**Министерство науки и высшего образования Российской Федерации** федеральное государственное бюджетное образовательное учреждение высшего образования

«Российский экономический университет имени Г.В. Плеханова»

Высшая школа кибертехнологий, математики и статистики Кафедра прикладной информатики и информационной безопасности

Направление 10.03.01 Информационная безопасность

**О Т Ч Е Т**

**по учебной практике студента:**

***практике по получению первичных профессиональных умений и навыков***

Выполнила студентка гр. 15.11Д- ИБ16/20б

3 курс, ВШКМиС

Гнездилова Маргарита Николаевна

Проверила:

Ассистент кафедры ПИиИБ Королева Д.С.

*(оценка) (подпись)*

*(дата)*

**Москва 2023**

**Оглавление**

[Введение 3](#_Toc140777949)

[Ознакомительный системы обзор RuSIEM 4](#_Toc140777950)

[Заключение 8](#_Toc140777951)

[Список использованной литературы 9](#_Toc140777952)

# Введение

Данной практическая работа разделена на 2 части. Первая часть работы посвящена ознакомительному обзору системы RUSIEM. Описание, назначение, история создания аналитической системы RUSIEM, возможности системы и цели использова

# Ознакомительный системы обзор RuSIEM

## 1. Описание

RuSIEM представлен на рынке тремя продуктами с разными функциональными возможностями.

* RuSIEM — коммерческая версия системы класса SIEM, включающая корреляцию в режиме реального времени, визуализацию данных и поиск по ним, долгосрочное хранение сырых и нормализованных событий, инцидент менеджмент и отчеты.
* RvSIEM — бесплатный, свободно распространяемый продукт класса Log Management (управление журналами), с помощью которого можно выполнять нормализацию полученных логов, обогащать события, искать данные в журналах, строить отчёты и создавать информационные панели. Количество обрабатываемых событий — до 500 в секунду.
* RuSIEM Analytics — модуль, который позволяет выявлять аномалии, формировать аналитические отчёты, управлять активами, построить процесс управления уязвимостями и реализовать много других дополнительных возможностей.

## 2. История создания

Любая ИТ-система создается с какой-то целью. Одни системы начинаются с идеи, другие — с желания проверить определенную гипотезу. Некоторые решения создаются с целью заработка или исходя из текущих потребностей клиента/клиентов или рынка.  
 Система RuSIEM появилась примерно по этому же принципу. Первому заказчику компании нужно было иметь возможность управлять событиями информационной безопасности. Это был 2014 год, когда были введены санкции против России. Почти все производители SIEM, представленных тогда в России, были из США, и при малейшем сомнении отказывали интеграторам в поставке. Также произошло и с заказчиком компании RuSIEM. Он обратился к нам, мы предложили решение на базе связки open source решений класса Log management (предназначенных для сбора событий, хранения и навигации по ним), известных как ELK (Elasticsearch-Logstash-Kibana).  
 Однако решение имело много минусов. Но за счет дописывания и переписывания кода, добавления собственных модулей и реализации поддержки большого количества источников "из коробки" были устранены указанные проблемы и расширен набор возможностей

Ключевые этапы развития системы:

* 2014 — создание продукта.
* 2015 — анонс функциональности первой коробочной версии и первая партия ключей для пилотных проектов. Появление симптоматики, Workflow и улучшение работы с инцидентами.
* 2016 — появление взаимосвязей, отчётов, модуля аналитики.
* 2017 — появление бесплатной версии продукта. Внедрение мультиязычности, собственной шины RuSIEM MQ. Переход с influxdb на БД разработки Яндекс — ClickHouse.
* 15.08.2017 — RuSIEM включена в реестр российского ПО.
* 2018 — обновление API и возможность управления всеми нодами удаленно, с единого интерфейса.
* 2019 — возможность создавать собственные парсеры и подключать любой источник самостоятельно.
* 2020 — поддержка Ubuntu 18. Функционал мониторинга внутренних микросервисов системы, функционал подключения подчиненных серверов. Закончена полноценная интеграция c R-Vision.
* 2021 — переработаны корневые сервисы RuSIEM: Оптимизирован поиск по событиям, оптимизирована аналитика. Добавлена статистика по парсерам, статистика по отработке корреляции. Поддержка Telnet и SSH для агента и модулей.
* 19.05.2021 — система получила сертификат ФСТЭК.
* С лета 2021 — в парсер добавлена функция разбора xml, добавлена первая версия модуля активов. Добавлена поддержка матрицы MITRE, модули Sysmon и System Info. Реализована поддержка ElasticSearch 7. Переработаны интерфейс для дашбордов событий и функционал симптоматики.

## 3. Назначение

Полная версия системы предназначена как для сбора и анализа информации, так и для обнаружения атак и различных аномалий в организации, проведения глубокого анализа и проактивного поиска угроз, а также оперативного реагирования на инциденты и их дальнейшего расследования. Система способна выявить угрозу, когда обычные средства детектирования по отдельности её не видят, но она может быть обнаружена при тщательном анализе и корреляции информации из различных источников.

Полная версия системы предоставляет следующие функциональные возможности:

* сбор с помощью собственного агента и пассивный прием событий;
* нормализация событий c долгосрочным хранением и оперативным поиском;
* обогащение событий мета-информацией, описывающей о чем событие в понятном для пользователя формате;
* поиск по событиям без знания типов и состава событий на основе симптоматики;
* приоритезация событий посредством весов симптоматики, в том числе составным весом;
* корреляция на последовательных событиях (счетчик);
* триггерная корреляция фактов различных событий;
* агрегация весов по объектной модели для обнаружения угроз без применения сигнатур;
* проверка ip, fqdn, md5/sha1 file, url, email по фид-листам с угрозами;
* встроенный инцидент-менеджмент для реагирования и фиксации угроз;
* автоматическое обновление продукта, правил корреляции, симптоматики и фидов;
* ролевая модель доступа в систему.

## 4. Возможности RuSIEM

1. Возможность отправки предупреждений на основе предопределенных настроек.
2. Отчеты и логирование для упрощения аудита.
3. Возможность просмотра данных на разных уровнях детализации

## 5. Где может применяться RuSIEM

1. Везде, где из журналов событий можно извлечь полезную информацию.
2. Аудит доступа, контроль доступа к критичным ресурсам, оценка числа посетителей сайта, обнаружение malware, контроль физического доступа, оценка продаж, интересов потребителей, снижение числа ложных срабатываний, аудит финансовых показателей, анализ сетевой активности, контроль автоматизированных устройств (конвейерных лент).

# Заключение

В первой части данной работы был сделан пересказ англоязычной статьи 2023 года на тему “Использование конфиденциальных данных для предотвращения дискриминации со стороны искусственного интеллекта: нужно ли новое исключение из общего регламента по защите данных?” и сделан следующий вывод, что в целом, существуют различные аргументы в пользу и против принятия исключения, которое позволяет использовать специальные категории данных для предотвращения дискриминации со стороны ИИ. Баланс между аргументами «за» и «против» найти сложно. Если такое исключение было принято, оно должно также включать меры предосторожности для сведения к минимуму рисков.

Во второй части практического задания был проведен ознакомительный обзор системы RUSIEM. А именно: описание, назначение, история создания аналитической системы RUSIEM, возможности системы и цели использования.

# Список использованной литературы

1. Using sensitive data to prevent discrimination by artificial intelligence: Does the GDPR need a new exception?: [Электронный ресурс] – Режим доступа: https://www.sciencedirect.com/science/article/pii/S0267364922001133 [-novye-](http://ironfriends.ru/kiberbezopasnost-v-industrii-4-0-novye-vyzovy-i-resheniya/) vyzovy-i-resheniya/ – Дата обращения 06.07.2023
2. Система RUSIEM: [Электронный ресурс] – Режим доступа: <https://docs.rusiem.tech/> – Дата обращения 06.07.2023
3. RUSIEM: [Электронный ресурс] – Режим доступа: https://rusiem.com/ – Дата обращения 06.07.2023
4. RuSIEM: принцип работы, плюсы, все решения: [Электронный ресурс] – Режим доступа: https://www.azone-it.ru/sistema-upravleniya-informacionnoy-bezopasnostyu-siem/rusiem – Дата обращения 06.07.2023