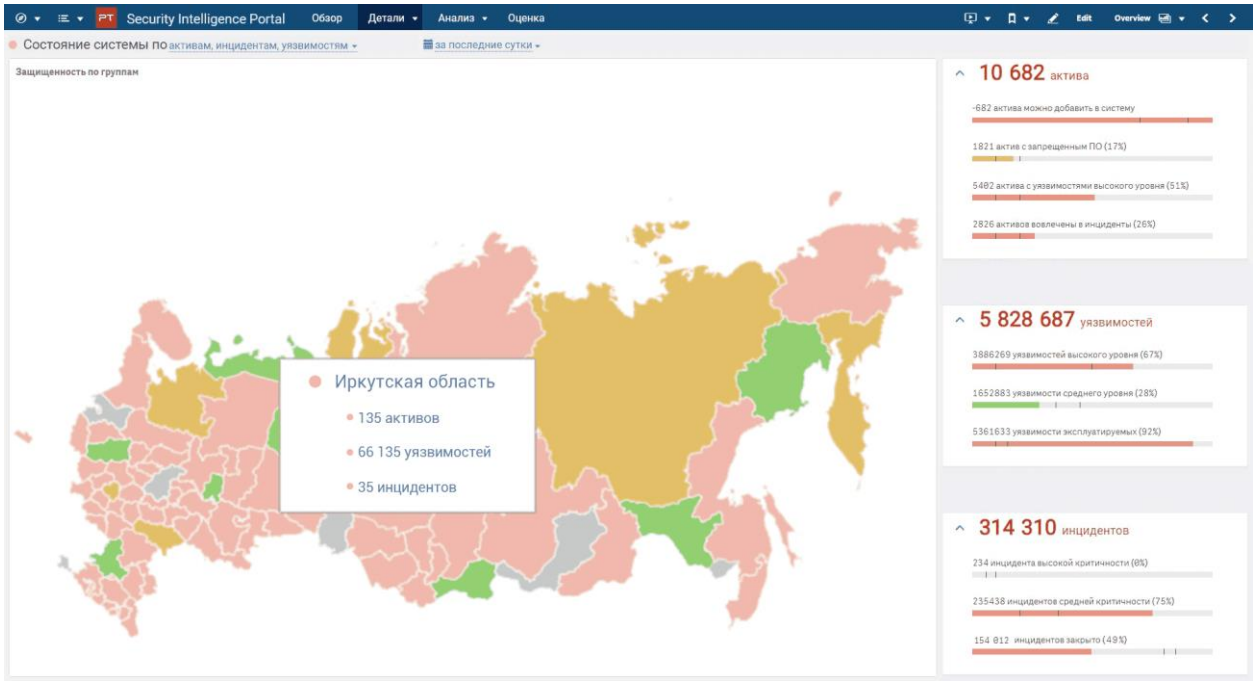



Рисунок 7 – Security Intelligence Portal (оценка уровня защищенности)

5. Общая информация об инцидентах с уязвимостями изображаются в графическом виде (панель индикаторов, диаграммы, общая статистика в виде чисел), указывая на наиболее опасные из инцидентов. (Пример представлен на рисунке 8);

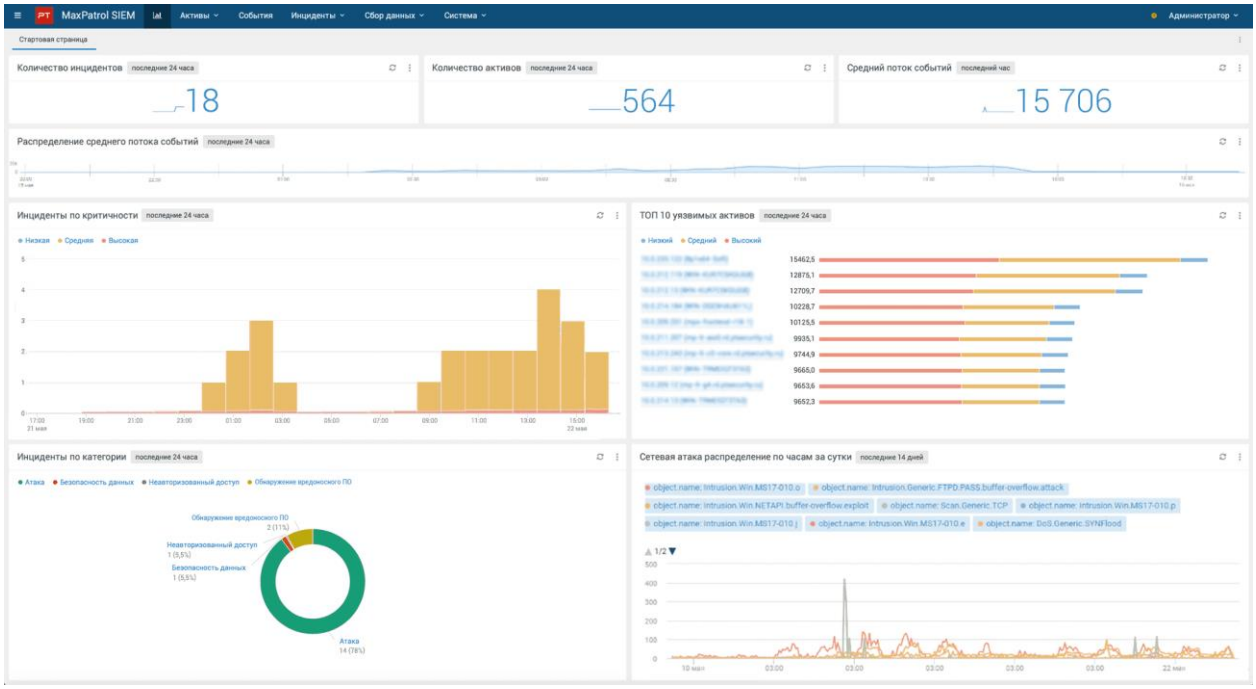



Рисунок 8 – Сводная информация

6. Благодаря встроенной базе знаний PT KB реализуется передача результатов экспертизы Positive Research. Данная особенность позволяет получать информацию о новых атаках и паттернах поведения злоумышленников, с учетом новых найденных уязвимостей, а также позволяет в автоматическом режиме обновлять правила корреляции без внесения исправлений вручную. Так становится возможным своевременное детектирование актуальных типов угроз;

7. Одной из ключевых особенностей для отечественных компаний и предприятий является факт, что MP SIEM – сертифицирован ФСТЭК и Минобороны России, а также входит в реестр отечественного ПО. Сопровождается технической поддержкой в режиме 24/7, документация полностью русифицирована. Общая схема архитектуры PT MaxPatrol SIEM представлена на рисунке 9.

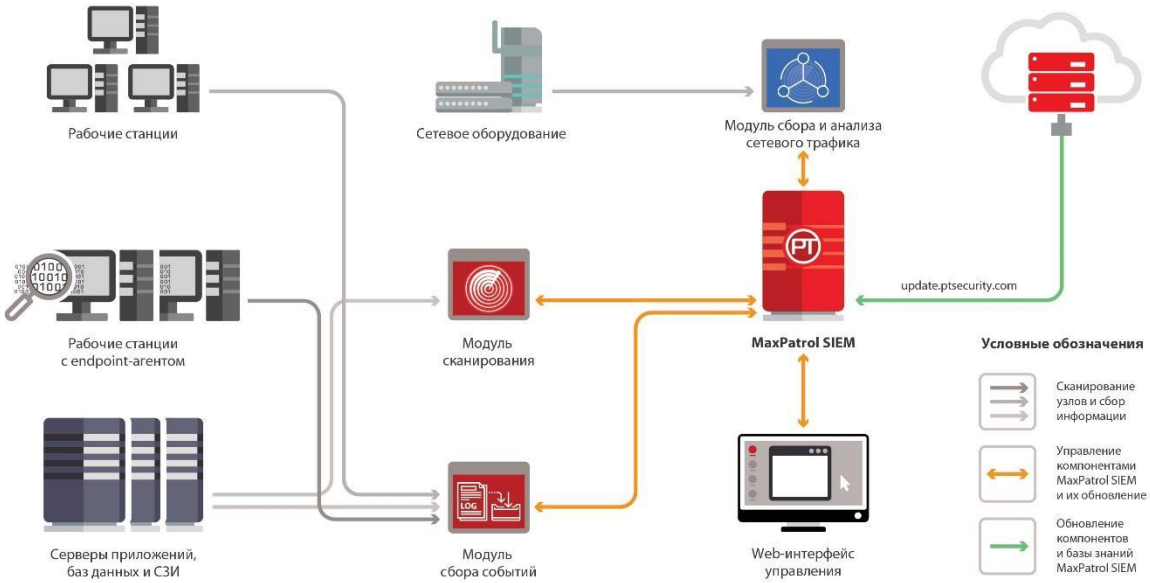



Рисунок 9 – Схема архитектуры PT MaxPatrol SIEM

Актив сети в MaxPatrol – это сканируемый сетевой узел, который определяется по набору параметров:

1. Type – класс ОС (Windows, Unix и т.д.);
2. Hostname – имя хоста, установленное непосредственно на нем;
3. MAC – физический адрес узла;
4. IP – логический адрес узла.

Дополнить информацию об активах сети можно с помощью кастомных (они же пользовательские) полей, такие как назначение узла и данные владельца этого хоста. Подробную информацию можно увидеть в паспорте актива сети, представленный на рисунке 10.

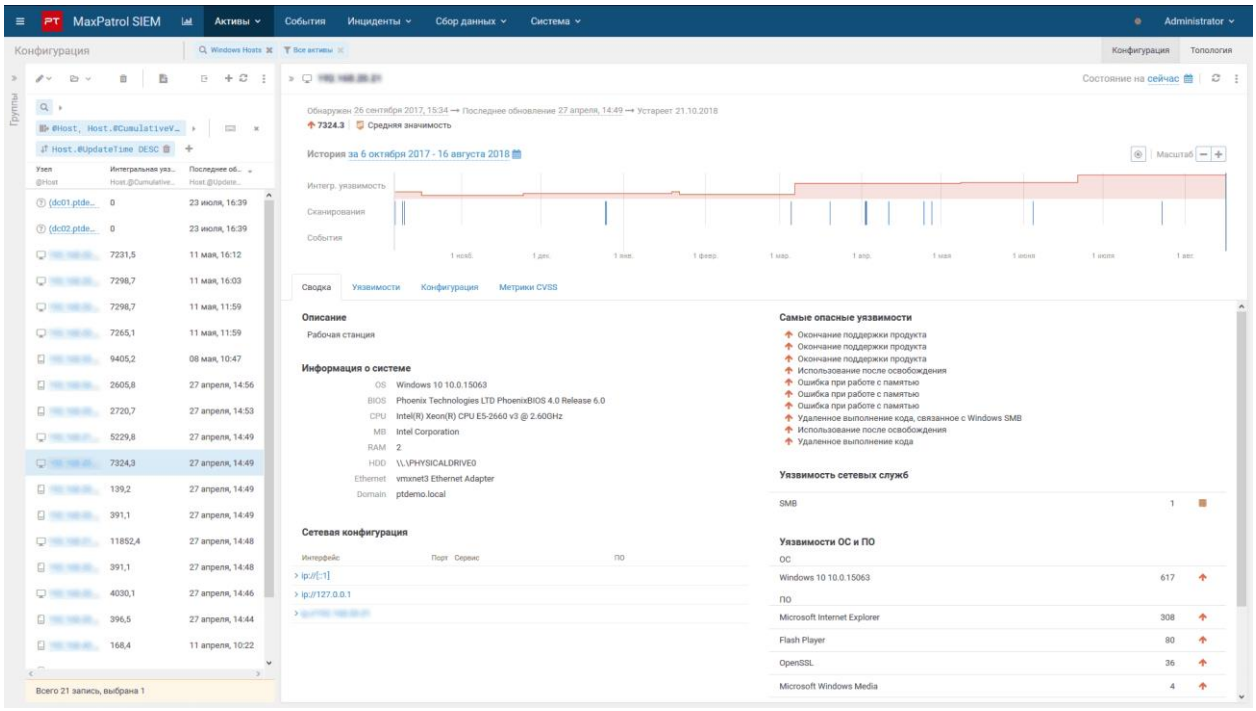



Рисунок 10 – Паспорт актива

Каждую единицу актива сети можно объединить в группы. Цель объединения – разделение активов и рост удобства пользования MaxPatrol SIEM. Группировка отображает в системе структуру предприятия, а также обеспечивает более качественное управление работой SIEM. Благодаря данной функции можно заблаговременно планировать сканирование групп сетевых узлов, быстро выполнять групповые операции, составлять отчеты.

Группировка активов применяется при:

• фильтрации данных для отчетов, графиков, отображения данных;

• привязке событий;

• привязке инцидентов;

• привязке пользователей;

• сборе данных.

Пример с отображением группы активов представлен на рисунке 11.

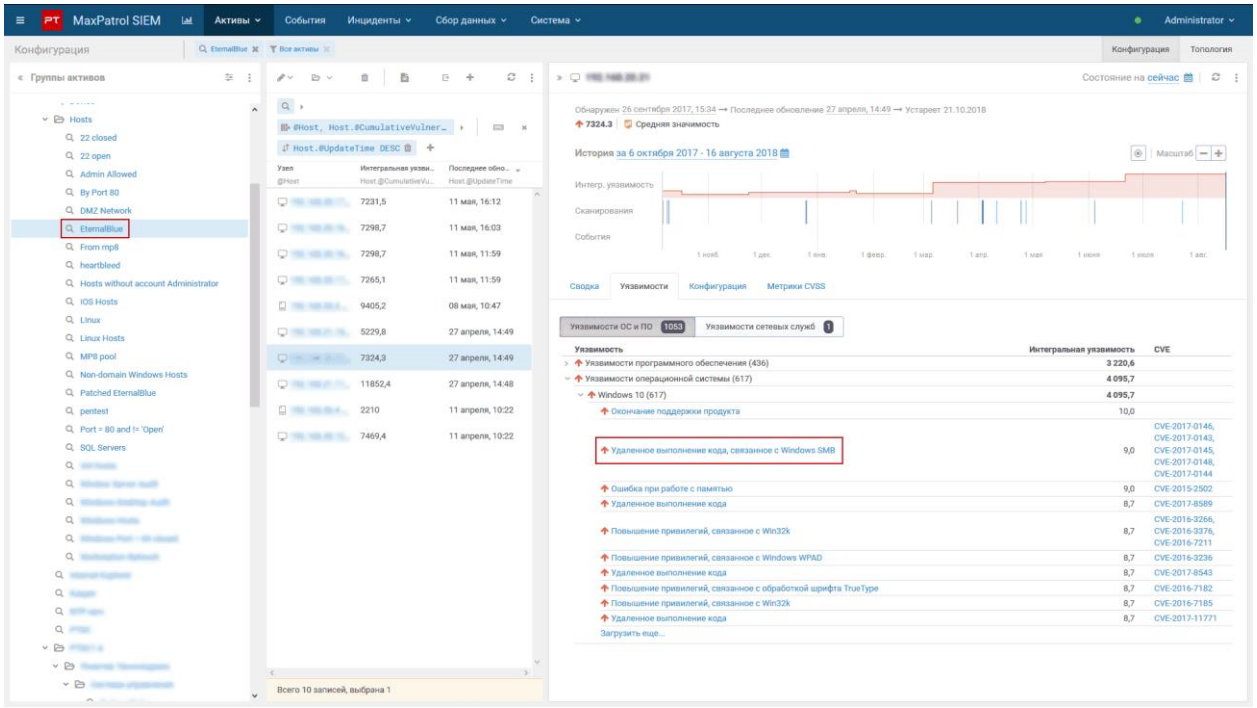



Рисунок 11 – Группа активов

**Жизненный цикл события информационной безопасности в PT MaxPatrol SIEM PT**

MaxPatrol SIEM осуществляет постоянный мониторинг ИБ в IT - инфраструктуре организации, у которой она развернута. Мониторинг производится с помощью сбора событий ИБ с подконтрольных источников и непрерывного слежения за состоянием активов сети. Источником событий ИБ способен быть какой-угодно элемент IT-инфраструктуры, для которого произведена настройка сбора данных и журналирование.

Актив - это объекты модели, являющийся частью IT-инфраструктуры компании. Активы изменяются с помощью получение данных из событий подключенных и настроенных источников, а также аудита IT-инфраструктуры компании.

Для того, чтобы обнаружить событие ИБ используется модель rule-based reasoning. Специалисты центров SOC сами создают различные правила, под специфику предприятий, которые описывают характерные признаки события ИБ. Событие ИБ фиксируется, если в общем потоке данных от источников

обнаруживается последовательность событий, которая была указана в одном из написанных правил, а также в случае модификации состояния актива, описанного в правиле.

Компонентом MP Agent производит сбор событий. MP Agent в зависимости от подключенных модулей способен производить пассивный или активный сбор событий с источников, а также аудит активов сети. От способа хранения событий на конечном источнике («расшаренные» папки, журналы операционных систем, системы управления базами данных и т. п.) подбираются определенные алгоритмы для их сбора — называемые транспортом. Для этого создаются шаблоны настройки — называемые профилем. У собранных событий могут быть отличия в предоставляемом формате (TXT, XML, JSON), а также в форме записи. Для анализа потока информации необходимо привести все собираемые события к единому виду.

Нормализация события — преобразование необработанного события к нормализованному виду с помощью формулы нормализации. Нормализованное событие представляет собой набор полей таксономии, заполненных данными из «сырого» события согласно установленным правилам, указанным в формуле нормализации. Однако поток событий, приходящих от источника часто содержит в себе множество одинаковых событий, отличающихся лишь единицей времени – т.е. одним полем таксономии. Чтобы этого избежать была организована агрегация событий.

Агрегация событий — это процесс отбора событий, работающий по заранее настроенному правилу агрегации. Агрегация объединяет отобранные события в одно агрегированное событие.

Обогащение событий — процесс заполнения полей таксономии обработанных событий согласно правилам обогащения. Поля заполняются данными, в соответствии с правилом обогащения, или данными из табличных списков.

Табличный список — это двумерный массив данных в PT MaxPatrol SIEM, который используется преимущественно в правилах корреляции и обогащения.

Корреляция событий — это процесс обнаружения событий ИБ с помощью анализа потока уже заранее нормализованных событий. При обнаружении одной последовательности событий, соответствующей последовательности в условии заранее настроенных правил корреляции, создается одно корреляционное событие.

Корреляционное событие — событие ИБ, где поля таксономии заполняются информацией о возможном нарушении согласно правилу корреляции.

Инцидент — это такое корреляционное событие, которое напрямую связано с нарушением ИБ. Сведения об инцидентах немедленно направляются пользователю MaxPatrol SIEM.

Табличные списки, о которых было сказано выше, являются важным элементом в PT MaxPatrol SIEM т.к. содержат в себе самую разную дополнительную информацию, а также исключения из правил. Пример, как выглядит табличный список, представлен на рисунке 12.

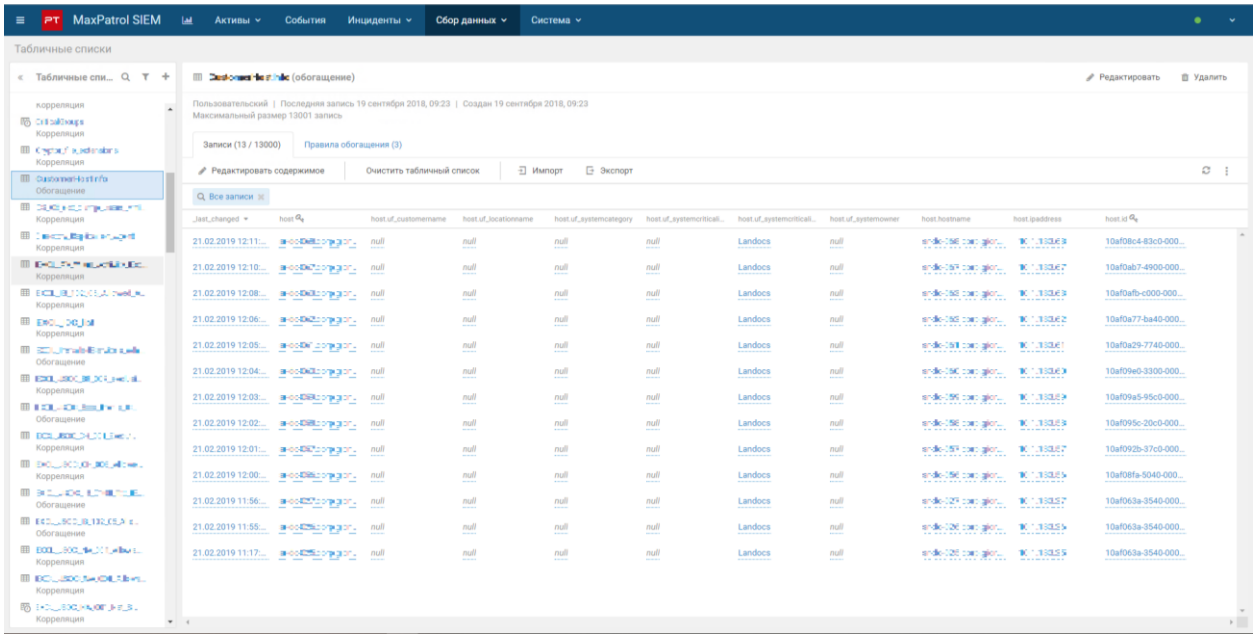



Рисунок 12 – Табличный список

Схема работы программных компонентов в процессе обработки событий представлена на рисунке 13.

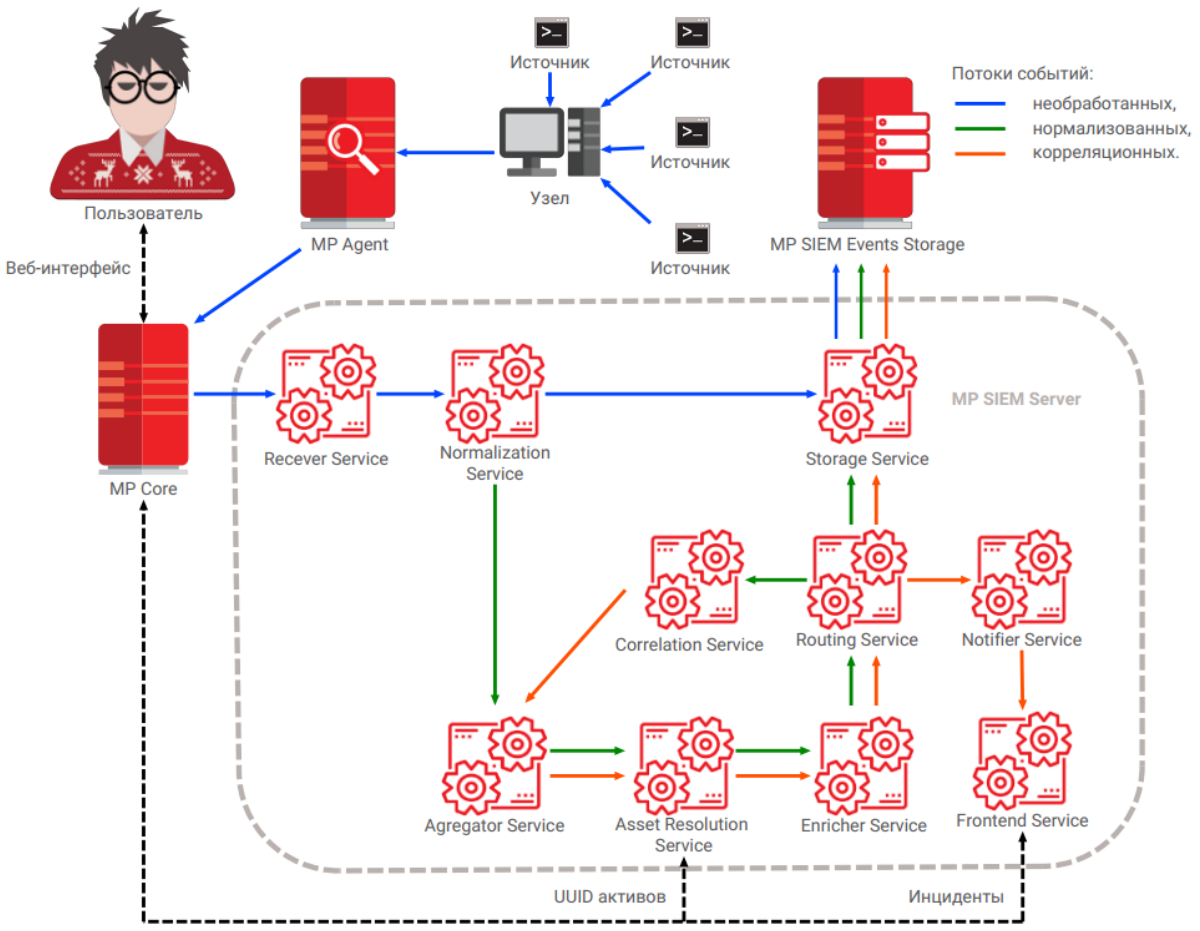



Рисунок 13 – Схема обработки событий в PT MaxPatrol SIEM

Теперь будут описаны компоненты PT MaxPatrol SIEM, принимающие участие в обработке событий.

MP Agent — компонент PT MaxPatrol SIEM, осуществляющий сбор событий с источников, а также проводящий аудит IT-инфраструктуры предприятия. Отправляет пакеты «сырых» событий через MP Core на MP SIEM Server.

MP Core — сервер управления PT MaxPatrol SIEM, который позволяет осуществить через web-интерфейс доступ пользователей. Хранит данные об активах сети.

Receiver Service — модуль MP SIEM Server для приема событий. Обрабатывает и передает необработанные события Normalization Service.

Normalization Service — модуль MP SIEM Server для нормализации необработанных событий по установленным формулам нормализации. Все «сырые» события попадают Storage Service, все обработанные и нормализованные события попадают в — Aggregator Service.

Storage Service — модуль MP SIEM Server для работы с хранилищем событий. Все события сохраняются в БД.

Aggregator Service — модуль MP SIEM Server для анализа потока нормализованных и корреляционных событий на соответствие указанным заранее правилам агрегации. События, подходящие по правилу агрегации, соединяются в единое агрегированное событие. После этого все агрегированные, а также не удовлетворяющие правилам агрегации события передаются Asset Resolution Service.

Asset Resolution Service — модуль MP SIEM Server ищет события, которые могут быть связаны с активами PT MaxPatrol SIEM. Для каждого нормализованного события выполняется запрос к MP Core на наличие в модели endpoints актива, параметры которого соответствуют параметрам источника события. Если актив существует, то в событии указывается UUID актива. События передаются Enricher Service.

Enricher Service — модуль MP SIEM Server для обогащения событий данными в соответствии с правилами обогащения. События от этого модуля передаются далее в Routing Service.

Routing Service — модуль MP SIEM Server для маршрутизации и предварительной обработки событий. Нормализованные и корреляционные события передаются Storage Service. События, удовлетворяющие условиям правил корреляции, передаются далее в Correlation Service. Зарегистрированные корреляционные события передаются далее в Notifier Service.

Correlation Service — модуль MP SIEM Server для регистрации событий ИБ в IT-инфраструктуре компании с помощью проверки всего потока уже нормализованных событий в соответствии с правилами корреляции. После чего зарегистрированные корреляционные события передаются далее в Aggregator Service.

Notifier Service — сервис MP SIEM Server входящий в состав модуля Correlation Service, предназначенный для передачи информации об инцидентах в модуль Frontend Service.

Frontend Service — модуль MP SIEM Server для доступа MP Core к данным сервера через специальный API и ведения журнала функционирования сервера.

## 1.5 Сравнение PT MaxPatrol SIEM, выявление его преимуществ и недостатков относительно всемирно известной SIEM HP ArcSight

В данной работе для сравнения была выбрана зарубежная, всемирно распространенная и некогда эталонная SIEM HP ArcSight. Сравнение PT MaxPatrol SIEM будет проведено с ней. Также стоит отметить, что HP ArcSight – считается одной из самых распространенных SIEM на отечественном рынке.

### 1.5.1 Подключаемые источники

Каждый из разработчиков предоставляет большой набор готовых к использованию smart-коннекторов. Для корректной работы достаточно правильно настроить аудит на самом источнике событий. Иногда необходимо производить самостоятельное написание специального flex-коннектора для сбора событий с нестандартных источников. Каждые из решений содержит данный функционал. В HP ESM ArcSight в настоящий момент времени осуществлен немного лучше**.**

### 1.5.2 Правила

Оба SIEM включают стандартный минимальный набор корреляционных правил от самого производителя для самых типовых ситуаций и инцидентов ИБ. Однако сфера ИБ постоянно и очень быстро изменяется. Сейчас основным

критерием является предоставление возможности написания правил корреляции на стороне пользователя SIEM. Каждое из решений содержит данный функционал. Стоит отметить, что в MaxPatrol SIEM добавлена функция постоянного получения новых данных об атаках и, соответственно, корректировки правил корреляции в автоматическом режиме благодаря взаимодействию с Positive Research.

### 1.5.3 Консоль

Консоль HP ArcSight - это отдельное ПО с названием «ArcSight Console». Если нужно добавить в канал с событиями дополнительные поля таксономии, то ArcSight не перестраивает канал с нуля, подобно MP SIEM, а догружает нужные пользователю поля.

В HP ArcSight SIEM все поля категоризированы и структурированы.

В MaxPatrol SIEM консоль представлена в виде веб-интерфейса. Если нужно добавить в канал с событиями дополнительные поля таксономии, запрос к БД производится заново. В MP Core организована возможность группировки событий в канале с событиями по различным отдельным параметрам, что является ощутимым достоинством и очень удобной функцией при расследовании инцидента ИБ, т.к. можно сфокусировать внимание на самые важные группы событий.

В ArcSight реализовать данный механизм можно только при создании отчёта в форматах Excel или PDF средствами самой SIEM-системы.

### 1.5.4 Запросы к базе данных

Для работы с БД пользователь применяет язык, разработанный самой компанией Positive Technologies, PDQL. К оператору PT MaxPatrol SIEM предъявляются высокие требования к навыкам работы с MP Core и знанию языка PDQL для выполнения запросов к базам данных. Так пользователь отечественной SIEM-системы должен отчетливо понимать поиск каких событий необходим, а также какие переменные для этого необходимо

применить при таком поиске, т.к. он самостоятельно создаёт полноценный запрос к БД.

В HP ArcSight апроса к БД сильно упрощен и представлен в графическом конструкторе.

### 1.5.5 Контент

В HP ArcSight правила корреляции состоят из общих переменных и логических структур, которые коррелятор и база данных «понимают». Предусмотрено создание собственных переменных, если потребуется. Запросы к базе данных и фильтры – это классические SQL команды.

В MP SIEM «контент» строится на языке PDQL, как и сами запросы к базе данных. Чтобы написать правило корреляции специалисту информационной безопасности важно иметь навыки программирования, т.к. правила корреляции создаются с помощью высокоуровнего программного кода.

### 1.5.6 Адаптация к изменениям инфраструктуры

В случае с HP ArcSight SIEM адаптация происходит в большей степени вручную. Возможность автоматического обнаружения и настройки источников ограничена. Существует функционал, первично собирающий события ИБ с конечных источников, которые передают собранные события уже на коннекторы ArcSight. Настройка аудита с необходимых автоматизированных рабочих мест для сбора событий производится путем применения групповых политик. При очередном добавлении автоматизированных рабочих мест в подсеть производится автоподключение его к коннекторам ArcSight.

В ArcSight в качестве активов выступают так называемые Asset'ы. HP ArcSight SIEM актуализирует такие asset’ы следующим образом: запускается сканирование (например, с помощью другого ПО - MaxPatrol) определённой подсети, а уже результаты сканирования загружаются в ArcSight и обновляют имеющиеся или отсутствующие данные о конкретных источниках.

В PT MaxPatrol SIEM процесс добавления и удаления источников событий полностью автоматизирован, т.к. сканнер уже интегрирован, и актуализация данных осуществляется самой системой без дополнительных расходов ресурсов.

### 1.5.7 Ректроспективный поиск событий

В ArcSight поиск событий за продолжительный временной период, например за один месяц от настоящего времени способен достигать несколько дней и недель (зависит от построенного запроса), так как запрос к базе данных, в которой хранятся уже нормализованные события, проходит через множество Java-машин.

В MP SIEM такой поиск работает намного быстрее, т.к. производится запрос к базе данных напрямую. События за один месяц можно получить приблизительно за одну минуту (в случае такого же построенного запроса и при равных условиях в мощностях SIEM-систем).

### 1.5.8 Просмотр «сырых» логов

В MP SIEM есть возможность просмотра необработанного и ненормализованного события из уже нормализованного напрямую в консоли. Такая функция позволяет найти ошибки при обогащении и нормализации поступающих в SIEM от источников событий. В HP ArcSight SIEM в явном виде данные о таких событиях не сохраняются. Такой функционал подлежит дополнительной натсройке.

Данный функционал PT MaxPatrol SIEM представлен на рисунке 14.

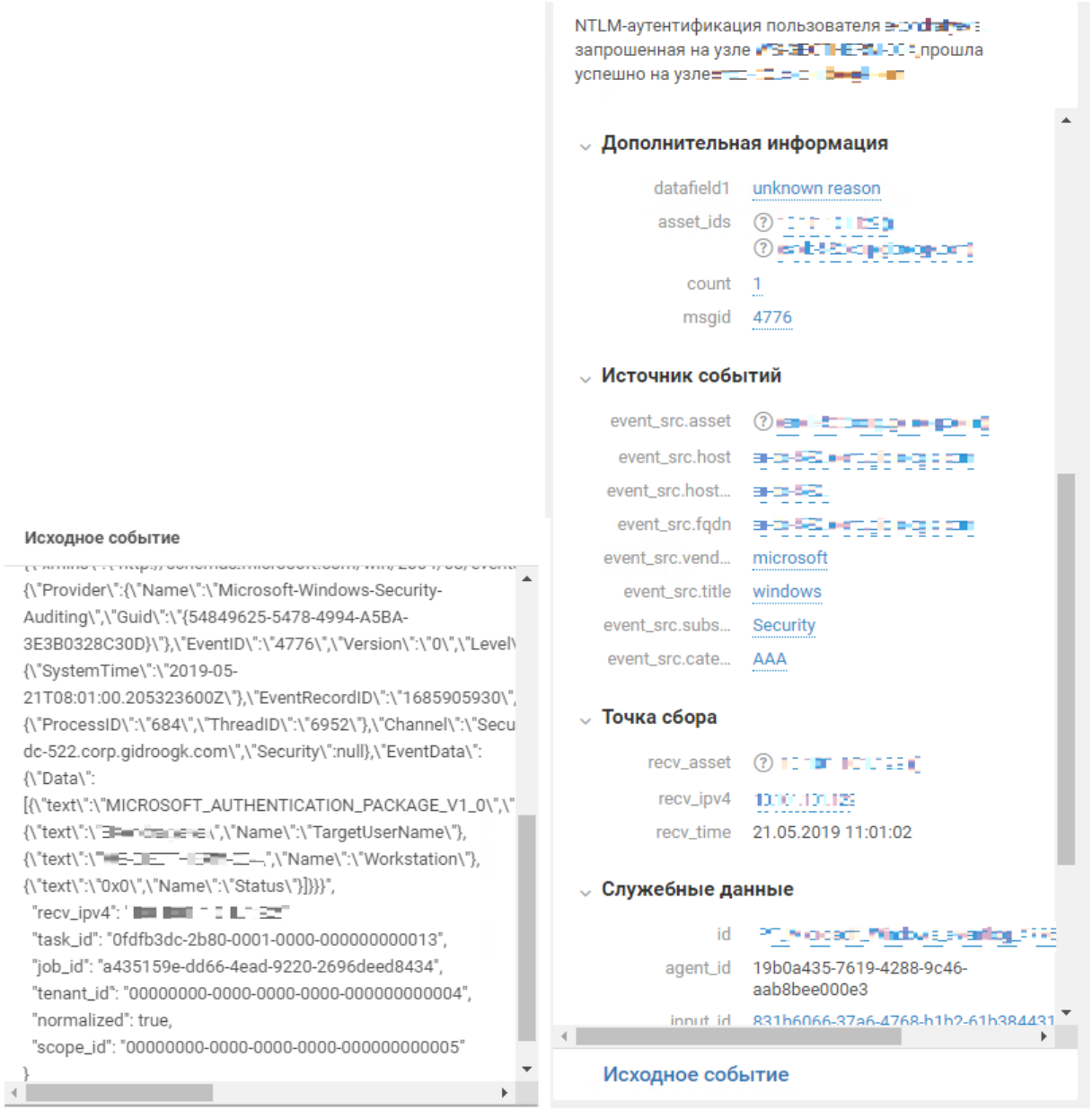



Рисунок 14 – Просмотр исходного события аутентификации Microsoft Windows

Можно сделать вывод, что непрерывно и динамично развивающийся PT MaxPatrol SIEM ничуть не хуже эталонной HP ArcSight SIEM, а по некоторому функционалу превосходит данную систему. Из года в год Positive Technologies продолжает совершенствовать свою продукцию по всем параметрам.

# ГЛАВА 2. РАЗРАБОТКА ПОДСИСТЕМЫ АНАЛИЗА ИНЦИДЕНТОВ В ИНФОРМАЦИОННОЙ СЕТИ ПРЕДПРИЯТИЯ

## 2.1 Требования к разработке

К разработке предъявляются следующие требования:

- Корреляция и обработка событий безопасности:

Корреляция — процесс, который позволяет обнаружить взаимосвязи между событиями, оценить степень важности этих взаимосвязей, определить их приоритеты и составить план действий, соответствующий ситуации. Данное требование лежит в основе разработки.

- Функциональность:

Подсистема должна проводить дополнительный анализ событий, связанных с подбором пароля, и более точно отличать легитимную активность от реальных инцидентов.

- Надежность:

Разработка обязана функционировать исправно на протяжении всей эксплуатации. Ведь сбой в работе подсистемы можем привести к тому, что настоящий инцидент будет определен как ложное срабатывание, что может привести предприятие к серьезным убыткам как материальным, так и репутационным.

- Снижение процента ложных срабатываний;

Одна из основных задач разработанной подсистемы – это снижение процента ложных срабатываний для повышения эффективности работы SIEM-системы.

- Снижение затрат человеко-часов на трудоемкие и рутинные операции.

Вторая из основных задач разработанной подсистемы – снижение затрат сил и времени специалистов информационной безопасности, что позволяет им переключиться на другие важные и критические задачи тем самым повысив эффективность работы отдела информационной безопасности.

## 2.2 Подготовка MP SIEM Server к работе

В этом разделе приводятся инструкции по установке компонента MP SIEM Server на операционную систему Debian и его первоначальной настройке. Команды в интерфейсе терминала Debian необходимо выполнять от имени суперпользователя (root).

### 2.2.1 Подготовка к установке компонента PT UCS на Debian

Перед началом установки необходимо:

1. Обеспечить для сервера с компонентом PT UCS соединение с интернетом.

2. Добавление источников пакетов SaltStack:

wget \

https://repo.saltstack.com/apt/debian/9/amd64/latest/SALTSTACK-GPG-KEY.pub

apt-key add SALTSTACK-GPG-KEY.pub

echo \

'deb http://repo.saltstack.com/apt/debian/9/amd64/lateststretch main'\

>>/etc/apt/sources.list.d/saltstack.list

3. В файл /etc/apt/sources.list добавить строки

deb http://ftp.ru.debian.org/debian/ stretch main contrib non-free

deb-src http://ftp.ru.debian.org/debian/ stretch main contrib non-free

4. Обновить локальный индекс пакетов до последней версии в репозиториях:

apt-get update

### 2.2.2 Установка компонента PT UCS

1. Установка пакета PT UCS:

dpkg -i salt-pt-scm_14.deb

2. Установка необходимых зависимостей:

apt-get -f install

Компонент PT UCS установлен.

### 2.2.3 Настройка компонента PT UCS

1. Открыть порты 443/TCP для исходящих соединений, 4505/TCP и 4506/TCP для входящих соединений.

2. В конфигурационном файле /etc/salt/master.d/pt_scm_sys.conf отключить автоматическое подтверждение Salt Minion на Salt Master:

auto_accept: False

3. Перезапустить службу salt-master:

service salt-master restart

4. На сервере PT UCS выполнить команду:

salt-key –L

5. Авторизовать модули Salt Minion:

salt-key -a <FQDN сервера с модулем Salt Minion>

Компонент PT UCS настроен.

### 2.2.4 Установка компонента PT CP

1. Распаковать архив cybsi-lite-14-debian.tar:

tar -xf cybsi-lite-<Номер версии>-debian.tar –C <Каталог для распаковки архива>

2. Запустить установку пакета:

dpkg -EGi /<Каталог для распаковки архива>/cybsi-lite-<Номер версии>/*.deb

3. Открыть порты 2080/TCP и 2443/TCP для входящих соединений.

Компонент PT CP установлен.

### 2.2.5 Настройка получения данных от репутационного сервиса компании "Лаборатория Касперского"

1. Разместить файл kaspersky.pfx в каталоге /opt/pt/cybsilite/app/.

2. В файле /opt/pt/cybsi-lite/app/config.yml изменить значение параметра kaspersky → enable: enable: true

3. В качестве значения параметра kaspersky → pfx_pass указать пароль от файла kaspersky.pfx.

4. Перезапустить компонент PT CP:

docker-compose -f /opt/pt/cybsi-lite/docker-compose.yml restart cybsi-lite

Получение данных от репутационного сервиса компании "Лаборатория Касперского" настроено.

### 2.2.6 Установка доверенных сертификатов для компонентов MP Core, Knowledge Base и PT MC

При установке компонентов MP Core, Knowledge Base и PT MC для их веб-сайтов автоматически устанавливаются самоподписанные сертификаты, поставляемые в составе дистрибутива.

1. Установка доверенного сертификата для веб-сайтов компонентов MP Core и PT MC:

   mpxcore set -p SSLCertificateThumb <Отпечаток сертификата>

   2. Если вы хотите установить доверенный сертификат для веб-сайта компонента Knowledge Base, выполните команду:

   mpxptkb set -p SSLCertificateThumb <Отпечаток сертификата>

   3. Установка доверенного сертификата для подписи маркера временного доступа:

   ptms set -p TokensCertificateThumb <Отпечаток сертификата>

Доверенные сертификаты для компонентов MP Core, Knowledge Base и PT MC установлены.

## 2.3. Разработка подсистемы анализа инцидентов.

### 2.3.1 Настройка корреляции системы мониторинга

Корреляция в рамках SIEM, это сопоставление информации из разных событий с целью последующего реагирования. На рисунке 20 представлены способы реагирования системы мониторинга на события.

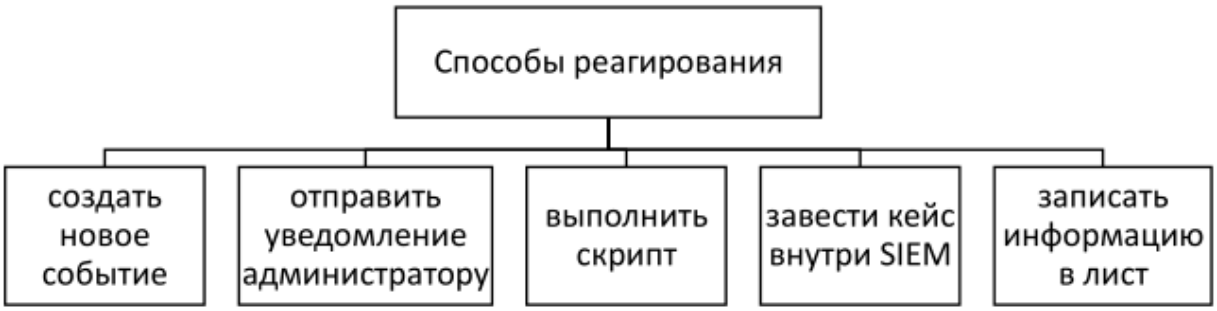



Рисунок 20 - Способы реагирования

Способы реагирования

Главная задача корреляции – это обогащение событий дополнительной информацией. Например, у нас есть IP адреса источников, которые раздал DHCP-сервер нашим клиентам, и мы видим обращения с этого адреса на межсетевом экране к ботнет серверам, но там нет информации о имени пользователя, обращаться на DHCP сервер долго, а нам нужно сразу узнать имя пользователя. Для этого мы собираем лог-файлы с рабочей станции для того, чтобы понять какому пользователю назначен IP адрес, который уличили в попытке подключения к ботнету и уже в скореллированном событии видим полную

информацию о том, кто это сделал. Это пример эффективной корреляции.

Пример неэффективной корреляции – это прежде всего корреляция событий, которые будут часто срабатывать и не будут нести никакой полезной

информации, например, события о блокировке/обнаружении атаки на IPS совместно с событие о разрешительном срабатывании правила на межсетевом экране. Это правило будет неэффективным в силу того, что будет огромное количество спама, при этом как правило IDS/IPS не отличаются точностью своих сигнатур, а значит дают большое количество ложных срабатываний. Основным критерием неэффективной корреляции является спам неинформативным событиями (уведомлениями).

Для проведения корреляции необходима большая база самописных правил корреляции, так как в исходной системе они отсутствуют.

В данной работе мной был изучен язык eXtraction and Processing, разработанный Positive Technologies для написания правил корреляции и обогащения событий данных в процессе обработки событий источников в PT MaxPatrol SIEM.

Создание правила корреляции и логика работы листа началась с того, что мною была подготовлена выборка из 5000 инцидентов, связанных с подбором пароля. Каждый инцидент из выборки содержал в себе причину срабатывания, полное расследование с подробным описанием, а также результат расследования.

Инциденты были разделены на 3 основные группы, основанные на результатах расследования. Полученная статистика изображена на рисунке **.


После получения статистики был составлен список всех ключевых параметров, используемых специалистами информационной безопасности при расследовании.

В данные параметры вошли:

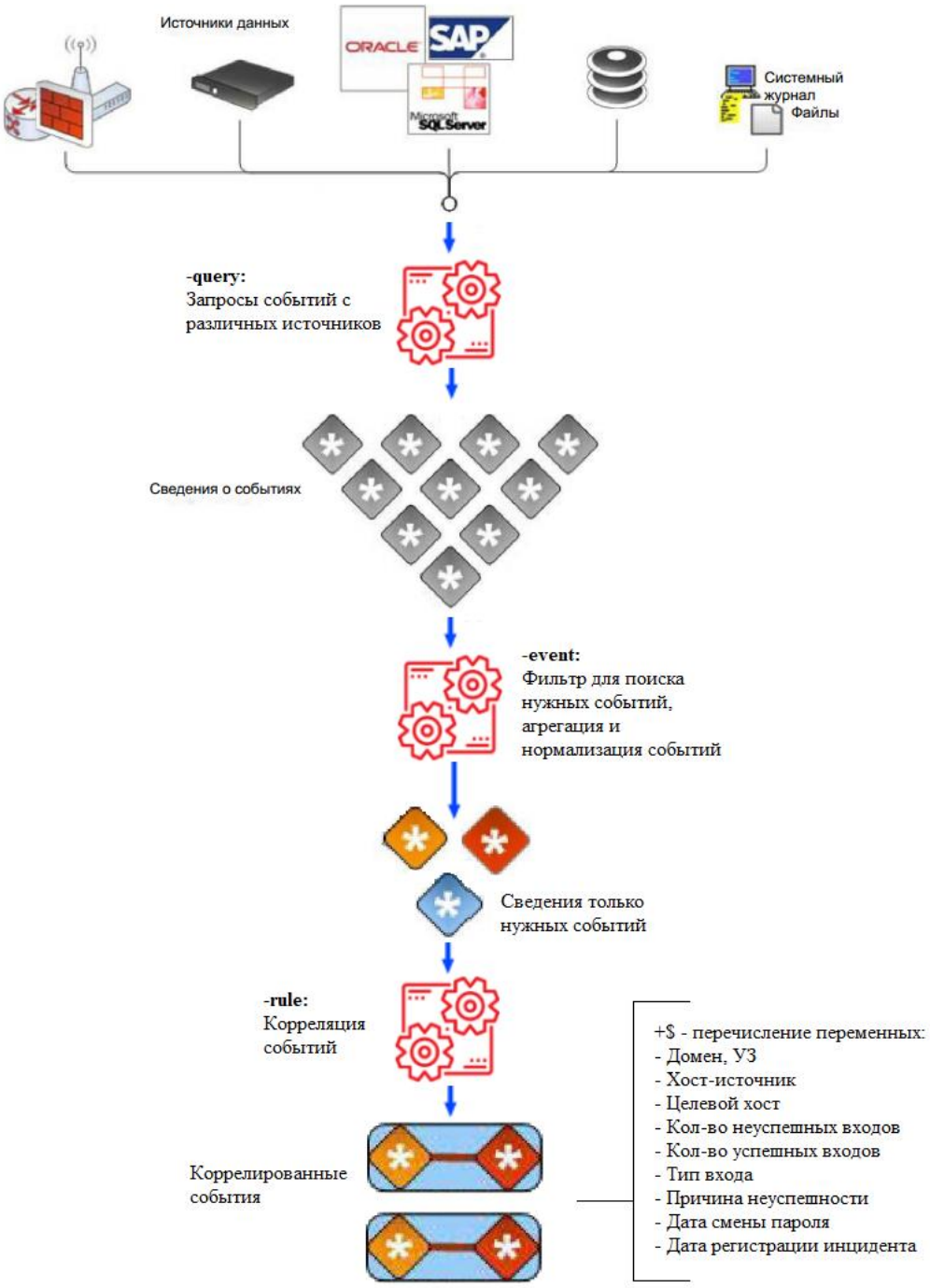
- Домен и учетная запись – позволяет определить тип УЗ (пользовательская, сервисная, системная, административная), а также домен, которому она принадлежит;
- Хост-источник – данные о хосте (IP-адрес, имя хоста, сетевая зона) с которого совершались попытки входа;
- Целевой хост – данные о хосте (IP-адрес, имя хоста, сетевая зона) на который совершались попытки входа;
- Количество неуспешных попыток – изначально сообщают о попытках подбора пароля;

- Количество успешных попыток – позволяют определить успешность атаки;
- Тип входа – позволяет дополнительно охарактеризовать инцидент;
- Причина неуспешности – также позволяет дополнительно охарактеризовать инцидент;
- Дата смены пароля – позволяет отфильтровать случаи, когда попытки подбора сводятся к тому, что у учетной записи истёк срок действия пароля или он был изменён на новый;
- Дата регистрации инцидента – дата, когда инцидент был обнаружен. С этой даты идёт подсчёт времени жизни записи в листе;
- Время жизни записи – дата, когда запись в листе должна быть стёрта или обновлена.

На основе отобранных параметров была сформирована структура правила корреляции, а после разработан алгоритм работы всей подсистемы. Структура и алгоритм представлены на рисунках **, ** и **.

| Rule_Bruteforce |
| --- |
| -query GetStatistic<br>-query GetStatisticDictionaryAttack<br>-query GetUniqueLoginCount<br>-query GetSameSourceSameLoginStat<br>-query GetParameterThresholds<br>-event All_Failure_logon<br>-event All_Success_logon<br>-event All_Password_changed<br>-rule Profile_Failure_Logon<br>-rule Dynamic_List_Bruteforce |
| +$timekey_string<br>+$getCount<br>+$getCountDictionary<br>+$setCountDictionary<br>+$unique_login_count_by_source<br>+$getSameSourceSameLogin<br>+$setSameSourceSameLogin<br>+$firstdetecttime<br>+$getIsAssetCriticalThreshold<br>+$getIsAssetNotCriticalThreshold<br>+$thresholdAssetNotCritical<br>+$reasonfailure<br>+$type_logon<br>+$domen_and_login |

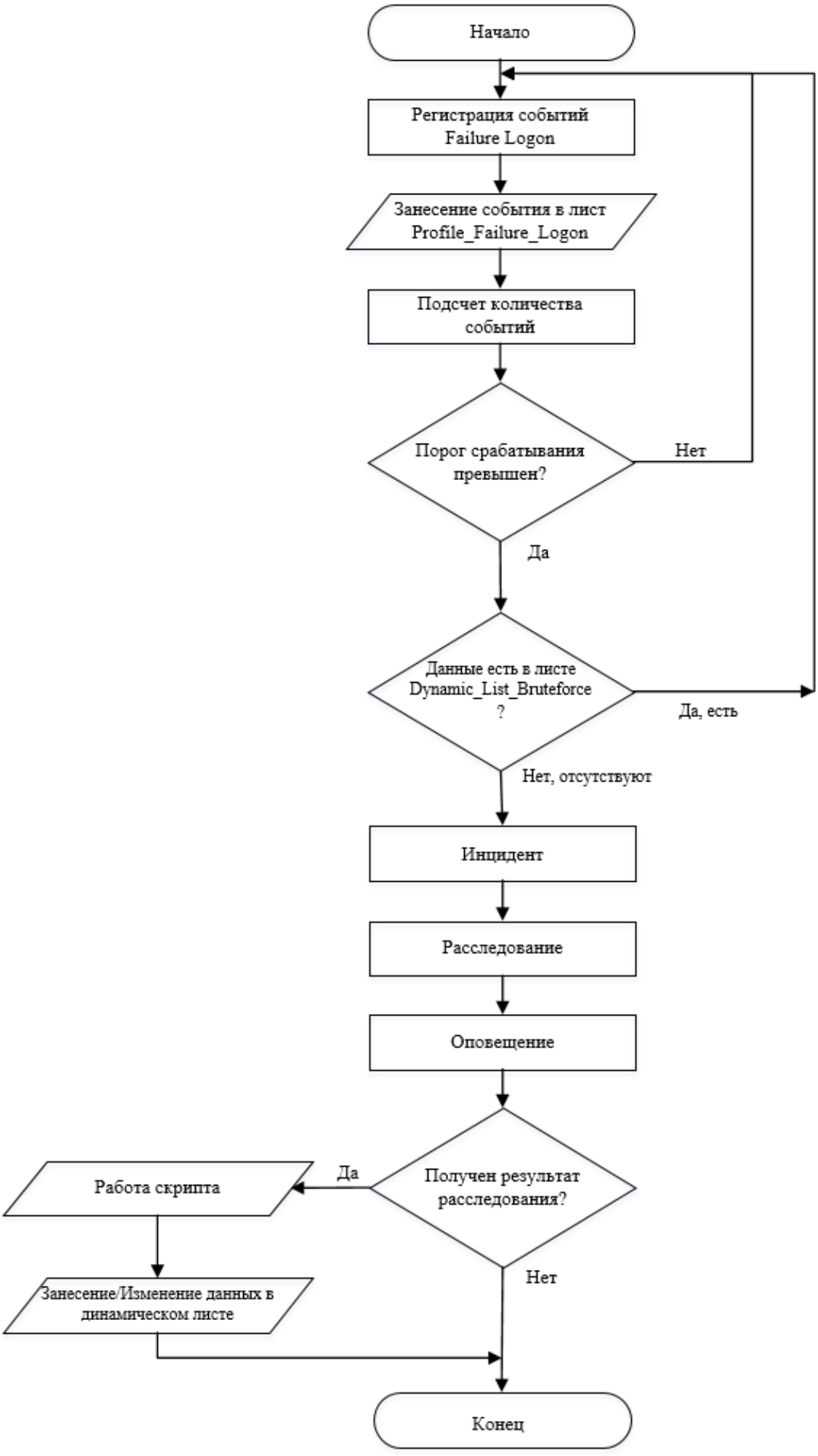
Структура корреляционного правила




Визуализация структуры корреляционного правила

В приложении А приведен разработанный мною программный код для правила корреляции «Rule_Bruteforce» (инцидент «Подбор пароля», его разбор приведен в главе 3 данной работы), основанный на перечисленных

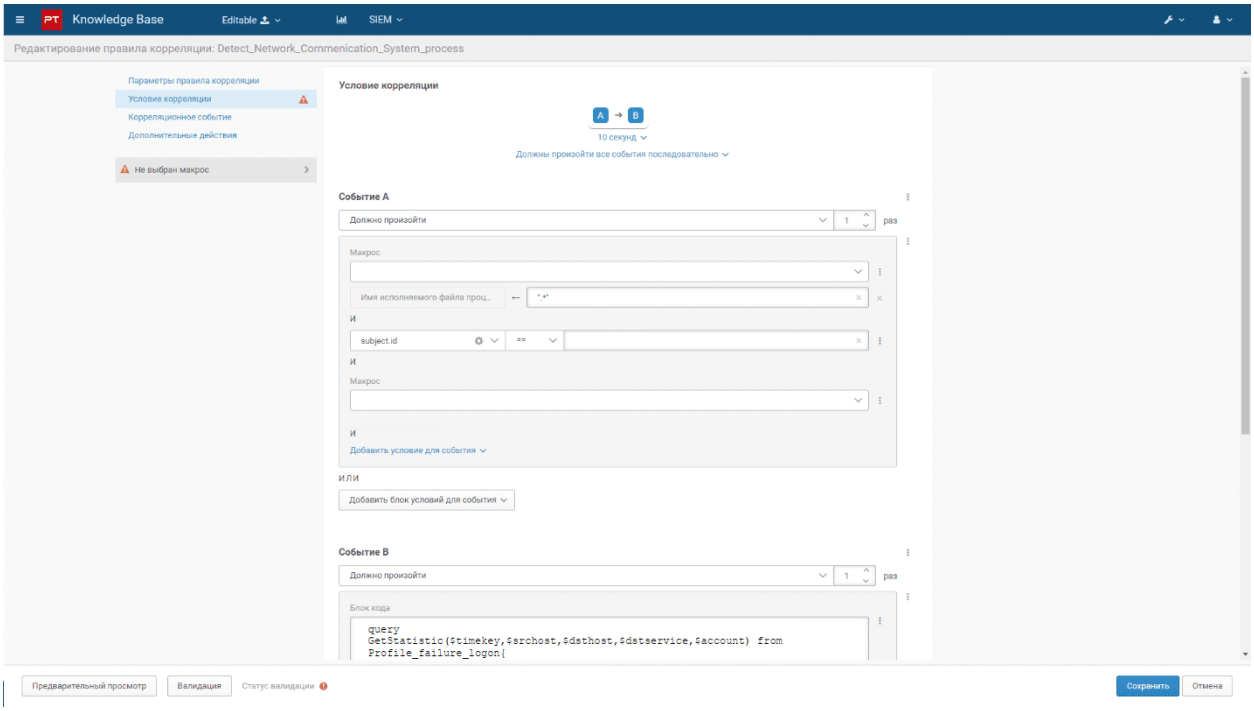
выше параметрах. На рисунке 21 представлен алгоритм работы данного правила.


Начало
Регистрация событий Failure Logon
Занесение события в лист Profile_Failure_Logon
Подсчет количества событий
Порог срабатывания превышен?
Нет
Да
Данные есть в листе Dynamic_List_Bruteforce ?
Да, есть
Нет, отсутствуют
Инцидент
Расследование
Оповещение
Получен результат расследования?
Да
Работа скрипта
Занесение/Изменение данных в динамическом листе
Нет
Конец

В приложении В приводится разработанный мною программный код для получения необходимых данных для заполнения списка после получения результата проведенного расследования.

### 2.3.2 Внедрение подсистемы анализа инцидентов

Код для работы правила корреляции, представленные в приложении А, пишется непосредственно в среде самой SIEM MaxPatrol из-за чего достаточно лишь сохранить написанное правило в директории с остальными самописными правилами корреляции.




Код, представленный в приложении В, помещается в корневую директорию PT MaxPatrol API в виде отдельного файла формата .py и вызывается самой SIEM после срабатывания корреляционного правила и закрытия инцидента на SIEM.


Интеграция скрипта на языке Python

Правило корреляции Rule_Bruteforce позволяет:

1. Обнаружить потенциальную атаку на этапах установки (подбор пароля учетной записи в целях получения контроля над машиной с использованием доставленной на этапе доставки полезной нагрузки), продвижения по сети (компрометация учетной записи администратора уже закрепившимся нарушителем) или действия над объектами (в целях получения доступа к конфиденциальным данным на файловом сервере);

2. Обнаружить попытки получения доступа к консоли средств защиты информации: межсетевых экранов и прокси-серверов. При получении контроля над указанными выше средствами защиты информации злоумышленник может изменить правила фильтрации или трансляции трафика (NAT), что позволит реализовать этап управления. В случае реализации такого сценария взаимодействие с командным центром не будет детектироваться и останавливаться;

3. Детектировать неисправности с компонентами, отвечающими за сетевую аутентификацию, например, компонента NetLogon на контроллере домена. При таком типе неисправности в полях таксономии будет также добавлена причина, указывающая на отключенный компонент.

Разработанный алгоритм фактически самостоятельно выполняет следующие две рекомендации из трех:

1. Проверяет, производилась ли смена пароля от учетной записи, под которой зафиксированы неуспешные попытки аутентификации. Если смена пароля зафиксирована, выяснить, являлась ли смена легитимной;

2. Если в окрестности инцидента имеются успешные попытки аутентификации и все действия подтверждены пользователем, сбрасывает текущие сессии учетной записи, под которой зафиксированы неуспешные попытки;

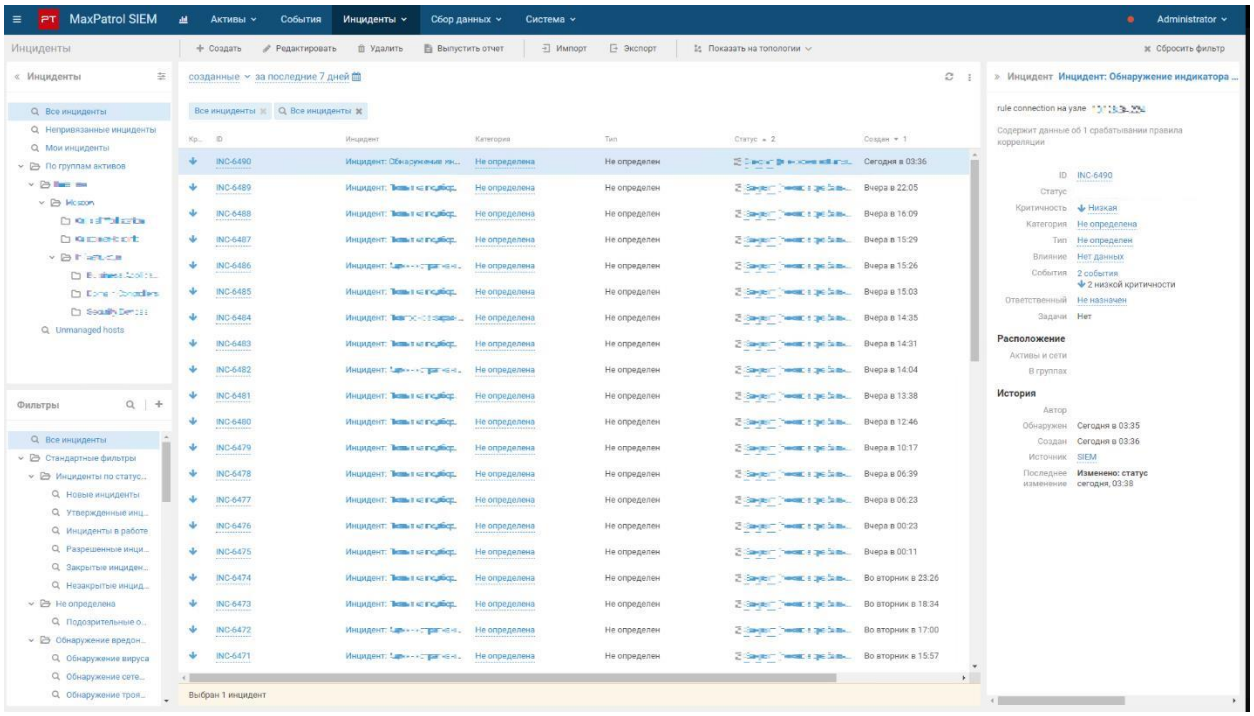
3. Если смена пароля не зафиксирована, и пользователь не подтвердил действия в окрестности инцидента, то необходимо изолировать узел-источник, провести его проверку, а также временно заблокировать учетную запись.

После внедрения подсистемы анализа инцидентов была собрана новая статистика. Полученные данные говорят о том, что эффективность работы SIEM-системы повысилась – задачи, поставленные перед разрабатываемой подсистемой, осуществлены. Статистика после внедрения приведена на рисунке **.

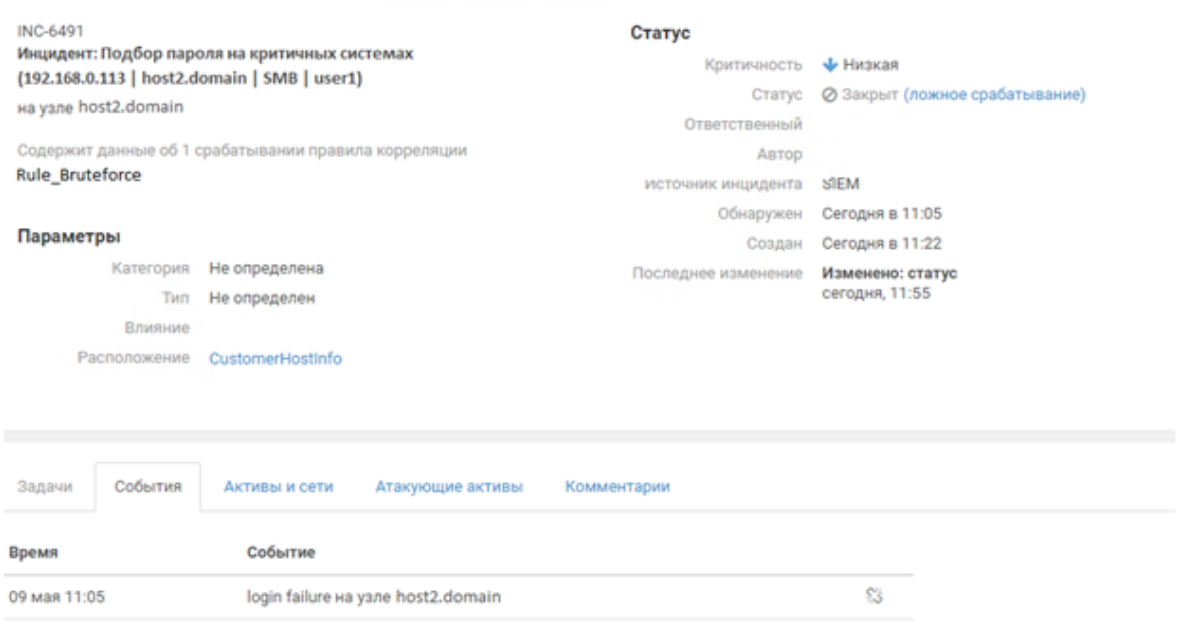
# ГЛАВА 3. РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ ИБ С ПОМОЩЬЮ РАЗРАБОТАННОЙ ПОДСИСТЕМЫ

## 3.1 Разбор инцидента «Подбор пароля» в ручном режиме

Реальные адреса, имена узлов, сценариев, правил, подсетей и активов заменены на вымышленные в целях сохранения коммерческой тайны. Описанию хода расследования данные изменения не помешают.



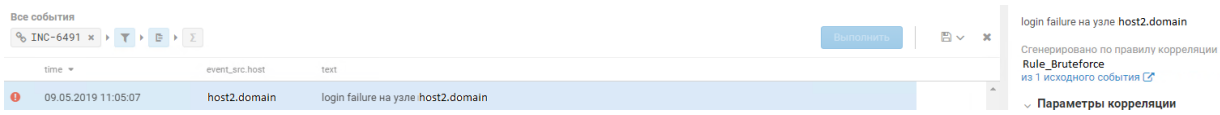

При выборе инцидента будет открыта карточка инцидента, содержащая в себе краткую информацию об инциденте, правило корреляции, по которому был заведен инцидент, сведения об активах, участвующих в инциденте, а также события, попавшие под корреляционное правило. Карточка инцидента представлена на рисунке **.



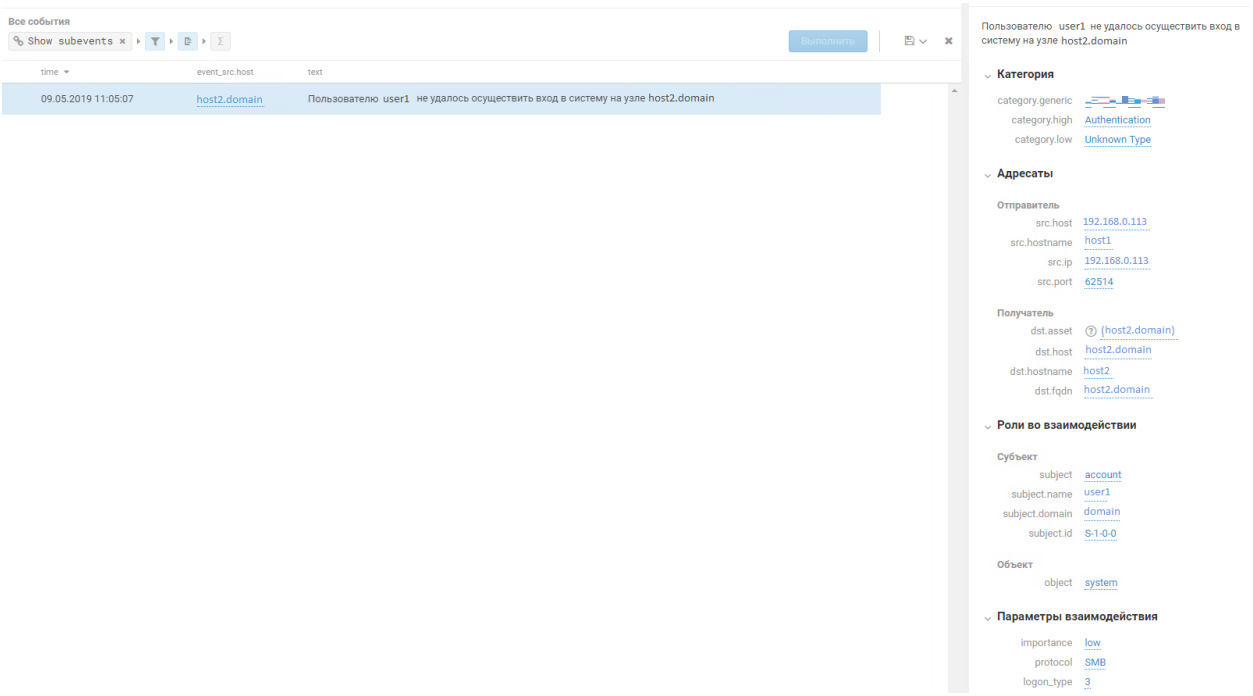

На карточке инцидента видны ключевые поля таксономии, дающие основную информацию об инциденте:

1. Обозначение инцидента в базе: INT-6491;
2. Правило корреляции: Rule_Bruteforce;
3. Корреляционное событие: login failure на узле host2.domain.

Информация о корреляционном событии представлена на рисунке **.




На рисунке ** видно, что событие сгенерировано на узле host2.domain из одного исходного события, информация о котором представлена на рисунке **, по правилу корреляции Rule_Bruteforce. Оно учитывает количество неуспешных попыток аутентификации в системе под одной учетной записью за 10 минут, порог срабатывания – 15 попыток. В данном случае зафиксировано 113 попыток. Исходное событие – пятнадцатая неуспешная попытка аутентификации.




На рисунке 26 указаны поля таксономии, характеризующие исходное событие инцидента:

1. Текст события: Пользователю user1 не удалось осуществить вход в систему на узле host2.domain (источник события – host2.domain);

2. Отправитель (источник) взаимодействия: host1 – 192.168.0.113;

3. Получатель (цель) взаимодействия: host2.domain;

4. Субъект (учетная запись, под которой производятся попытки аутентификации): domain\user1;

5. Тип входа: 3 (SMB).

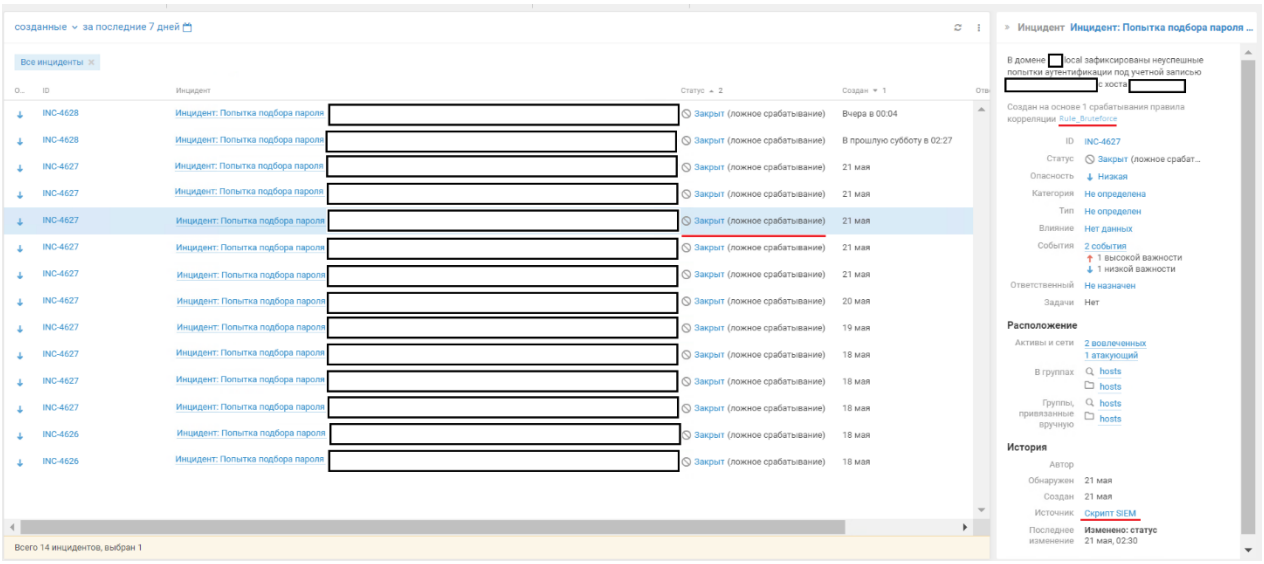
Таким образом, характеристика инцидента выглядит следующим образом: Пользователь domain\user1 осуществил 113 неуспешных попыток аутентификации (тип входа: 3, SMB) на узле host2.domain с узла host1 – 192.168.0.113.

Результат расследования показал, что попытки связаны с работой службы, которая пыталась работать, используя старый пароль. Пароль был сменён за несколько часов до инцидента. Специалист по защите информации потратил 30 минут на расследование данного «инцидента».

### 3.2 Разбор инцидента «Подбор пароля» после внедрения подсистемы.

После расследования данные об инциденте были занесены подсистемой в динамический лист.

Результат работы подсистемы представлен на рисунке **.




Инцидент был сгенерирован и сразу же автоматически закрыт как ложное срабатывание на основе измененного правила Rule_Bruteforce с помощью «Скрипт SIEM».

Инцидент мог и не генерироваться совсем, однако функция генерации инцидента была сохранена с целью редактирования и отладки кода и проведения ретроспективных проверок.

Как результат, специалисту по информационной безопасности не пришлось откладывать какую-либо активную задачу и тратить свои силы и время на расследование ложного инцидента.

# 5. ЭКОНОМИЧЕСКОЕ ОБОСНОВАНИЕ

## 5.1 Маркетинговый анализ

В процессе…

## 5.2 Расчеты затрат на создание продукта

### 5.2.1 Расходы по зарплате исполнителям

$$З_{з/п} = З_{осн} * (1 + К_{доп}) * (1 + К_{с/ф}) \quad (5.1)$$

$З_{осн}$ – основана зарплата работников, определяемая в зависимости от трудоемкости этапов разработки, квалификации и уровня оплаты

$$З_{осн} = \sum_{j=1}^{m} \sum_{i=1}^{n} З_{ijчас} t_{ij} \quad (5.2)$$

m – кол-во этапов разработки;

n – кол-во разработчиков, принимающих участие в процессе разработки;

$З_{ijчас}$ – часовая зарплата специалиста;

$T_{ij}$ – затраты времени в часах i-го разработчика на j-ом этапе;

m=2;

n=2;

$З_{1час}$ = 150 руб/час;

$З_{2час}$ = 200 руб/час;

$T_{11}$ = 30 часов;

$T_{12}$ = 50 часов;

$T_{21}$ = 0 часов;

$T_{22}$ = 40 часов;

Все виды работ выполняются 2 людьми в течении тридцати рабочих дней по 4 часа в день, в которые входят 2 этапа разработки.

Коэффициенты, учитывающие дополнительную заработную плату и отчисления в социальные фонды:

$К_{доп} = 0{,}08;$

$К_{с/ф} = 0{,}3;$

Получаем следующие значения:

$З_{осн} = 40*150+40*150+200*40 = 20000\,р.$

$З_{з/п} = 20000*(1+0{,}08)*(1+0{,}3) = 28080\,р.$

### 5.2.2 Расходы по арендной плате за помещение

Проектирование, разработка осуществляется в офисном помещении площадью $17\,м^2$.

Расчет затрат на арендную плату вычисляется по следующей формуле:

$$З_{ар} = Ц_{ар} S_{пл} T_{раз} / 365 \qquad (5.3)$$

$Ц_{ар}$ - арендная плата за 1 кв. м. площади в год ($Ц_{ар}$ - 7000р/кв. м.);

$S_{пл}$ – арендуемая площадь кв. м. ($S_{пл}$ – 30 $м^2$);

$T_{раз}$ – время на разработку в календарных днях ($T_{раз}$ – 30 дней);

Помещение арендуется на две недели, его стоимость составит:

$З_{ар} = 7000*(2*6+5)*30/365 = 9780$ р.

### 5.2.3 Размер необходимой арендуемой площади

$$S_{пл} = \sum_{j=1}^{m} n_j q_{чел} + 5 \qquad (5.4)$$

$q_{чел}$ – 6 кв. м. (норма площади на 1 человека)

Так как в работе над проектом будет задействовано 2 человека, необходимая площадь составит 1 2 м$^2$.

Площадь арендованного помещения составляет $S_{пл} = 2*6+5 = 17$ м$^2$, что соответствует требованиям.

### 5.2.4 Расходы на освещение и отопление

$$З_{эн} = P * t_{дн} * T_{разр.раб} * W_э + S_{пл}(T_{разр} / 365) W_{тепл} \quad (5.5)$$

Суммарная мощность энергоприемников в помещении 0,5 кВт.

Продолжительность работы энергоприемников в течении дня $t_{дн}$ =8 часов. Продолжительность разработки в рабочих днях $T_{разр.раб}$ = 30 дней.

Тарифы на электроэнергию и тепловую энергию:

$W_э$ = 5 р. за 1 квт/ч

$W_{тепл}$ = 68р. за кв.м.

Таким образом рассчитаем $З_{эн}$ =600+167= 767 р.

### 5.2.5 Расходы на оплату машинного времени

$$З_{маш} = \sum_{j=1}^{nм} T_{jээ} * Ц_{маш} \quad (5.6)$$

Стоимость одного машино-часа работы составит 150 р.

Рассчитаем оплату машинного времени при продолжительности 2 этапов суммарно в 120 часов:

$З_{маш} = 150*120 = 18000$ р.

### 5.2.6 Косвенные расходы организации разработчика

$$З_{косв} = З_{осн} * К_{косв} \quad (5.7)$$

$К_{косв}$ принимаем за 1.3.

Рассчитаем:

$З_{косв} = 20000 * 1.3 = 26000$ р.

Таким образом затраты  на разработку составляют:

28847 + 9780 + 767 + 18000 + 26000 = 83394 р.

## 5.3. Расчёт экономической эффективности разрабатываемой подсистемы.

Целью этого раздела является определение показателей экономической эффективности затрат на приобретение новых видов информационно - измерительной техники, аппаратных средств защиты информации, средств автоматизации и регулирования производственных процессов, программных продуктов и других разработок. Эти затраты для пользователя носят характер инвестиций – долговременных вложений капитала с целью получения прибыли. Принятие решения инвестиционного характера, как и другой вид управленческой деятельности, основывается на использовании различных методов, позволяющих обоснованно принимать решения в области инвестиционной политики.

Поскольку инвестирование, это долговременный процесс, чаще всего для определения экономической эффективности инвестиций используются методы, основанные на дисконтированных оценках. Дисконтирование применяется дляобеспечения сопоставимости затрат и будущих доходов.

Предварительно необходимо провести обоснование пороговой процентной ставки (r), на основе которой рассчитываются коэффициенты дисконтирования К:

$$K=1/(1+r)^t \quad (5.8)$$

Устанавливаем пороговую ставку в 15% процентов.

r = 15%

t=3

$K_1$=0,8696 $K_2$=0,7561 $K_3$=0,6575

### 5.3.1 Затраты на текущий ремонт и межремонтное обслуживание

$$Р_т = S_{эл} + З_р \quad (5.9)$$

$S_{эл}$ – стоимость заменяемых в процессе ремонта элементов

$З_р$ – зарплата ремонтных рабочих

$$S_{эл} = \sum_{i=1}^{1} Т_{год} S_i n_i \lambda_i \quad (5.10)$$

$Т_{год}$ – годовой фонд времени работы проектируемого объекта

$S_i$ – стоимость 1шт i-го элемента

$n_i$ – количество элементов каждого i-го наименования

$\lambda_i$ – интенсивность отказов i-го элемента, 1/ч

i – число наименований элементов в схеме

$$З_р = К_с Т_{год} \sum_{i=1}^{1} n_i \lambda_i \, t_р r_{ср} \quad (5.11)$$

$К_с$ – коэффициент, учитывающий премию, дополнительную зарплату и отчисления в социальные фонды

$t_р$ – среднее время в часах, затрачиваемое на устранение одного заказа на ремонт или замену невосстанавливаемых элементов

$r_{ср}$ – средняя зарплата ремонтных рабочих в час.

На основе формул определим затраты на текущий ремонт и межремонтное обслуживание:

$P_T$ = 5570+3500 = 9070 руб

### 5.3.2 Амортизационные отчисления

$$A = П * На /100 \quad (5.12)$$

При норме амортизационных отчислений 33% и первоначальной стоимости техники и работы в рублях составит $A$ = 20000∗0,33 = 6600 р.

### 5.3.3 Эксплуатационные расходы

$$Э = З + Р_т + М + А \quad (5.13)$$

Используя результаты проведенных ранее расчетов, найдем сумму эксплуатационных расходов:

Э = 20000 + 9070 + 11013 + 6600 = 46683 р.

### 5.3.4 Расчет дисконтированной стоимости

Формула чистой дисконтированной стоимости:

$$ЧДС = \sum_{i=0}^{t} ЧДП_i/(1+r)^t) – И \quad (5.14)$$

$$ЧДП = \Delta Э_i \quad (5.15)$$

$$\Delta Э_i = (Э_с - \Delta Э_н) \quad (5.16)$$

Значение $Э_С$ = 95000 р./год, в связи с дополнительными расходами на постоянный мониторинг за состоянием системы обнаружения и предотвращения вторжения.

Значение $Э_Н$ = 46683 р./год

Рассчитаем по имеющимся данным величину $\Delta Э_i$ = 95000 – 46683 = 48317р.

Тогда соответственно *ЧДП* = 48317 р.

Пороговая ставка r составляет 15%

Рассчитаем *ЧДС:*

*ЧДС* = (48317*0,8696 + 48317*0,7561 + 48317*0,6575) – 83394 = 26922 р.

При R1 = 30% чистая дисконтированная стоимость равна:

*ЧДС* (48317*0,8 + 48317*0,64 + 48317*0,512) – 83394 = 4363р.

При R2 = 35% чистая дисконтированная стоимость равна:

*ЧДС*- = (48317*0,7692 + 48317*0,5917 + 48317*0,4552) – 83394 = -1459р.

### 5.3.5 Расчет внутренней нормы доходности

R1 = 30% = 0.3

R2 = 35% = 0.35

Определим *ВНД* по следующей формуле:

$$ВНД = r1 + (ЧДС_{+} * (r_2 - r_1)) / (ЧДС_{+} + | ЧДС_{-} |) \quad (5.17)$$

ВНД составит =0.3+(4363 *(0.35-0.3))/ (4363 + 1459) = 33,7%

Полученное ВНД > r (15%) – затраты оправданы.

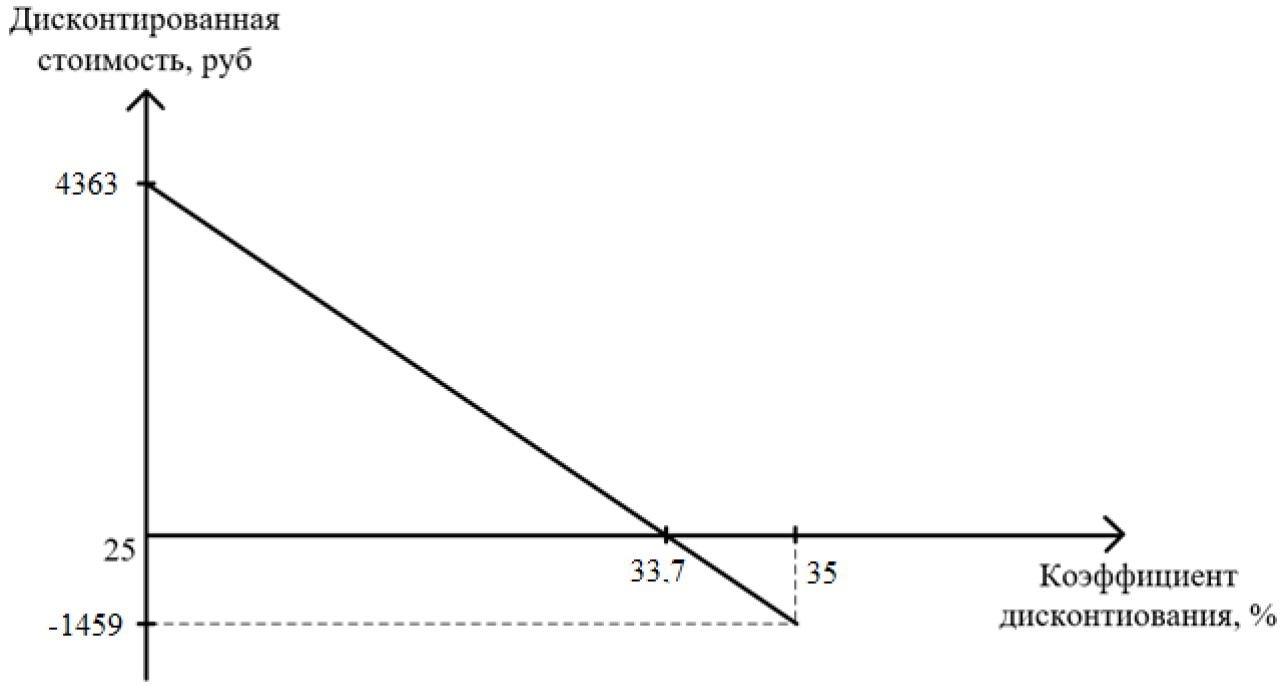



Рисунок 5.1 – График ВНД

5.3.6 Расчет срока полного возмещения инвестиций

$$СВПИ = n + (И - \sum_{i=1}^{n} ЧДС_i) / ЧДС_{n+1} \quad (5.18)$$

При *И* = 83394 р. СВПИ = 2 + (83394 – 72689)/26922 = 2,3976 = 2,4 года.

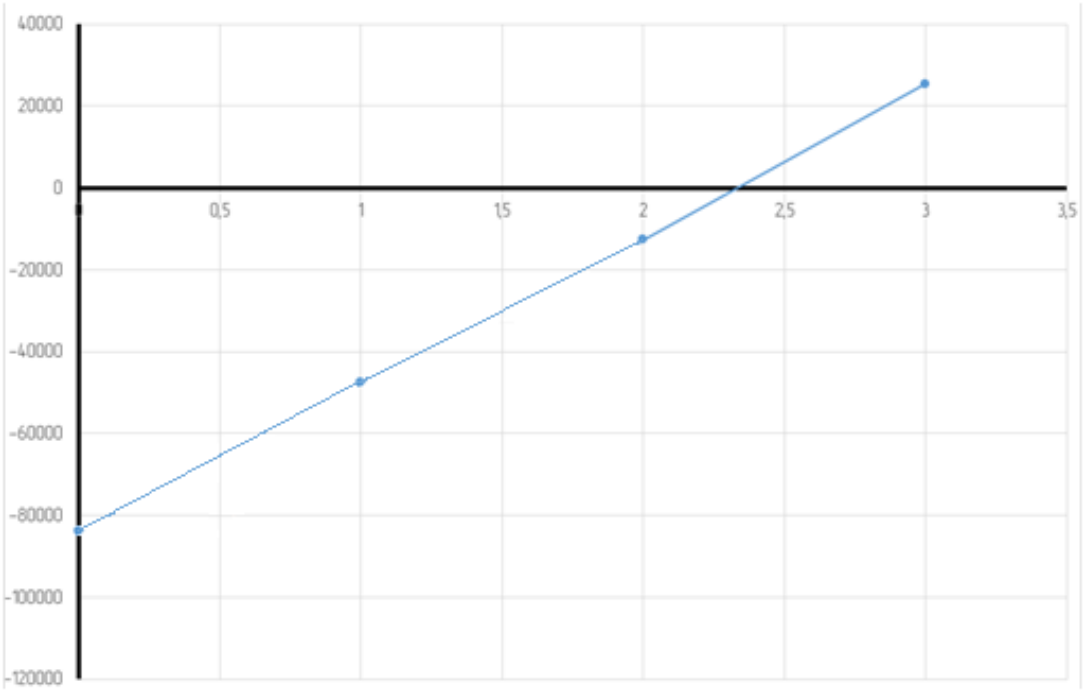



Рисунок 5.2 – График полного возмещения инвестиций

## 5.5 Заключение

В результате проделанной работы, можно сказать, что при ставке 15% ЧДС составит 26922р., что говорит об экономической эффективности подсистемы, а ВНД = 33,7%, больше 15%, что свидетельствует об устойчивости разработки. Срок полного возмещения инвестиций составляет чуть меньше, чем два с половиной года.

## ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ЖИЗНЕДЕЯТЕЛЬНОСТИ

### Анализ опасных и вредных производственных факторов при работе пользователей

Анализируется работа с видео-дисплейными терминалами (ВДТ) и персональными электронно-вычислительными машинами (ПЭВМ) как система «человек-машина-среда» (ЧМС). Для этого каждое звено системы рассматривается отдельно.

#### Человек

##### Описание пользователей системы

Пользователями ПО являются инженеры-технологи. Данное ПО предназначено для использования в предприятии ООО «Борей», которое занимается производством и продажей электрической и тепловой энергий и мощностей.

##### Условия труда при работе с ВДТ и ПК

Видеодисплейные терминалы (ВДТ) и персональные компьютеры (ПК) являются источником ряда вредных и опасных факторов производственной среды: излучения электромагнитных полей, воздействия статического электричества. Также условия труда при работе на ВДТ и ПК усугубляются повышенным уровнем шума, неудовлетворительными климатическими условиями, недостаточной освещенностью на фоне зрительного и нервноэмоционального напряжения. Работа, связанная с ВДТ и ПК, сопровождается ограниченной двигательной активностью и монотонностью.

#### Машина

##### Характеристики

Пользователи работают с ПЭВМ типа IBM PC.

##### Шум

Шум, создаваемый одним ПК, невелик, он находится в диапазоне 30-68 дБ. Но, поскольку на рабочем месте находится не один ПК, то шум, производимый ими, является достаточно высоким. Кроме того, данный тип шума оказывает отрицательное воздействие на человека еще и тем, что он является монотонным. Шум нарушает нервную систему; шумовые явления обладают свойством кумуляции: накапливаясь в организме, он все больше и больше угнетает нервную

систему. Шум – причина преждевременного утомления, ослабления внимания, памяти.

Электромагнитные излучения

Основным источником электромагнитных излучений от мониторов ПЭВМ (ПК) является высокочастотный трансформатор строчной развертки, который размещается в задней или боковой части терминала. Таким образом, уровень излучения со стороны задней панели дисплея выше, причем стенки корпуса не экранируют излучение. Требования к электромагнитным полям дисплея приведены в таблице 1.

Таблица 1 – Допустимые значения параметров электромагнитных излучений

| Наименование параметров | Допустимое значение |
|---|---|
| Напряженность электромагнитного поля на расстоянии 50 см вокруг ВДТ по электрической составляющей не более: в диапазоне частот 5 Гц – 2 кГц; в диапазоне частот 2-400 кГц | 25 В/м<br>2,5 В/м |
| Плотность магнитного потока составляет не более: в диапазоне частот 5 Гц – 2 кГц; в диапазоне частот 2 – 400 кГц | 250 нТл<br>25 нТл |
| Поверхностный электростатический | 500 В |

| | |
|---|---|
| потенциал не превышает | |

Электробезопасность

При проведении наладочных работ, а также в процессе эксплуатации ВДТ и ПК человек может прикоснуться к находящимся под напряжением проводникам электрического тока. Персональные ЭВМ относятся к электроустановкам напряжением до 1000 В. Исключение составляют дисплеи, в которых напряжение питания анодов электронно-лучевых трубок составляет несколько киловольт.

Среда

Микроклимат

Работы на ВДТ и ПЭВМ по тяжести и энергозатратам относятся к категории – легкие физические работы (1а, 1б). К категории 1а относятся работы, производимые сидя и не требующие физического напряжения, при которых энергозатраты составляют до 120 ккал/ч. При выполнении таких работ, температура воздуха в холодный период года не более 22–24 оС, в теплый период года не более 23-25 оС. К категории 1б относятся работы, производимые сидя, стоя или связанные с ходьбой и сопровождающиеся некоторым физическим напряжением, при которых энергозатраты составляют от 120 до 150 ккал/ч. При выполнении таких работ, температура воздуха составляет в холодный период года 21-23 оС, в теплый период 22-24 оС. Относительная влажность на рабочих местах составляет 40-60 %, а скорость движения воздуха – не более – 0,1 м/с. Работы пользователей системы относятся к категории 1а.

Оптимальные параметры микроклимата приведены в таблице 2. Микроклимат соответствует этим параметрам.

Таблица 2 – Оптимальные параметры микроклимата

| Температура, $C^o$ | Относительная влажность, % | Абсолютная влажность, % | Скорость движения воздуха, м/с |
|---|---|---|---|
| 19 | 62 | 10 | < 0,1 |

| | | | |
|---|---|---|---|
| 20 | 58 | 10 | < 0,1 |
| 21 | 55 | 10 | < 0,1 |

Естественное и искусственное освещение

Естественное освещение осуществляется через светопроемы, обеспечивающие коэффициент естественной освещенности (к.е.о.) не ниже 1,2% в зонах с устойчивым снежным покровом. Искусственное освещение в помещениях эксплуатации ВДТ и ПЭВМ осуществляется системой общего равномерного освещения. Допускается применение системы комбинированного освещения. Освещенность на поверхности стола в зоне размещения рабочего документа составляет 300-500 лк. Для подсветки документов допускается установка светильников местного освещения.

Производственные здания и помещения

Здания и сооружения, деятельность в которых связана с широким применением ВДТ и ПК размещаются с учетом розы ветров по отношению к соседним предприятиям, которые являются источниками выделения вредных факторов, коррозийно-активных, неприятно пахнущих и пыли.

Площадь помещения определяется количеством рабочих мест с ПК, исходя из расчета на одно рабочее место не менее 6 м2. Высота помещения составляет не менее 3,3 м, объем на одно рабочее место не менее 20,0 м3.

Помещения оборудуются системами отопления, приточно-вытяжной вентиляцией и кондиционированием воздуха.

Организация и оборудование рабочих мест с ВДТ и ПЭВМ

При организации рабочего места пользователя ВДТ и ПЭВМ обеспечивается соответствие конструкции всех элементов рабочего места и их взаимного положения эргономическим требованиям.

Конструкция рабочего стола обеспечивает оптимальное размещение на рабочей поверхности используемого оборудования с учетом его количества и конструктивных особенностей (размер ВДТ и ПЭВМ, клавиатуры и др.) характера работы.

Конструкция рабочего стула (кресла) обеспечивает поддержание рациональной рабочей позы при работе на ВДТ и ПЭВМ, позволяет изменить позу с целью снижении статического напряжения мышц шейно-плечевой области и спины для предупреждения развития утомления.

Экран видеомонитора находится от глаз пользователя на оптимальном расстоянии 600-700 мм, но не ближе 500 мм с учетом размеров алфавитноцифровых знаков и символов.

Клавиатура располагается на поверхности стола на расстоянии 100-300 мм от края, обращенного к пользователю или на специальной, регулируемой по высоте рабочей поверхности, отделенной от основной столешницы.

Рабочие места с ВДТ и ПЭВМ по отношению к световым проемам располагаются так, чтобы естественный свет падал сбоку, преимущественно слева.

Схемы размещения рабочих мест с ВДТ и ПЭВМ учитывают расстояния между рабочими столами с видеомониторами (в направлении тыла поверхности одного видеомонитора и экрана другого), которые составляют не менее 2,0 м, а расстояния между боковыми поверхностями видеомониторов не менее 1,2 м.

Пожарная безопасность

В помещениях с ВДТ и ПК присутствуют все основные факторы, необходимых для возникновения пожара.

Наиболее пожароопасным местом являются кабельные линии. Наличие горючего изоляционного материала, вероятных источников зажигания в виде электрических искр и дуг, разветвленность и недоступность делают кабельные линии местом вероятного возникновения и развития пожара.

По взрыво-пожароопасности помещения с ВДТ и ПК относятся к категории В – пожароопасные (в помещениях имеются твердые сгораемые вещества и материалы).

Режим труда и отдыха при работе с ПК

Рациональный режим труда и отдыха предусматривает соблюдение определенной длительности непрерывной работы на ПК и перерывов,

регламентированных с учетом продолжительности рабочей смены, вида и категории трудовой деятельности.

Выделяют три вида работ, выполняемых на ПК: группа А – работа по считыванию информации с экрана с предварительным запросом, группа Б – работа по выводу информации, группа В – творческая работа в режиме диалога с ПК. Работа пользователей системы относится к группе В. Категории тяжести и напряженности работы на ПК (I, II, III) определяются уровнем нагрузки за рабочую смену: для группы В – по суммарному времени непосредственной работы на ПК (таблица 3).

Таблица 3 – Виды и категории трудовой деятельности с ПК

| Категория работы (по тяжести и напряженности работы с ВДТ и ПЭВМ) | Уровень нагрузки за рабочую смену при видах работы на ПК |
|---|---|
| Группа В, час | |
| I | до 2,0 |
| II | до 4,0 |
| III | до 6,0 |

Работа пользователей системы относится к категории III.

Количество и длительность регламентированных перерывов, их распределение в течение рабочей смены устанавливается в зависимости от категории тяжести и напряженности работы на ПК и продолжительности рабочей смены.

При 8-часовой рабочей смене и работе с ПК регламентированные перерывы устанавливаются:

для III категории работы – через 1,5-2,0 ч от начала рабочей смены и через 1,5-2,0 ч после обеденного перерыва продолжительностью 20 мин. каждый или продолжительностью 15 мин через каждый час работы.

# ЗАКЛЮЧЕНИЕ

Целью моей выпускной квалификационной работы заключалось в разработке подсистемы анализа инцидентов в информационной сети предприятия.

Чтобы успешно достичь поставленной цели вся работа была декомпозирована на отдельные задачи. В первую очередь мной был проведен анализ работы SIEM-систем, проведены наиболее эффективные архитектурные решения среди существующих Российских и зарубежных систем. В ходе данного анализа были выделены две SIEM-системы – зарубежная HP Arcsight SIEM и отечественная PT MaxPatrol SIEM. Данные системы широко распространены, обладают широким функционалом, постоянно и динамически развиваются.

После выбора двух SIEM-систем было произведено полное сравнение данных решений. MaxPatrol SIEM показала себя с наилучшей стороны, превзойдя своего конкурента по многим параметрам при анализе инцидентов ИБ и аудите IT-инфраструктуры организаций.

Определив MaxPatrol как наиболее перспективное решение, провел полное изучение его инфраструктуры, жизненный цикл обработки событий, работы всех компонентов, модулей, служб и сервисов, собрал статистику и выявили актуальные проблемы системы. Актуальной проблемой стало количество ложных срабатываний при неэффективных использованиях правил корреляции.

Для устранения данной проблемы была разработана и реализована подсистема анализа инцидентов на основе динамических табличных списков и расширения правил корреляций для анализа событий и обнаружения инцидентов. Был разработан блок, изначально не поддерживаемый системой, – время жизни той или иной записи в табличных списках, что позволило сделать их динамическими и постоянно меняющимися вместе с инфраструктурой и задачами предприятия.

Подсистемы была успешно внедрена и проверена на работоспособность. Для проверки правильной работы было проведено расследование инцидента «Подбор пароля». Это позволило убедиться, что подсистема функционирует правильно.

После этого была снова собрана статистика по инцидентам, что позволило оценить эффективность разработанной подсистемы. Процент обнаружения инцидентов ощутимо вырос, а процент ложных срабатываний, соответственно снизился.

Это позволило сотрудникам информационной безопасности сэкономить ресурсы в виде человеко-часов и переключиться на выполнение других, не менее важных задач.

Таким образом, поставленные задачи решены в полном объеме. Цель, поставленная в данной квалификационной работе достигнута.

## СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. ГОСТ Р ИСО/МЭК 18044 - Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. – Введ. 2008-07-01 - М.: Изд-во стандартов, 2007. – 27 с.

2. Малыхина, Г.Ф. Администрирование данных информационных систем. Учебное пособие для студентов высших учебных заведений, обучающихся по направлению подготовки магистров "Системный анализ и управление" / Г.Ф. Малыхина, Н.Г. Полетаева. – Санкт-Петербург: Национальный исследовательский университет СПбГПУ, 2014. - 197 с.

3. Шалаевский, О.Н., Малыхина Г.Ф. Безопасность информационноизмерительных систем. Учебное пособие. / О.Н. Шалаевский, Г.Ф. Малыхина. – Санкт-Петербург: Национальный исследовательский университет СПбГПУ, 2012. - 153 с.

4. Бурлаков, Д.Н. Новые подходы при построении SOC (Security Operations Center) / Д.Н. Бурлаков. // Информационная безопасность. – 2013. - №4. – с. 31-33.

5. Канев, А.Н. Мониторинг событий и обнаружение инцидентов информационной безопасности с использованием SIEM-систем / А.Н. Канев // Международный студенческий научный вестник. – 2015. – №3. – с. 4-7.

6. Котович, А.С. Игра Штакельберга в комплексной защите информации / А.С. Котович, Г.Ф. Малыхина. // Неделя науки СПбГПУ: материалы научнопрактической конференции с международным участием. – Санкт-Петербург: Институт информационных технологий и управления СПбГПУ, 2014. - с. 239-241.

7. Шупик, В.Я., Малыхина Г.Ф. Безопасная информационная система для музея. / В.Я. Шупик, Г.Ф. Малыхина. // Сборник докладов студенческой научной конференции Института компьютерных наук и технологий. – СанктПетербург: Институт информационных технологий и управления СПбГПУ,2016. - с. 216-218

8. Типичные ошибки при внедрении SIEM-решений. [Электронный ресурс] // rvision.pro: сайт компании R-Vision – 2018. – URL: https://rvision.pro/blog-posts/6-tipichnyh-oshibok-pri-vnedrenii-siem-reshenij-kakihizbezhat (дата обращения: 08.04.2019).

9. Типовая система мониторинга событий безопасности. [Электронный ресурс] // iitrust.ru: электронный документооборот – 2018. – URL: https://iitrust.ru/region/vpn/primery/monitoring-sobytiy.php, 2018 (дата обращения: 08.04.2019).

10. SIEM [Электронный ресурс] // wikipedia.org: электронная энциклопедия. – 2019. – URL: https://ru.wikipedia.org/wiki/SIEM (дата обращения 12.03.2019).

11. Threat Intelligence and SIEM (Part 1) — Reactive Security [Электронный ресурс] // recordedfuture.com: блог, посвященный информационным технологиям. – 2016. – URL: https://www.recordedfuture.com/siem-threatintelligence-part-1/ (дата обращения: 10.04.2019).

12. SIEM for beginners [Электронный ресурс] // 7sec.com: блог, посвященный информационной безопасности. – 2015. – URL: https://www.7sec.com/blog/siem-for-beginners/ (дата обращения: 10.04.2019).

13. Security Operations Center Soc Architecture [Электронный ресурс] // jerusalemhouseministries.net: блог на различную тематику. – 2018. – URL: https://www.jerusalemhouseministries.net/image/security-operations-center-socarchitecture (дата обращения: 10.04.2019).

14. PT MaxPatrol SIEM [Электронный ресурс] // ptsecurity.com: официальный сайт компании Positive Technologies. – 2017. – URL: https://www.ptsecurity.com/ru-ru/products/mpsiem/ (дата обращения: 20.03.2019).

15. Positive Technologies MaxPatrol SIEM [Электронный ресурс]. – Электротекстовые граф. дан. – Positive Technologies, 2019. – 5 частей руководства в электронном виде.

16. Disrupting the kill chain [Электронный ресурс] // microsoft.com: официальный сайт компании Microsoft. – 2016. – URL: https://www.microsoft.com/security/blog/2016/11/28/disrupting-the-kill-chain/ (дата обращения: 15.03.2019).

17. Cyber-Attack Chain [Электронный ресурс] // beyondtrust.com: блог, посвященный информационной безопасности. – 2018. – URL: https://www.beyondtrust.com/resources/glossary/cyber-attack-chain (датаобращения: 07.04.2019).

18. Positive Technologies. Защита периметра: старые атаки не хуже новых [Электронный ресурс] / Positive Technologies // habr.com: русскоязычный вебсайт в формате коллективного блога. – 2016. – URL: https://habr.com/ru/company/pt/blog/309072/ (дата обращения: 05.04.2019).

19. What is Threat Intelligence and why is it important? [Электронный ресурс] // blueliv.com: блог, посвященный информационной безопасности. – 2018. – URL: https://www.blueliv.com/blog/threat-intelligence/what-is-threatintelligence/ (дата обращения: 08.04.2019).

20. Ростелеком-Solar. Страх и ненависть Threat Intelligence или 8 практических советов по работе с TI [Электронный ресурс] / Ростелеком-Solar // habr.com:

русскоязычный веб-сайт в формате коллективного блога. – 2018. – URL: https://habr.com/ru/company/solarsecurity/blog/417297/ (дата обращения: 09.04.2019).

21. Indicators of Compromise in Threat Intelligence – Let’s speak some InfoSec Jargon [Электронный ресурс] // armordot.com: блог, посвященный информационной безопасности. – 2017. – URL: https://www.armordot.com/2017/09/29/indicators-of-compromise-threat-intelligencelets-speak-some-infosec-jargon/ (дата обращения: 10.04.2019).

22. Перспективный мониторинг. О потребителях и типах Threat Intelligence [Электронный ресурс] / Перспективный мониторинг // habr.com: русскоязычный веб-сайт в формате коллективного блога. – 2017. – URL: https://habr.com/ru/company/pm/blog/319666/ (дата обращения: 29.03.2019).

23. Ростелеком-Solar. Как работать с данными кибербразведки: учимся собирать и выявлять индикаторы компрометации систем [Электронный ресурс] / Ростелеком-Solar // habr.com: русскоязычный веб-сайт в формате коллективного блога. – 2019. – URL: https://habr.com/ru/company/solarsecurity/blog/438798/ (дата обращения: 09.04.2019).

**ПРИЛОЖЕНИЕ**

```
import requests
import re
import html
import csv
from requests.packages.urllib3.exceptions import InsecureRequestWarning
requests.packages.urllib3.disable_warnings(InsecureRequestWarning)
import datetime



class CustomSMTPServer(smtpd.SMTPServer):

    def process_message(self, peer, mailfrom, rcpttos, data):
        mailto = str(rcpttos[0])

        msg = email.message_from_string(data)
        # parser subject
        subject = msg.get('Subject')

        # parser body
        if msg.is_multipart():
            for part in msg.get_payload():
                if part.get_content_maintype() == 'text' and part.get('Content-
Disposition') == None:
                    msg_body = part.get_payload(decode=1)

                    print(msg_body)
        else:
            msg_body = msg.get_payload()

        send_email(mailfrom, mailto, subject, msg_body)
        return
server = CustomSMTPServer(('***.***.***.***', 25), None)
asyncore.loop()
```

```
class AccessDenied(Exception):
    pass


def authenticate(address, login, password, new_password=None, auth_type=0):
    session = requests.session()
    session.verify = False

    response = print_response(session.post(
        address + ':3334/ui/login',
        json=dict(
            authType=auth_type,
            username=login,
            password=password,
            newPassword=new_password
        )
    ), check_status=False)

    if response.status_code != 200:
        raise AccessDenied(response.text)

    if '"requiredPasswordChange":true' in response.text:
        raise AccessDenied(response.text)

    return session


def external_auth(session, address):

    response = print_response(session.get(address))

    if 'access_denied' in response.url:
        return False
```

```
    while '<form' in response.text:
        form_action, form_data = parse_form(response.text)

        response = print_response(session.post(form_action, data=form_data))

    return True


def parse_form(data):
    return re.search('action=[\'"]([^\'"]*)[\'"]', data).groups()[0], {
        item.groups()[0]: html.unescape(item.groups()[1])
        for item in re.finditer(
            'name=[\'"]([^\'"]*)[\'"] value=[\'"]([^\'"]*)[\'"]',
            data
        )
    }


def print_response(response, check_status=True):
    if check_status:
        assert response.status_code == 200
    return response


if __name__ == "__main__":
    # Настройки
    settings = dict()

    # адрес сиема
    settings['base_url'] = ''
    settings['clear_method_url'] = '/api/events/v1/table_lists/dynamic_list/clear'
    settings['import_method_url'] = '/api/events/v1/table_lists/dynamic_list/import'
    settings['signin_form_url'] =
'/account/login?returnUrl=/#/authorization/landing'
```

```
        # логин
        settings['user'] = ''
        # пароль
        settings['pass'] = ''

        # Аутентификация
        session = authenticate(settings['base_url'], settings['user'], settings['pass'])

        if not external_auth(session, settings['base_url'] + settings['signin_form_url']):
            print("Ошибка аутентификация.")
        # аутентификация прошла
        else:
            #
            if resp.status_code == 200:
                cur_date = datetime.datetime.now().strftime("%d.%m.%Y %H:%M:%S")

                # конвертируем в csv-файл
                with open(file_name, 'w', newline='') as csv_file:
                    fieldnames = ['_last_changed', 'ip']
                    writer = csv.DictWriter(csv_file, fieldnames=fieldnames, delimiter=';',
quoting=csv.QUOTE_ALL)
                    writer.writeheader()

                    for line in resp.iter_lines():
                        writer.writerow({
                            fieldnames[0]: cur_date,
                            fieldnames[1]: line.decode("utf-8")
                        })

                # очищаем старые данные1
                session.post(settings['base_url'] + settings['clear_method_url'])

                # загружаем новые данные
                with open(file_name, 'rb') as data:
                    headers = {'Content-Type': 'application/x-www-form-urlencoded'}
```

```
                resp = session.post(settings['base_url'] + settings['import_method_url'],
data=data, headers=headers)
                #print(resp.text)
            # ошибка аутентификации
            else:
                print("Не удалось получить данные.")
```