**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 4](#_Toc139573794)

[Термины и сокращения 5](#_Toc139573795)

[Пересказ англоязычной статьи 2023 года авторов Marvin van Bekkum, Frederik Zuiderveen Borgesius, по теме "Using sensitive data to prevent discrimination by artificial intelligence: Does the GDPR need a new exception?" из журнала “The Computer Law and Security Review” 6](#_Toc139573796)

[1. Введение 6](#_Toc139573797)

[2. Системы ИИ и дискриминация 8](#_Toc139573798)

[2.1. Причины дискриминации со стороны ИИ 8](#_Toc139573799)

[2.2. Использование специальных категорий данных полезно для устранения предвзятости систем ИИ. 9](#_Toc139573800)

[3. Закон о недискриминации 9](#_Toc139573801)

[4. Закон о защите данных 10](#_Toc139573802)

[5. Мешает ли GDPR предотвращению дискриминации? 11](#_Toc139573803)

[5.1. Запрет GDPR на обработку особых категорий данных 12](#_Toc139573804)

[5.2. Исключения из запрета 13](#_Toc139573805)

[6. Новое исключение из запрета на использование специальных категорий данных? 13](#_Toc139573806)

[6.1. Аргументы в пользу исключения 14](#_Toc139573807)

[6.3. Аргументы против исключения 14](#_Toc139573808)

[7. Возможные гарантии в случае принятия исключения 14](#_Toc139573809)

[8. Заключение 15](#_Toc139573810)

[Ознакомительный обзор системы RuSIEM 18](#_Toc139573811)

[1. Описание 18](#_Toc139573812)

[2. История создания 18](#_Toc139573813)

[3. Назначение 20](#_Toc139573814)

[4. Возможности RuSIEM 21](#_Toc139573815)

[5. Где может применяться RuSIEM 21](#_Toc139573816)

[Заключение 22](#_Toc139573817)

[Список использованной литературы 23](#_Toc139573818)

# Введение

Данной практическая работа разделена на 2 части. В первой части будет рассмотрена и пересказана англоязычная статья 2023 года авторов Marvin van Bekkum, Frederik Zuiderveen Borgesius, по теме " Using sensitive data to prevent discrimination by artificial intelligence: Does the GDPR need a new exception?" из журнала “The Computer Law and Security Review”. Данная статья затрагивает актуальную тему нынешнего времени о дискриминации и искусственном интеллекте. Она рассказывает, как общий регламент по защите персональных данных может помочь в борьбе с предрассудками ИИ при приеме решений. Вторая часть работы посвящена ознакомительному обзору системы RUSIEM. Описание, назначение, история создания аналитической системы RUSIEM, возможности системы и цели использования.

# Термины и сокращения

GDPR — Общий регламент по защите данных

HR — Отдел кадров

ИИ — Искусственный интеллект

# Пересказ англоязычной статьи 2023 года авторов Marvin van Bekkum, Frederik Zuiderveen Borgesius, по теме "Using sensitive data to

# prevent discrimination by artificial intelligence: Does the GDPR need a new exception?" из журнала “The Computer Law and Security Review.”

## Введение

Организации могут применять искусственный интеллект с разными целями, включая принятие решений о людях. Например, они могут использовать ИИ для выбора наилучших кандидатов из большого количества заявлений о приеме на работу. Однако использование систем ИИ может привести к дискриминации. Некоторые ИИ-системы могут отклонять заявки от людей определенной этнической принадлежности, даже если организация не стремится к такой дискриминации. Однако в Европе возникает проблема, когда организация хочет проверить, случайно ли ее система искусственного интеллекта дискриминирует людей на основе их этнической принадлежности. Проблема заключается в том, что организация может не иметь информации о этнической принадлежности заявителей. В рамках Общего регламента о защите данных (GDPR) запрещается использование определенных "особых категорий данных", таких как информация о расовой принадлежности, религии и сексуальных предпочтениях. Однако предложение Европейской комиссии о Законе об искусственном интеллекте содержит положение, позволяющее организациям использовать специальные категории данных для аудита своих систем ИИ. В данной статье исследуются вопросы, связанные с соответствием общим регламентом по защите данных в отношении использования специальных категорий персональных данных для предотвращения дискриминации с использованием ИИ. Авторы утверждают, что во многих случаях общий регламент по защите данных запрещает использование данных специальной категории. Они также представляют аргументы за и против создания исключения из запрета общего регламента по защите данных на использование специальных категорий персональных данных для предотвращения дискриминации со стороны систем ИИ. Хотя данная статья основана на европейском праве, ее результаты могут быть применимы и за пределами Европы.

В этой статье вносится три новых вклада в литературу. Во-первых, авторы объединяют юридические знания в области недискриминации и защиты данных, а также исследования в области искусственного интеллекта и компьютерных наук. Они рассматривают существующие работы в различных дисциплинах, связанных с использованием данных специальных категорий для предотвращения дискриминации.

Во-вторых, авторы показывают, что в большинстве случаев общий регламент по защите данных не позволяет использовать специальные категории данных для борьбы с предвзятостью. хотя общий регламент по защите данных предусматривает возможность исключений с учетом определенных условий, такое исключение для использования данных специальной категории не было установлено. Авторы не согласны с теми учеными, которые предполагают, что общий регламент по защите данных позволяет такой сбор данных.

В-третьих, авторы анализируют аргументы за и против введения нового исключения в общий регламент по защите данных, позволяющего бороться с предвзятостью в системах ИИ. Они представляют веские аргументы в пользу обеих точек зрения.

Статья структурирована следующим образом: В разделах 2 и 3 представлены ключевые термины, описывается, как ИИ может дискриминировать на основе этнической принадлежности, и вводится законодательство о недискриминации. В разделах 4 и 5 анализируется структура общего регламента по защите данных в отношении специальных категорий данных и обсуждается, мешает ли эта структура сбору таких данных организациями. В разделе 6 представлены аргументы за и против введения нового исключения для сбора и использования данных специальной категории в аудите систем ИИ. В разделе 7 рассматриваются возможные меры безопасности, сопровождающие такое исключение, и в разделе 8 делается вывод.

## 2. Системы ИИ и дискриминация

Системы искусственного интеллекта (ИИ) представляют собой компьютерные системы, способные выполнять задачи, которые обычно требуют человеческого интеллекта, такие как визуальное восприятие, распознавание речи, принятие решений и перевод между языками, согласно Оксфордскому словарю. Однако в нашем исследовании мы сосредоточимся на системах ИИ, которые принимают решения, имеющие серьезные последствия для людей.

Для примера, допустим, что банк использует систему искусственного интеллекта для принятия решения о том, следует ли предоставить клиенту ипотечный кредит или нет. Решение, принятое этой системой, может иметь значительные последствия для жизни и финансового положения клиента. Определение, предоставить кредит или отказать в нем, может оказать существенное влияние на возможности клиента приобрести жилье и обеспечить свое будущее.

Такие системы ИИ часто основаны на алгоритмах и моделях, которые обрабатывают большое количество данных и используют их для принятия решений. Однако важно отметить, что эти системы могут подвергаться влиянию искаженных или несбалансированных данных, что может привести к некорректным или дискриминационным результатам. Поэтому необходимо тщательно обращаться с использованием систем ИИ, особенно когда они принимают решения, которые могут оказывать воздействие на жизнь людей.

### 2.1. Причины дискриминации со стороны ИИ

Дискриминационные входные данные являются одним из основных источников дискриминации системами ИИ. Представим ситуацию, где HR-отдел организации в прошлом дискриминировал женщин. Предположим, что сама организация не осознает прошлую дискриминацию, проводимую ее HR-отделом. Если организация использует исторические данные для обучения своей системы ИИ, эта система может воспроизводить дискриминацию. Примером служит проект системы найма компании Amazon, который был прекращен из-за обнаруженной дискриминации до его применения на практике.

Системы ИИ могут принимать дискриминационные решения в отношении кандидатов на работу, например, нанося ущерб определенным этническим группам, даже если сама система не имеет прямого доступа к данным об этнической принадлежности. Представьте себе систему ИИ, которая учитывает почтовые индексы, принадлежащие кандидатам. Почтовые индексы могут быть связаны с этнической принадлежностью людей. Таким образом, система может отклонять всех лиц определенной этнической принадлежности, даже если организация гарантировала, что система не учитывает этническую принадлежность. На практике система ИИ может учитывать сотни переменных в сложных комбинациях, которые коррелируют с этнической принадлежностью. Такие переменные, связанные с защищенными атрибутами, например, этнической принадлежностью, могут быть названы "прокси-атрибутами". Такие корреляции могут привести к дискриминации по средствам непрямых показателей. Разработчики ИИ или организации, использующие системы ИИ, могут не осознавать, что эта система приводит к дискриминационным последствиям из-за прокси-атрибутов.

### 2.2. Использование специальных категорий данных полезно для устранения предвзятости систем ИИ.

Авторы статьи представляют следующий пример: предположим, что организация стремится узнать, дискриминирует ли их система искусственного интеллекта соискателей определенной этнической принадлежности. Для проведения такой проверки организация должна знать этническую принадлежность как соискателей, подавших заявки на работу, так и фактически нанятых сотрудников. Предположим, что половина соискателей, отправивших письма с заявлениями о приеме на работу, имеют иммигрантское прошлое. Система искусственного интеллекта выбирает лучшие 50 писем из тысячи. При принятии решений система ИИ учитывает различные атрибуты, такие как выбранный университет или курсы. Однако из этих пятидесяти писем, выбранных системой ИИ, ни одно не принадлежит иммигрантам. Такие данные вызывают вопросы о возможной несправедливости или незаконной предвзятости системы ИИ.

Такой пример показывает, что система ИИ требует дополнительного исследования с целью определения, существует ли несправедливость или противозаконная предвзятость. Важно выявить, какие атрибуты и факторы влияют на принятие решений системой ИИ и как они могут повлиять на разные этнические группы. Для обеспечения справедливого и недискриминационного применения системы ИИ необходимо применять соответствующие меры, например аудит системы, исправление несоответствий и устранение проблемных алгоритмов. Это позволит предотвратить потенциальную дискриминацию и обеспечить равные возможности для всех соискателей на рабочие места.

## 3. Закон о недискриминации

Право на недискриминацию является важным правом человека и защищено международными и региональными нормативными актами, такими как Европейская конвенция о правах человека (1950 г.), Международная конвенция о ликвидации всех форм расовой дискриминации (1965 г.), Международный пакт о гражданских и политических правах (1966 г.) и Хартия основных прав Европейского союза (2000 г.).

В контексте Европейского Союза законодательство запрещает две формы дискриминации: прямую и косвенную дискриминацию. Директива о расовом равенстве (об этнической принадлежности) подчеркивает, что принцип равного обращения означает отсутствие прямой или косвенной дискриминации на основе расового или этнического происхождения. Прямая дискриминация определяется как неблагоприятное обращение к человеку по признаку расового или этнического происхождения в аналогичной ситуации.

В данной статье акцент делается на косвенной дискриминации. Косвенная дискриминация со стороны системы ИИ может проявиться, когда система, казалось бы, нейтральна, но в итоге приводит к дискриминации людей с защищенными характеристиками. Например, даже если система ИИ исключает прямые указатели на защищенные атрибуты, она может все равно использовать показатели, которые являются прокси-атрибутами для защищенных характеристик.

Важно отметить, что независимо от того, является ли дискриминация случайной или намеренной, организация всегда несет ответственность, даже если она не осознавала, что ее система ИИ косвенно дискриминирует.

В отличие от прямой дискриминации, косвенная дискриминация может быть исключена в определенных случаях. Если организация, которая может быть подозреваемым дискриминатором, преследует законную цель с использованием нейтральной практики, и эта практика пропорциональна для достижения такой цели, то косвенная дискриминация не считается незаконной. Однако, если система ИИ имеет дискриминационные последствия, применяются общие нормы закона Европейского Союза о недискриминации.

## 4. Закон о защите данных

Право на неприкосновенность частной жизни и защиту персональных данных являются фундаментальными правами. Эти права защищены международными и региональными нормативными актами, такими как Европейская конвенция о правах человека (1950 г.), Международный пакт о гражданских и политических правах (1966 г.) и Хартия основных прав Европейского союза (2000 г.).

С начала 1970-х годов развивается новая область права - закон о защите данных. В Европейском Союзе право на защиту персональных данных имеет статус основного права. Хартия основных прав Европейского Союза прямо гарантирует право на защиту персональных данных. Закон о защите данных устанавливает права для лиц, чьи данные обрабатываются (субъекты данных), и накладывает обязательства на стороны, которые обрабатывают персональные данные (контролеры данных). Закон о защите данных направлен на обеспечение защиты персональных данных и при этом учитывает другие ценности и права. Важно отметить, что закон о защите данных направлен не только на защиту частной жизни, но также на защиту права на недискриминацию и других прав.

Защита персональных данных имеет большое значение в эпоху цифровой информации, где массовое сбор и обработка данных становятся все более распространенными. Люди имеют право на контроль над своими персональными данными и на обеспечение их безопасности и конфиденциальности. Закон о защите данных устанавливает стандарты и требования, которые должны соблюдаться при обработке персональных данных, и предусматривает санкции в случае их нарушения.

Основываясь на этих правовых нормах, организации, использующие системы искусственного интеллекта, должны учитывать право на недискриминацию, защиту частной жизни и персональных данных. Они должны разрабатывать и применять этические и законные методы использования данных и систем ИИ, чтобы предотвратить дискриминацию и нарушение прав личности. Это поможет создать более справедливое и доверительное использование ИИ в обществе.

## 5. Мешает ли GDPR предотвращению дискриминации?

### 5.1. Запрет GDPR на обработку особых категорий данных

Согласно Общему регламенту ЕС по защите данных (GDPR), особое внимание уделяется праву на защиту данных, что дополняет положения Хартии ЕС. Общий регламент по защите данных, а также его предшественник - Директива о защите данных 1995 года, содержат принципиальный запрет на использование особых категорий данных, также известных как «чувствительные данные». Более строгий режим обработки особых категорий данных объясняется стремлением предотвратить несправедливую дискриминацию. Ранее, в 1972 году, Совет Европы заявил о конфиденциальности личных данных, отметив, что информация, относящаяся к интимной частной жизни лиц или могущая привести к несправедливой дискриминации, не должна записываться или распространяться.

Большинство оснований для защиты данных в директивах ЕС о недискриминации также являются особыми категориями данных, определенными в статье 9(1) общий регламент по защите данных. Однако есть два исключения. Во-первых, "возраст" и "пол" являются защищенными характеристиками в законодательстве о недискриминации, но не считаются особыми категориями данных в контексте общий регламент по защите данных. Во-вторых, "политические взгляды", "членство в профсоюзах", "генетическая информация" и "биометрические данные" являются особыми категориями данных, но не защищены европейскими директивами о недискриминации.

Изображение выглядит как текст, круг, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 1 - Перекрытие между защищенными характеристиками и специальными категориями данных.

Запрет, установленный общим регламентом по защите данных на обработку особых категорий данных, может затруднить предотвращение дискриминации системами искусственного интеллекта. Например, организация использует систему ИИ для подбора лучших кандидатов из множества заявлений о приеме на работу и желает проверить, не случайно ли ее система ИИ дискриминирует определенные этнические группы. Для проведения такой проверки организации необходимы данные об этнической принадлежности соискателей. Однако, без таких данных проведение такого аудита становится сложны

### 5.2. Исключения из запрета

Статья 9(2) общий регламент по защите данных содержит список исключений из общего запрета на обработку особых категорий данных. Подразделы (a), (b), (f), (g) и (j) содержат возможные исключения для сбора и использования данных особой категории.

Некоторые специалисты по недискриминации предполагают, что закон о защите данных не препятствует сбору и использованию специальных категорий данных для борьбы с дискриминацией. Один ученый считает, что «необходимо развеять мифы» о том, что законодательство о защите данных должно исключать обработку данных о равенстве. Однако авторы не нашли в литературе подробных аргументов в пользу того, что общий регламент по защите данных позволяет использовать специальные категории данных в целях недискриминации.

Однако общий регламент по защите данных действительно ограничивает возможность организаций использовать данные особой категории для предотвращения дискриминации со стороны их систем искусственного интеллекта. В некоторых исключительных ситуациях организация может получить действительное согласие субъектов данных на такое использование. В других случаях потребуется закон ЕС или национальное законодательство, позволяющее использовать данные особой категории для борьбы с предвзятостью систем ИИ. В настоящее время в ЕС такие законы отсутствуют.

## 6. Новое исключение из запрета на использование специальных категорий данных?

### 6.1. Аргументы в пользу исключения

Авторы приводят два основных аргумента в пользу создания нового исключения, которое позволяет использовать данные специальной категории для предотвращения дискриминации, вызванной ИИ:

1. Несколько типов организаций могут использовать данные для проверки того, различает ли система ИИ.
2. Сбор данных имеет символическую функцию.

### 6.3. Аргументы против исключения

Авторы выделяют три аргумента, против введения нового исключения, позволяющего использовать специальные категории данных для снижения рисков дискриминации. Эти аргументы включают:

1. Аргументы, связанные с простым хранением специальных категорий данных. Они указывают на потенциальные риски хранения таких данных и возможность их злоупотребления. Авторы предостерегают от возможного нарушения права на неприкосновенность частной жизни и защиту персональных данных.
2. Аргументы, связанные с новым использованием этих данных. Эти аргументы указывают на потенциальные негативные последствия расширенного использования специальных категорий данных, таких как возможное создание профилей и целевая маркетинговая реклама. Авторы подчеркивают необходимость баланса между предотвращением дискриминации и защитой прав на неприкосновенность частной жизни и свободу выражения.
3. Аргументы, указывающие на практические препятствия, которые делают исключение нежелательным в настоящее время. Эти аргументы обращают внимание на сложности и сложности реализации такого исключения в практическом плане. Авторы предупреждают о возможности недостаточного контроля и мер безопасности при использовании специальных категорий данных.

В целом, существуют различные аргументы как в пользу, так и против принятия исключения, которое позволило бы использовать специальные категории данных для предотвращения дискриминации со стороны систем искусственного интеллекта. Найти баланс между этими аргументами довольно сложно. В случае принятия такого исключения также требуются меры предосторожности для минимизации рисков и обеспечения соблюдения прав на неприкосновенность частной жизни и защиту персональных данных.

## 7. Возможные гарантии в случае принятия исключения

Предложение Европейской комиссии о Законе об искусственном интеллекте (Законе об ИИ) представляет некоторые возможности и гарантии в отношении использования данных специальной категории. В начале 2021 года Европейская комиссия представила предложение Закона об ИИ, в котором сформулировано исключение из запрета на обработку данных специальной категории.

Предлагаемое исключение определяется следующим образом: В той мере, в которой это строго необходимо для обеспечения мониторинга, обнаружения и исправления предвзятости в отношении систем искусственного интеллекта с высоким риском, поставщики таких систем могут обрабатывать специальные категории персональных данных, указанные в статье 9 Общего регламента по защите данных (GDPR). При этом требуется соблюдение надлежащих гарантий основных прав и свобод физических лиц, включая технические ограничения на повторное использование и использование самых современных мер безопасности и сохранения конфиденциальности, таких как псевдонимизация или шифрование, когда анонимность может существенно повлиять на цель обработки данных.

В предложенном положении предусмотрены различные гарантии, направленные на предотвращение злоупотребления данными специальной категории. Это включает технические ограничения на повторное использование данных, использование современных мер безопасности и сохранения конфиденциальности, а также требования к псевдонимизации или шифрованию для защиты анонимности в случаях, когда это необходимо для достижения цели обработки данных. Все эти гарантии направлены на обеспечение соблюдения основных прав и свобод физических лиц при обработке данных специальной категории в контексте систем искусственного интеллекта с высоким риском.

## 8. Заключение

В этой статье было рассмотрено, нужно ли общему регламенту по защите данных новое исключение из запрета на использование специальных категорий данных, чтобы организация могла смягчить дискриминацию со стороны искусственного интеллекта. Авторы наметили аргументы в пользу и против такого нового исключения.

Среди основных аргументов в пользу данного исключения были выделены следующие:

* Организации могут использовать данные специальной категории для проведения проверки систем искусственного интеллекта на предмет наличия дискриминации.
* Тестирование распознавания искусственного интеллекта может увеличить доверие потребителей к таким системам.

В свою очередь, основные аргументы против такого исключения включают в себя:

* Хранение личных данных, таких как этническая принадлежность, может рассматриваться как нарушение частной жизни.
* Существует риск неправильного использования таких данных или возможности утечки данных.
* Исключение может быть использовано для сбора специальных категорий данных для целей, не связанных с тестированием дискриминации искусственного интеллекта.
* Простое разрешение организациям собирать данные специальной категории не гарантирует, что они смогут эффективно устранить предвзятость в своих системах искусственного интеллекта. Аудит и устранение предвзятости в таких системах остаются сложными задачами.

Поэтому, несмотря на аргументы в пользу и против, внедрение такого исключения требует тщательного рассмотрения и необходимости применения соответствующих мер предосторожности для минимизации рисков и обеспечения соблюдения основных прав и свобод физических лиц.

# Ознакомительный обзор системы 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

Каждая ИТ-система имеет свои цели и задачи. Некоторые системы возникают из идей, другие — из желания проверить гипотезу. Некоторые разработки создаются с целью получения прибыли или удовлетворения потребностей клиентов или рынка.

Таким же образом была создана система RuSIEM. Первый заказчик компании нуждался в средстве для управления событиями информационной безопасности. Это произошло в 2014 году, когда были введены санкции против России. Практически все производители SIEM, представленные тогда в России, были из США, и в случае малейшего сомнения отказывались поставлять интеграторам. То же самое произошло и с заказчиком RuSIEM. Он обратился к нам, и мы предложили решение на основе комбинации открытых решений класса Log management, известных как ELK (Elasticsearch-Logstash-Kibana).

Однако изначальное решение имело свои недостатки. С помощью внесения изменений и доработок кода, добавления собственных модулей и расширения поддержки большого количества источников данных "из коробки", мы смогли устранить указанные проблемы и расширить набор возможностей системы RuSIEM.

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> – 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](https://www.azone-it.ru/sistema-upravleniya-informacionnoy-bezopasnostyu-siem/rusiem%20)  – Дата обращения 06.07.2023
5. Общий регламент по защите данных: [Электронный ресурс] – Режим доступа: <https://ru.wikipedia.org/wiki/%D0%9E%D0%B1%D1%89%D0%B8%D0%B9_%D1%80%D0%B5%D0%B3%D0%BB%D0%B0%D0%BC%D0%B5%D0%BD%D1%82_%D0%BF%D0%BE_%D0%B7%D0%B0%D1%89%D0%B8%D1%82%D0%B5_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85> – Дата обращения 06.07.2023