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 100301.043.007.01 ТЗ

Обучающемуся Емелиной Алине Анатольевне 4 курс, ИАИТ, 2 группа

Тема: Система мониторинга действий пользователя автоматизированной информационной системы

Исходные данные (или цель работы): разработка системы мониторинга действий пользователя автоматизированной информационной системы.

Перечень подлежащих исследованию, разработке, проектированию вопросов:

Наименование вопроса	Результаты освоения ОПОП
1.Постановка цели и задачи для ВКР, обзор литературных источников	ОК -1, ОК -3, ОК – 6.
2. Аналитический обзор и классификация угроз, связанных с действиями пользователя	ОК - 8, ОПК - 1
3. Аналитический обзор существующих систем мониторинга событий безопасности информационной системы	ОПК - 4, ПК -12
4. Анализ актуальных угроз предприятия	ОК - 4, ОК – 5, ПК – 5
5. Анализ действий пользователей предприятия	ОПК - 3, ОПК - 5, ПК -1, ПК - 15.
6. Составление правил и структурной схемы функционирования системы мониторинга действий пользователя в информационной системе	ОПК -2, ПК -10, ПК -11
7. Программная реализация системы мониторинга действий в автоматизированной информационной системе	ПК -2, ПК - 3, ПК-6, ПК-14.
8. Технико-экономическое обоснование разработки	ОК - 2, ОК - 9, ОПК -6, ПК -7.
9. Обеспечение безопасности жизнедеятельности	ОПК- 7, ПК – 4, ПК -13

Перечень презентационного материала:
1. Плакат «Аналитический обзор существующих систем мониторинга событий информационной системы»
2. Плакат «Анализ предприятия»
3. Плакат «Методика анализа действий пользователей»
4. Плакат «Анализ действий пользователей»
5. Плакат «Анализ корреляционной зависимости между отслеживаемыми параметрами в системе»
6. Плакат «Структурная схема и правила функционирования системы»
7. Плакат «Программная реализация системы мониторинга действий пользователя в автоматизированной информационной системе»
8. Плакат «Технико-экономическое обоснование разработки»

Нормоконтролер:

старший преподаватель Н.В. Андреева

(должность, ф.и.о. нормоконтролера)

Дата выдачи задания: «____» _____ 20__г.

Задание согласовано и принято к исполнению.

Руководитель:
Н.Е. Карпова___
(И. О. фамилия,)

Студент:
А.А. Емелина_____
(И. О. фамилия)

Зам. заведующего кафедрой «ЭСИБ», к.т.н., доцент
(должность, уч. степень, уч. звание)

ИАИТ, 2 группа
(факультет, группа)

_____
(подпись, дата)

_____
(подпись, дата)

Тема утверждена приказом по СамГТУ № _____ от "____"_____20___г.

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 Емелиной Алины Анатольевны
(фамилия, имя, отчество, курс, факультет, группа)

Тема: Система мониторинга действий пользователя автоматизированной информационной Системы
(полное название темы квалификационной работы, в соответствии с приказом об утверждении тематики ВКР)

	Этапы выполнения ВКР	Дата (срок) выполнения		Отметка о выполнении
		план	факт	
	Разработка структуры ВКР. Проведение литературного обзора	1.12.2020 - 20.01.2021	1.12.2020 - 20.01.2021	
	Сбор фактического материала (лабораторные, исследовательские работы и др.)	21.01.2021- 09.03.2021	21.01.2021- 09.03.2021	
	Подготовка рукописи ВКР	10.03.2021- 05.05.2021	10.03.2021- 05.05.2021	
	Доработка текста ВКР в соответствии с замечаниями научного руководителя	06.05.2021- 07.06.2021	06.05.2021- 07.06.2021	
	Предварительная защита квалификационной работы на кафедре	25.05.2021	25.05.2021	
	Ознакомление с отзывом научного руководителя	08.06.2021	08.06.2021	
	Подготовка доклада и презентационного материала	09.06.2021- 20.06.2021	09.06.2021- 20.06.2021	

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

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

Факультет автоматики и информационных технологий

Кафедра Электронные системы и информационная безопасность

ДОПУСТИТЬ К ЗАЩИТЕ

Заведующий кафедрой_____Скобелев П.О.

«___» _____ 20 г.

Выпускная квалификационная работа
СамГТУ 100301.043.007.02 ПЗ

Тема: Система мониторинга действий пользователя автоматизированной информационной системы

(полное название темы квалификационной работы, в соответствии с приказом об утверждении тем ВКР)

Обучающийся Емелина Алина Анатольевна 4 курс, ИАИТ, 2 группа

(фамилия, имя, отчество, курс, факультет, группа)

Руководитель работы _____ к.т.н., доцент Карпова Н.Е.

(должность, подпись, дата, фамилия, инициалы)

Нормоконтролер _____ старший преподаватель Андреева Н.В.

(подпись, дата, фамилия, инициалы)

Консультант _____ старший преподаватель Андреева Н.В.

(подпись, дата, фамилия, инициалы)

Консультант _____ д.т.н., профессор, Яговкин Н.Г.

(подпись, дата, фамилия, инициалы)

Самара 2021г.

РЕФЕРАТ

Пояснительная записка содержит 77 страниц, 13 иллюстраций, 17 таблиц, 1 приложение, 27 источников. Графический материал выполнен на 8 листах формата А1 и в презентации Microsoft PowerPoint.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, НЕЧЕТКИЕ ПРАВИЛА, ЭТАЛОН ПОВЕДЕНИЯ ПОЛЬЗОВАТЕЛЯ, НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП, КОЭФФИЦИЕНТ КОРРЕЛЯЦИИ, СИСТЕМА МОНИТОРИНГА, АУДИТ, ПОВЕДЕНЧЕСКИЙ АНАЛИЗ

Объект исследования: юридическая компания ООО «Юрдел». Результатом проектирования является разработка системы мониторинга действий пользователя в автоматизированной информационной системе.

В данной работе изложен анализ существующих систем мониторинга действий пользователя, на основании анализа показаны достоинства и недостатки данных систем. В практической части ВКР проанализированы актуальные угрозы предприятия, после чего составлен эталон действий пользователя в информационной среде предприятия на основе математического аппарата нечеткой логики. Произведен анализ корреляционной зависимости исследуемых параметров поведения пользователя, после чего были разработаны нечеткие правила для функционирования системы мониторинга действий пользователя в информационной системе. Итогом работы является разработка системы мониторинга действий пользователя для предприятия ООО «Юрдел».

Приведено технико-экономическое обоснование проекта, а также рассмотрены в опросы обеспечения безопасности жизнедеятельности.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Большинство преступлений, связанных с информационной безопасностью, совершается сотрудниками организаций. Это подтверждает опрос [28], согласно которому 90% организаций отмечают уязвимость перед внутренними угрозами.

Средства защиты информации можно разделить на:

1. Технические (аппаратные) – Это различные по типу устройства (механические, электромеханические, электронные и др.), которые на уровне оборудования решают задачи информационной защиты, например, такую задачу, как защита помещения от прослушивания.

2. Программные – включают программы для идентификации пользователей, контроля доступа, шифрования информации, удаления остаточной (рабочей) информации типа временных файлов, тестового контроля системы защиты

3. Организационные меры складываются из организационно-технических (подготовка помещений с компьютерами, прокладка кабельной системы с учетом требований ограничения доступа к ней и др.) и организационно-правовых (национальные законодательства и правила работы, устанавливаемые руководством конкретного предприятия). [23]

С растущим объемом информации, которая обрабатывается в электронном виде и передается между различными информационными системами (ИС) в сети Интернет, все большую актуальность имеют программные и аппаратные средства защиты информации.

В настоящее время существует значительное число систем, реализующих механизмы защиты информационных систем как от внешних, так и от внутренних угроз.

К таким системам относятся системы выявления вторжений (СВВ). Они делятся на системы, которые реагируют на уже известные угрозы (атаки) -

комплексные системы, и системы, которые осуществляют мониторинг и анализ действий пользователя в системе.

Системы, осуществляющие мониторинг, позволяют проводить идентификацию и аутентификацию пользователя и осуществлять анализ его действий, в том числе выявляя аномалий в его поведении. Они делятся на поведенческие и биометрические. Поведенческие системы позволяют обнаруживать подозрительное поведение, которое не соответствует типичным действиям пользователя в системе. Биометрические системы дают возможность распознавать пользователей по их физическим индивидуальным особенностям (отпечатки пальцев, голосу, кисти рук, ДНК и др.). Данные системы в основном применяются в СКУД (системах контроля и управления доступом), что позволяет злоумышленнику, получив доступ к системе, беспрепятственно ее использовать в своих целях. [8]

Поведенческие системы являются более гибкими, по сравнению с биометрическими, и позволяют анализировать действия пользователя в информационной среде, в том числе с точки зрения выявления ранее неизвестных аномалий поведения. [9]

Сложности, с которыми сталкиваются разработчики моделей, связаны с тем, что все методы, касаются описания поведения человека, которое плохо поддается формализации. [15] Поэтому для описания поведенческих особенностей человека адекватно использовать математический аппарат, который позволяет отобразить все многообразие и сложность поведения человека. Нечеткие множества и нечеткая логика позволяют учесть инвариантность поведения человека, описать конкретные действия пользователя в системе и учесть вероятностью несанкционированных действий в информационной среде. Важным преимуществом моделей реальных систем, построенных на основе нечеткой математики, является их большая гибкость и адекватность реальному миру, а также сравнительно с традиционными моделями более быстрое получение окончательного результата через специфическое построение и простоту используемых нечетких операций. [11]

Учитывая все вышеизложенное, **целью** данной работы является разработка системы мониторинга действий пользователя в информационной среде на основе использования математического аппарата нечеткой логики.

Задачи:

1) Аналитический обзор и классификация угроз, связанных с действиями пользователя.
2) Аналитический обзор существующих систем мониторинга событий безопасности информационной системы
3) Сбор статистических данных о поведении пользователя в информационной системе.
4) Составление правил и структурной схемы функционирования системы мониторинга действий пользователя в информационной системе
5) Программная реализация системы мониторинга действий в автоматизированной информационной системе
6) Технико-экономическое обоснование разработки
7) Обеспечение безопасности жизнедеятельности

1. АНАЛИТИЧЕСКИЙ ОБЗОР И КЛАССИФИКАЦИЯ УГРОЗ, СВЯЗАННЫХ С ДЕЙСТВИЯМИ ПОЛЬЗОВАТЕЛЯ

Организация обеспечения безопасности информации должна носить комплексный характер и основываться на глубоком анализе возможных негативных последствий. При этом важно не упустить какие-либо существенные аспекты. Анализ негативных последствий предполагает обязательную идентификацию возможных источников угроз, факторов, способствующих их проявлению и, как следствие, определение актуальных угроз безопасности информации.[12]

В ходе такого анализа необходимо убедиться, что все возможные источники угроз идентифицированы, идентифицированы и сопоставлены с источниками угроз все возможные факторы (уязвимости), присущие объекту защиты, всем идентифицированным источникам и факторам сопоставлены угрозы безопасности информации. [20]

Носителями угроз безопасности информации являются источники угроз. В качестве источников угроз могут выступать как субъекты (личность) так и объективные проявления. Причем, источники угроз могут находиться как внутри защищаемой организации - внутренние источники, так и вне ее - внешние источники. Деление источников на субъективные и объективные оправдано исходя из предыдущих рассуждений по поводу вины или риска ущерба информации. А деление на внутренние и внешние источники оправдано потому, что для одной и той же угрозы методы парирования для внешних и внутренних источников могу быть разными.

Все источники угроз безопасности информации можно разделить на три основные группы:

1.Обусловленные действиями субъекта (антропогенные источники угроз).

2. Обусловленные техническими средствами (техногенные источники угрозы).

3. Обусловленные стихийными источниками. [20]

В данной работе будет реализована система реагирования на действия антропогенных источников угроз.

Рассмотрим основные источники антропогенных угроз. В качестве антропогенного источника угроз можно рассматривать субъекта, имеющего доступ (санкционированный или несанкционированный) к работе со штатными средствами защищаемого объекта. Субъекты (источники), действия которых могут привести к нарушению безопасности информации могут быть как внешние, так и внутренние.

Внешние источники могут быть случайными или преднамеренными и иметь разный уровень квалификации.

К ним относятся:

-криминальные структуры;

-потенциальные преступники и хакеры;

-недобросовестные партнеры;

-представители надзорных организаций и аварийных служб;

Внутренние субъекты (источники), как правило, представляют собой высококвалифицированных специалистов в области разработки и эксплуатации программного обеспечения и технических средств, знакомы со спецификой решаемых задач, структурой и основными функциями и принципами работы программно-аппаратных средств защиты информации, имеют возможность использования штатного оборудования и технических средств сети.

К ним относятся:

-основной персонал (пользователи, программисты, разработчики);

-представители службы защиты информации;

-вспомогательный персонал (уборщики, охрана);

-технический персонал (жизнеобеспечение, эксплуатация). [20]

Классификация угроз, исходящих от действий человека:

По видам возможных источников:

- угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, имеющими доступ к конфиденциальной информации.

- угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, не имеющих доступа к конфиденциальной информации, реализующие угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена;

По способам реализации:

• угрозы, реализуемые при подключении информационных ресурсов к сетям связи общего пользования;

• угрозы, реализуемые при подключении информационных ресурсов к сетям международного информационного обмена.

По виду несанкционированных действий:

-хищение (копирование) информации;

-уничтожение информации;

-модификация (искажение) информации;

-нарушение доступности (блокирование) информации;

-отрицание подлинности информации;

-навязывание ложной информации. [18]

Отметим, что подавляющее большинство компаний чувствует уязвимость пред источниками внутренних угроз.

Отчет об угрозах инсайдеров от Crowd Research Parthners показал, что 90 % организаций чувствуют себя уязвимыми со стороны внутренних угроз.

Основные факторы риска включают в себя большое количество пользователей с чрезмерными правами доступа (37%), растущее число устройств с доступом к конфиденциальным данным (36%). Генеральный директор и основатель Cybersecurity Insiders Холгер Шульц считает, что это связано с тем, что в компании либо инсайдеры устраиваются на работу со злонамеренным умыслом, либо источником угроз могут выступать сотрудники, которые обладают доступом к большим объемам конфиденциальной информации компании. Системы СВВ помогают определять такого рода угрозы и не допускать разглашения инсайдерской (конфиденциальной) информации [28].

Так как по статистике большое количество преступлений, связанных с информацией, совершают сотрудники организаций, особенно важным и актуальным вопросом является мониторинг действий пользователя в информационной среде. Для создания такой системы, разработчики определяют перечень отслеживаемых параметров, в каждом параметре на основе статистических данных, либо оценок экспертов определяется эталонное поведение пользователя, и в случае отклонения от эталонного поведения, в системе будет генерироваться событие информационной безопасности, а затем будет происходить информирование системного администратора о возможной угрозе.

Перечень отслеживаемых параметров очень обширен.

Для уменьшения рисков утечки служебной информации необходимо применять следующие методы:

Приведены следующие методы:

-Мониторинг локальных действий,

-Мониторинг времени работы пользователя

-Мониторинг доступа к директориям

-Мониторинг использования съемных устройств

-Мониторинг использования программ удаленного администрирования

-Мониторинг клавиатуры,

-Сохранение в буфер-обмена всей информации, которая была скопирована

-Сохранение всех действий с файлами, сохранение набора профилей и переписок.

Также важным компонентом для разработки эффективной системы обнаружения вторжений в критическую инфраструктуру являются наборы данных, характеризующие различные виды атак (в т ч. Эксплуатаций критических уязвимостей), а также анализ исходящего сетевого трафика. [14]

Методы мониторинга:

-анализ эксплуатаций уязвимостей

- анализ ресурсов, к которым обращается пользователь

-анализ входящих соединений, с потенциально – опасных ресурсов.

В [26] проводится глубокий сравнительный анализ различных наборов данных, полученных в результате мониторинга работы промышленных систем управления на различных уровнях. В данной работе анализируется поведение пользователя в корпоративных сетях, нам также необходимо исследовать из каких основных компонентов складывается безопасность Active Directory, данная информация необходима для составления эталонного поведения пользователя. Doug White говорит о безопасности Active Directory. Он выделяет три компонента в области обеспечения безопасности AD: физический, логический, аудит. Физическая безопасность является отправной точкой для разработки хороших политик безопасности AD. На очень детальном уровне важно понимать, какие существуют ресурсы, кто может получить доступ к этим ресурсам и какие устройства имеют надежный доступ. Логический предполагает оценку угроз, которые исходят не от конкретной физической угрозы, а от других компьютеров, привилегий и отдельных лиц в домене или лесу. [26]

2. АНАЛИТИЧЕСКИЙ ОБЗОР СУЩЕСТВУЮЩИХ СИСТЕМ МОНИТОРИНГА СОБЫТИЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Одной из главных сложностей в защите АСУ ТП от деструктивных информационных воздействий является наличие большого количества векторов атаки, которые различаются реализацией в зависимости от выбранного для атаки уровня. Однако существующие объективные сложности не означают, что нужно отказываться от главной цели — обеспечения безопасного и непрерывного функционирования информационно-телекоммуникационных систем и сетей в составе АСУ ТП.

Выделяются основные задачи киберзащиты в АСУ ТП:

-выявление и блокирование угроз безопасности системы и их источников.

-обеспечение высокого уровня защищённости от несанкционированной и деструктивной активности, что касается как самой АСУ ТП, так и её межсетевого взаимодействия с корпоративной сетью и внешними системами.

-обеспечение целостности, достоверности, доступности и своевременности поступления информации от управляемых технологических процессов на все уровни управления АСУ ТП.

Решение каждой из перечисленных задач подразумевает необходимость реализовать ряд требований, в целом сходных для различных сфер, в которых функционируют АСУ ТП. Это — требования к реагированию на инциденты нарушения безопасности, к обнаружению вторжений, к анализу защищённости, к защите информации при её передаче по каналам связи, к борьбе с вредоносным программным кодом и другим процессам. На зарубежном и отечественном рынке представлено некоторое количество средств защиты информации, рассмотрим некоторые из них. [24]

1.Производимый компанией «Уральский центр систем безопасности» комплекс DATAPK, является основой для системы оперативного мониторинга и контроля защищённости АСУ ТП, архитектура которой разрабатывалась с

целью выявлять предпосылки реализации угроз и не допускать возникновения инцидентов в сфере информационной безопасности.

В части выявления угроз и предотвращения инцидентов DATAPK автоматизирует процесс санкционирования изменений, внесённых в конфигурацию АСУ ТП, автоматически выявляет и визуализирует отклонения текущей конфигурации от эталонной, проверяет соответствие АСУ ТП установленным техническим требованиям по обеспечению безопасности, документирует процедуры и результаты контроля в виде отчётов с информацией о выявленных несоответствиях. Также он способен собирать события безопасности с компонентов системы, анализировать события безопасности и выявлять признаки компьютерных инцидентов, периодически выполнять поиск уязвимостей в компонентах АСУ ТП.

Режимы работы DATAPK может функционировать в одном из трёх режимов, различающихся объёмом собираемых сведений и степенью влияния на компоненты АСУ ТП.

Пассивный мониторинг. Особенностью этого режима является отсутствие прямого влияния на компоненты АСУ ТП: комплекс взаимодействует с системой в одностороннем порядке, сбор событий возможен только в том случае, если её компоненты настроены на самостоятельную отправку событий, при которой не требуется подтверждение их получения со стороны сервера (с помощью механизмов Syslog или SNMP).

Активный мониторинг. Он предполагает двусторонний обмен данными с использованием штатных механизмов (WinRM, RPC и т.д.).

Сканирование защищённости. Этот режим оказывает наиболее значительное влияние на работу компонентов АСУ ТП с целью выявления ошибок безопасности в них. В первую очередь предполагается его использование для проведения технологических работ, например на этапе развёртывания АСУ ТП или в рамках выполнения плановых мероприятий по поиску уязвимостей.

Преимущества:

-Комплексный анализ данных из различных источников (сетевой трафик, конфигурации, события).

-Определение текущего состава компонентов АСУ ТП, выявление несанкционированных изменений и существующих уязвимостей, оценка выполнения установленных требований по ИБ.

- Обнаружение компьютерных атак в технологической сети АСУ ТП, выявление сетевых аномалий.

-Идентификация, проверка подлинности и контроль доступа субъектов к системе и к отдельным функциям DATAPK.

-Защита архивных файлов, параметров настройки средств защиты информации и ПО, а также иных данных, не подлежащих изменению в процессе обработки информации.

Недостатки:

-Громоздкий пользовательский интерфейс

-Отсутствие простого варианта полного развёртывания DATAPK с помощью пошагового мастера.

-Недоступность через веб-интерфейс тонкой настройки DATAPK в части добавления, например, поддерживаемых протоколов и настройки ряда параметров комплекса (необходимо использовать внешние конфигурационные файлы).

-стоимость данной системы в районе 1 500 000 миллиона рублей, а также постоянное обслуживание и обновление данной системы также будет обходиться примерно в 500 000 рублей, ежегодное обновление лицензии в районе 1 000 000 миллиона рублей. [21]

2.Symantec DLP Suite - комплексное решение для обнаружения, контроля и защиты конфиденциальной информации от утечки, независимо от места хранения и способа использования.

Осуществляет:

-Поиск мест хранения и анализ конфиденциальных данных хранящихся на портативных и настольных компьютерах, на серверах, в репозиториях баз данных, на SharePoint серверах и любых других сетевых ресурсах организации

-Контроль за расспространением информации

-Препятствует распространению конфиденциальных данных через корпоративные ЦОДы, клиентские системы, удаленные офисы и компьютеры конечных пользователей

-Предотвращение утечки данных

-Контролирует инциденты, связанных с передачей данных на компьютерах пользователей: отправка писем по электронной почте, мгновенные сообщения, публикации корпоративных данных в интернете, копирование данных на съемные устройства, вывод на печать, передача по факсу, функции копирования и вставки

-Универсальные политики и проактивная защита от утечки конфиденциальных данных за пределы организации фиксирует, предупреждает и автоматически блокирует любые нарушениях внутренних бизнес-процессов способных привести к утечке.

Достоинства:

- Большое количество методов для анализа: контентный, цифровые отпечатки, автоматическое обучение, анализ контекста, гибридный анализ.

- Многоуровневая защита инфраструктуры: функциональный агент, высокопроизводительные сетевые компоненты, защита многих хранилищ.

- Возможность масштабирования системы для обеспечения функционирования в сложных высоконагруженных инфраструктура.

- Поддержка большого числа сетевых протоколов для перехвата и анализа данных.

Недостатки:

- нет возможности лингвистического анализа

-отсутствие возможности отслеживать мессенджеры

-высокая стоимость (примерно 3 000 000 рублей), ежегодное продление лицензии в районе 1 200 000 рублей, а также необходимость большого количество специалистов, которые будут отвечать за эксплуатацию системы.
-сложна в установке. [27]

3. FortiSIEM представляет собой комплексное и масштабируемое корпоративное решение, обеспечивающее охват сети от IoT до облака и включающее в себя запатентованные аналитические инструменты, которые обеспечивают эффективное управление сетевой безопасностью и производительностью в режиме реального времени.
Основные возможности FortiSIEM:
-Комплексное средство анализа состояния сети в режиме реального времени.
-Высокая производительность и скорость анализа событий в режиме реального времени.
-Большое число правил корреляции и генерируемых отчетов, доступных при внедрении продукта из коробки.
-Большое число протоколов интеграции со сторонними устройствами и системами.
Недостатки:
-Отсутствие русской локализации.
-Отсутствует поддержка подключения к ФинСерт или ГосСОПКА (актуально для отечественного рынка).
-Сложность в обслуживании и внедрении
-Высокая стоимость около 2 млн. рублей, ежегодное продление лицензии в районе 1 150 000 рублей [22]

Стоит отметить, что в основе разрабатываемых правил реагирования на различные отслеживаемые параметры лежат математические модели, к таким моделям относятся:
-модели принятия решения с привлечением экспертов, основанные на теории вероятности;

-модели оперативного контроля с применением математической статистики;
-модели, описывающие схемы и потоки в информационной системе на основе теории графов;
-модели, основанные на использовании нечетких множеств;
-методы раннего обнаружения внутреннего нарушителя информационной безопасности с применением сетей Байеса;
-системы, основанные на нейронных сетях [7,13,17].

Отметим, что рассматриваемое нами предприятие имеет небольшой бюджет, а также определенные задачи, приоритетной целью является мониторинг за действиями пользователя по определенным параметрам.

Для описания поведенческих особенностей человека адекватно использовать математический аппарат, который позволяет отобразить все многообразие и сложность поведения человека. Нечеткие множества и нечеткая логика позволяют учесть инвариантность поведения человека, описать конкретные действия пользователя в системе и учесть вероятностью несанкционированных действий в информационной среде. Важным преимуществом моделей реальных систем, построенных на основе нечеткой математики, является их большая гибкость и адекватность реальному миру, а также сравнительно с традиционными моделями более быстрое получение окончательного результата через специфическое построение и простоту используемых нечетких операций. [10]

3. РАЗРАБОТКА СИСТЕМЫ

3.1 Описание предприятия и служебной информации.

Объектом данной ВКР является организация ООО «ЮРДЕЛ», данное предприятие оказывает юридические услуги населению на коммерческой основе.

Таблица 1 - Аппаратные средства, используемые в ООО «ЮРДЕЛ».

Наименование	Характеристика	Количество
АРМ Сотрудников	ОС – Windows 10, АВПО Kaspersky End-point Security	30
Контроллер домена	ОС – windows Server 12	1
Сетевой маршрутизатор	Cisco ASA C891F-K9	3
СУБД	Microsoft SQL Server	1
Межсетевой экран	Cisco Firepower 1010 Security Appliance	1

Защищаемая информация на предприятии:

-персональные данные клиентов (в т.ч данные, охраняемые законом ФЗ от 31.05.2002 № 63 –ФЗ (ред. От 31.07.2020) «Об адвокатской деятельности и адвокатуре в Российской Федерации») [1]

-персональные данные сотрудников

-данные о деятельности Компании (планах развития, партнерах компании, финансах)

Отметим, что необходимость внедрения системы анализа действий пользователя в информационной среде, в первую очередь, обуславливается тем, что сотрудники данного предприятия работают с персональными

данными граждан при оказании юридических услуг, утечка персональных данных клиентов может привести к потери репутации компании, финансовому ущербу, а также нарушению таких законов, как

-Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ (последняя редакция) [2]

- «Об адвокатской деятельности и адвокатуре в Российской Федерации» 31.05.2002 № 63 –ФЗ (ред. От 31.07.2020). [1]

В случае нарушения этих законов, ответственность понесут как руководители компании, так и сотрудники, допустившие нарушение. Утечка информации составляющую Коммерческую тайну может также привести к потери репутации компании, финансовому ущербу.

Поэтому на данном предприятии существует необходимость контролировать действия пользователей в информационном пространстве и оповещать администратора безопасности в том случае, если они могут нанести вред информационной системе. Поэтому обнаружение подозрительного и аномального (опасного) поведения пользователей является важной и актуальной задачей.

Под подозрительным и аномальным повелением будем понимать активность пользователей, не связанную с рабочими задачами, которая может привести к утечке или модификации информации компании.

До настоящего момента на предприятии поставленная задача решалась с помощью предустановленных средств защиты (KasperskyAnti-Virus, Firewall операционной системы). Несмотря на используемые способы защиты, не все вредоносные действия пользователей оказывались вовремя обнаруженными и предотвращенными в реальном режиме времени. Эта ситуация привела к необходимости разработки автоматизированной системы мониторинга и анализа действий пользователей информационной системы предприятия.

Перечень необходимых параметров для отслеживания определяется начальником службы информационной безопасности компании, исходя из актуальных угроз безопасности предприятия.

Актуальными угрозами для предприятия считаются:

- **Угроза несанкционированного копирования защищаемой информации**

Описание угрозы**:** Угроза заключается в возможности неправомерного получения нарушителем копии защищаемой информации путём проведения последовательности неправомерных действий, включающих: несанкционированный доступ к защищаемой информации, копирование найденной информации на съёмный носитель (или в другое место, доступное нарушителю вне системы).

Данная угроза обусловлена слабостями механизмов разграничения доступа к защищаемой информации и контроля доступа лиц в контролируемой зоне.

Реализация данной угрозы возможна в случае отсутствия криптографических мер защиты или снятия копии в момент обработки защищаемой информации в нешифрованном виде

Объект воздействия**:** Объекты файловой системы

Последствия реализации данной угрозы: Нарушение конфиденциальности [19]

-**Угроза несанкционированного удаления защищаемой информации**

Описание угрозы**:** Угроза заключается в возможности причинения нарушителем экономического, информационного, морального и других видов ущерба собственнику и оператору неправомерно удаляемой информации путём осуществления деструктивного программного или физического воздействия на машинный носитель информации.

Данная угроза обусловлена недостаточностью мер по обеспечению доступности защищаемой информации в системе, а равно и наличием уязвимостей в программном обеспечении, реализующим данные меры.

Реализация данной угрозы возможна в случае получения нарушителем системных прав на стирание данных или физического доступа к машинному носителю информации на расстояние, достаточное для оказания эффективного деструктивного воздействия

Объект воздействия**:** объекты файловой системы

Последствия реализации данных угроз**:** Нарушение доступности [19]

-Угроза несанкционированной модификации защищаемой информации

Описание угрозы: гроза заключается в возможности нарушения целостности защищаемой информации путём осуществления нарушителем деструктивного физического воздействия на машинный носитель информации или деструктивного программного воздействия (в т.ч. изменение отдельных бит или полное затирание информации) на данные, хранящиеся на нём.

Реализация данной угрозы возможна в случае получения нарушителем системных прав на запись данных или физического доступа к машинному носителю информации на расстояние, достаточное для оказания эффективного деструктивного воздействия

Объект воздействия: Объекты файловой системы

Последствия реализации данных угроз: Нарушение целостности [19]

-Угроза восстановления и/или повторного использования аутентификационной информации

Описание угрозы: Угроза заключается в возможности доступа к данным пользователя в результате подбора (например, путём полного перебора или перебора по словарю) аутентификационной информации дискредитируемой учётной записи пользователя в системе, а также путём перехвата и повторного использования хэша пароля, для восстановления сеанса.

Данная угроза обусловлена следующими недостатками:

значительно меньшим объёмом данных хеш-кода аутентификационной информации по сравнению с ней самой (время подбора хеш-кодов меньше времени полного перебора аутентификационной информации);

слабостями алгоритма расчёта хеш-кода, допускающими его повторное использование для выполнения успешной аутентификации.

Реализация данной угрозы возможна с помощью специальных программных средств, а также в некоторых случаях – «вручную»

Объект воздействия: Системное программное обеспечение, микропрограммное обеспечение, учётные данные пользователя

Последствия реализации данных угроз**:** Нарушение конфиденциальности [19]

-Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации

Описание угрозы**:** Угроза заключается в пропуске и/или значительной временной задержке определения (выявления) событий безопасности информации, что приводит к отсутствию реакции на попытки несанкционированного доступа в информационную (автоматизированную) систему, на внедрение вредоносных программ.

Данная угроза обусловлена некорректной настройкой компонентов информационной (автоматизированной) системы и/или средств защиты информации, а также отсутствием таких компонентов и/или средств защиты информации.

Реализация данной угрозы возможна при отсутствии мер защиты, связанных с мониторингом, сбором и анализом данных о событиях информационной безопасности (отсутствием мер регистрации событий безопасности)

Объект воздействия**:** Программное обеспечение, каналы связи (передачи) данных

Последствия реализации данных угроз**:** Нарушение целостности, Нарушение доступности. [19]

Заметим, что данные описание данных угроз соответствует описанию угроз банка данных угроз безопасности информации ФСТЭК.

Таким образом, были сформированы требования к построению системы анализа:

1) Система должна поддерживать ОС Windows 7 и выше

2) Система должна оповещать администратора безопасности о произошедшем инциденте не позднее, чем через 5 минут от наступления подозрительного или аномального события

3) Должен быть разработан эталон легитимных действий пользователя

4) Система должна быть экономически эффективной

Для разработки такой системы на первом шаге было проведено исследование поведения пользователей этой системы с использованием математического аппарата нечеткой логики и выделение нормального (безопасного), а также подозрительного и аномального поведения.

На втором шаге были разработаны нечеткие правила функционирования данной системы.

На третьем шаге была разработана структура и система мониторинга и анализа действий пользователя в информационной среде и проведена ее апробация.

3.2 Анализ действий пользователей предприятия

В данной ВКР для определения нормального, подозрительного и аномального поведении пользователей был проведен анализ трех параметров информационной системы предприятия ООО «ЮРДЕЛ».

К этим параметрам были отнесены: количество неуспешных попыток входа в систему, время входа в информационную систему, доступ к критичным директориям. Изучение данных параметров позволяет осуществлять комплексный анализ действий пользователя и своевременно реагировать на аномальное поведение, связанное с несанкционированным доступом.

В рамках исследования были проанализированы журналы событий за 2 месяца 30 компьютеров, расположенных на предприятии. Анализ был проведен

с использованием метода экспертных оценок и метода относительных частот (прямого группового метода). В качестве экспертов были привлечены 9 человек, являющиеся работниками отдела информационной безопасности и администрирования предприятия, а также специалистами в области информационной безопасности.

При анализе выделенных параметров были определены их функции принадлежности. В общем случае степень принадлежности $\mu_A(x)$ – это некоторая не вероятностная субъективная мера нечеткости, определяемая в результате опроса экспертов о степени соответствия элемента x понятию, формализуемому нечетким множеством A. То есть функция принадлежности $\mu_A(x) \in [0, 1]$ ставит в соответствие каждому числу $x \in X$ число из интервала [0,1], характеризующее степень принадлежности решения к подмножеству A. [10]

Первым параметром является анализ Доступа к критичным директориям.

Основная цель отслеживания данного параметра: выявить успешные обращения к папкам с критичной информацией пользователем, не имеющих туда прав.

Подобная активность может быть целенаправленной попыткой сбора, либо модификации критичной информации, либо доступ может осуществляться из – под скомпрометированной УЗ.

При анализе параметра «Доступ к критичным директориям» было сформировано нечеткое множество A, соответствующее понятию «доступ до директории системе безопасен». Было выявлено 13 основных используемых директорий и сформировано множество X – множество используемых директорий, где объекты xi – конкретные директории, которые посещает пользователь во время работы в системе (см. таблицу 2).

Для определения того, является ли использование каждого конкретной директории нормальным или подозрительным поведением, экспертам предъявлялись различные наименования используемых директорий в системе xi и каждому из них задавался вопрос: с какой степенью уверенности $0 \leq \mu_A(x) \leq 1$

эксперт считает, что посещение данной директории в системе безопасно. Результаты экспертных оценок приведены в таблице 3.

Таблица 2 - Перечень основных используемых директорий.

x_i	Директория
x_1	"C:\Windows\Logs"
x_2	"C:\Windows\System"
x_3	"C:\Windows\База данных клиентов
x_4	"C:\Windows\персональные данные сотрудников
x_5	"C:\ProgramFiles"
x_6	"C:\Users*\Documents\Загрузки
x_7	\""C:\Documents and Settings\worker\Текущие клиенты
x_8	""C:\Documents and Settings\worker\Мои клиенты"
x_9	"C:\Windows\карточка сотрудника
x_{10}	""C:\Documents and Settings\worker\Командировки"
x_{11}	"C:\Users\ шаблоны документов"
x_{12}	"C:\Documents and Settings\ "
x_{13}	"C:\ "

На основании ответов экспертов по методу относительных частот (1) был проведен расчет $\mu_A(x)$.

$$\mu_A(x) = \frac{n_1}{n_1+n_2} = \frac{n_1}{m}, \quad (1)$$

где m – общее число экспертов, n1 – эксперты, которые на вопрос о принадлежности элемента $x \in X$ нечеткому множеству A отвечали положительно, n2 = m-n1 – эксперты, отвечавшие на этот вопрос отрицательно. Результат расчетов также приведены в таблице 3.

Таблица 3 - Результат экспертных оценок.

x	1	2	3	4	5	6	7	8	9	10	11	12	13
n1	1	1	2	3	4	5	6	7	8	8	8	9	9
n2	8	8	7	6	6	4	3	2	1	1	1	0	0
μA(x)	0.1	0.1	0.2	0.3	0.4	0.6	0.7	0.8	0.9	0.9	0.9	1.0	1.0

На основании данных в таблице 3 построим функцию принадлежности в аналитическом (2) и графическом виде (см. рисунок 1)

$$\mu_A(x) = \begin{cases} x_1, 0.1; \\ x_2, 0.1\ ; \\ x_3, 0.2; \\ x_4, 0.3; \\ x_5, 0.4; \\ x_6, 0.6; \\ x_7, 0.7; \\ x_8, 0.8; \\ x_9, 0.9; \\ x_{10}, 0.9; \\ x_{11}, 0.9; \\ x_{12}, 1; \\ x_{13}, 1. \end{cases} \quad (2)$$

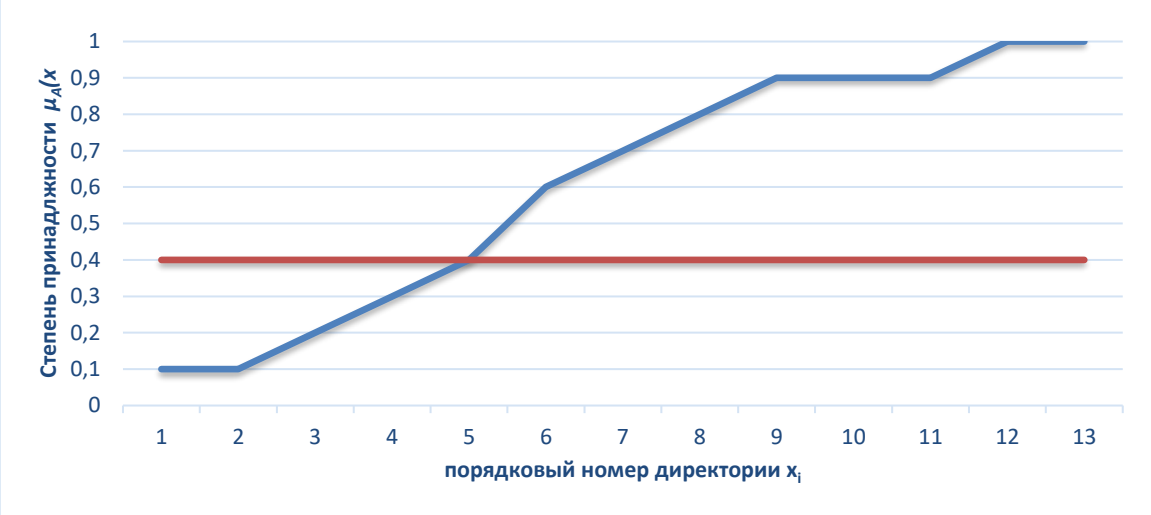

Рисунок 1 - Функция принадлежности в графическом виде для параметра «перечень основных используемых директорий»

На рисунке 1 видно, что аномальным поведением пользователя является посещение системных папок, а также папок, в которых хранятся персональные данные сотрудников, а также данные всех клиентов, к которым нет необходходимости постоянного доступа, так как текущие клиенты и клиенты конкретного юриста находятся в других директориях, данное поведение соответствует

условию $\mu_A(x) \leq 0.4$. Подозрительным поведением будем считать поведение, для которого $0.4 < \mu_A(x) \leq 0.6$.

Следующим отслеживаемым параметром является «время входа в информационную систему»

Основная цель отслеживания данного параметра: выявить компрометацию УЗ, несанкционированное использование определенных учетных записей.

При анализе параметра «Время входа в информационную систему» было сформировано нечеткое множество B, соответствующее понятию «временной интервал начала и окончания сессии пользователя безопасен». Определено 6 основных временных интервалов начала работы пользователя в системе и сформулировано множество T – множество временных интервалов начала сессии, где объекты ti – время, в которое пользователь посещает систему (см. табл.4).

Для определения того, является ли временной интервал начала сессии нормальным или подозрительным поведением, экспертам предъявлялись различные временные диапазоны входа и выхода пользователя из системы ti и каждому из них задавался вопрос: с какой степенью уверенности $0 \leq \mu_B(t) \leq 1$ эксперт считает, что данный временной интервал, обозначающий начало сессии пользователя безопасен. Результаты опроса сведены в таблице 5.

Таблица 4 - Время входа в систему

ti	Время (мин)
(t1)	08.10–10:30
(t2)	10.30–12.30
(t3)	12.30–13.30
(t4)	13.30–15.30
(t5)	15.30–17.50
(t6)	17:50-8:10

На основании ответов экспертов по методу относительных частот (3) был проведен расчет $\mu_B(x)$.

$$\mu_B(t) = \frac{n_1}{n_1+n_2} = \frac{n_1}{m}, \quad (3)$$

где m - общее число экспертов, n1 – эксперты, которые на вопрос о принадлежности элемента $t_i \in T$ нечеткому множеству B отвечали положительно, n2 = m-n1 – эксперты, отвечавшие на этот вопрос отрицательно. Результаты расчетов также приведены в таблице 4 для времени входа.

Таблица 5 - Результат экспертных оценок для времени входа в систему.

t	1	2	3	4	5	6
n_1	9	7	3	6	4	1
n_2	0	2	6	3	5	8
$\mu_B(t)$	1	0.8	0.3	0.6	0.4	0,1

На основании данных в таблице 5 построим функцию принадлежности в аналитическом (4) и графическом виде (рисунок 2).

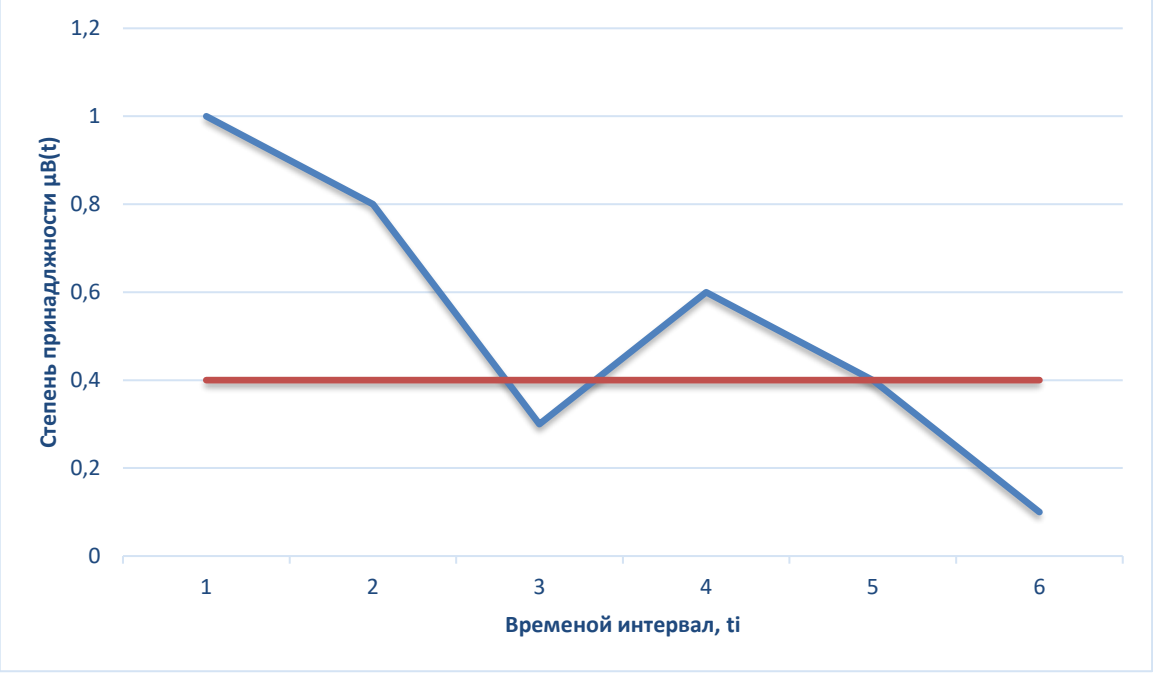

Рисунок 2 - Функция принадлежности в графическом виде для параметра «Время входа в систему».

$$\mu_B(t) = \begin{cases} t_1, 1; \\ t_2, 0.8\ ; \\ t_3, 0.3; \\ t_4, 0.6; \\ t_5, 0.4 \\ t_6, 0{,}1 \end{cases} \quad (4)$$

На рисунке 2 видно, что поведение, для которого $\mu_B(t) \leq 0.4$, можно считать аномальным. Можно отметить 2 варианта аномального поведения: время работы в обеденное время (t3) и сеансы работы в информационной системе в нерабочее время. Подозрительным поведением будем считать поведение, для которого $0.4 < \mu_B(t) \leq 0.6$

Следующим отслеживаемым параметром является «Количество неуспешных аутентификаций».

Основная цель отслеживания данного параметра: выявить попытки получить доступ к системе путем подбора паролей для критичных УЗ

При анализе параметра «Количество неуспешных аутентификаций» было сформировано нечеткое множество С, соответствующее понятию «количество неуспешных попыток аутентификации безопасно». Всего рассмотрено 5 интервалов количества неуспешных попыток аутентификации, регистрируемых в течение 20 минут и сформулировано множество К– множество, обозначающее неуспешные аутентификации, где объекты Кi – количество неуспешных аутентификаций (см. таблицу 6).

Для определения того, является ли количество неуспешных аутентификаций нормальным или подозрительным поведением, экспертам предъявлялись различное количество неуспешных попыток аутентификации из системы Кi и каждому из них задавался вопрос: с какой степенью уверенности $0 \leq \mu_c(к) \leq 1$ эксперт считает, что данное количество неуспешных аутентификаций безопасно.

Таблица 6 - Количество неуспешных аутентификаций.

K_i	Количество попыток, шт
($к_1$)	0-3
($к_2$)	4-6
($к_3$)	7-10
($к_4$)	11-13
($к_5$)	14–17

На основании ответов экспертов по методу относительных частот (5) был проведен расчет μ_c(к).

$$\mu_c(к) = \frac{n_1}{n_1+n_2} = \frac{n_1}{m}, \quad (5)$$

где m - общее число экспертов, n1 – эксперты, которые на вопрос о принадлежности элемента $k_i \in K$ нечеткому множеству B отвечали положительно, n2 = m-n1 – эксперты, отвечавшие на этот вопрос отрицательно. Результаты экспертных оценок приведены в таблице 7.

Таблица 7 - Результат экспертных оценок количества неуспешных аутентификаций.

k	1	2	3	4	5
n_1	9	7	5	3	1
n_2	0	3	4	6	8
μ_c(k)	1	0.8	0.55	0.3	0.1

На основании данных в табл. 6 построим функцию принадлежности в аналитическом (6) и графическом виде (рисунок 3).

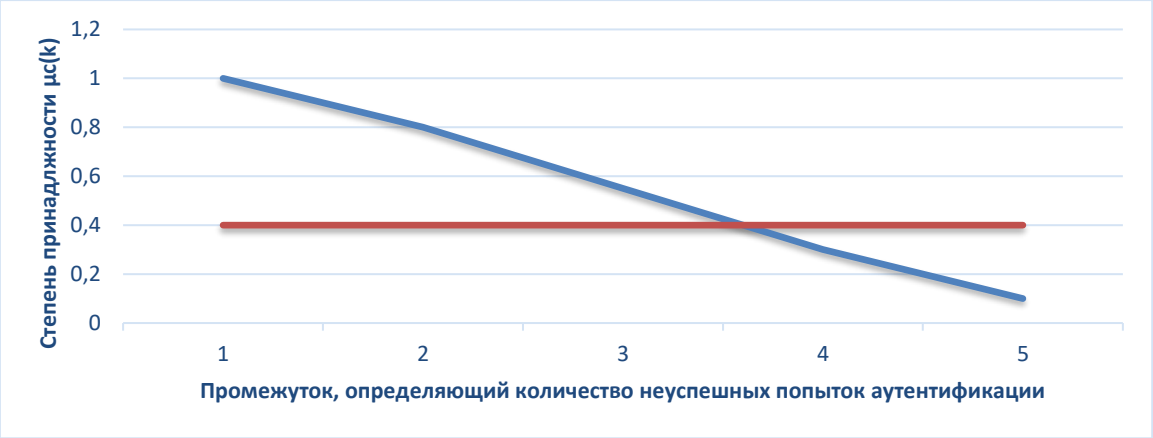

Рисунок 3 - Функция принадлежности в графическом виде для параметра «Количество неуспешных аутентификаций.

$$\mu_c(c) = \begin{cases} t_1, 1; \\ t_2, 0.8\ ; \\ t_3, 0.55; \\ t_4, 0.3; \\ t_5, 0.1 \end{cases} \quad (6)$$

На рисунке 3 видно, что поведение, для которого $\mu_c(k) \leq 0.4$, можно считать аномальным. Стоит отметить, что количество неуспешных аутентификаций превышающий порог в 11 можно считать аномальным. Подозрительным поведением будем считать поведение, для которого $0.4<\mu_c(k) \leq 0.6$

Используя полученные данные, найдем корреляционную зависимость, которую можно использовать при разработке нечетких правил для системы мониторинга действий пользователя в информационной среде.

Корреляционная зависимость — статистическая взаимосвязь двух или более случайных величин. Мы строили гипотезу о том, что действия пользователя в компьютерной системе взаимосвязаны друг с другом. Корреляционный анализ необходим для возможного уменьшения количества итераций при прохождении алгоритма, что в дальнейшем позволяет ускорить анализ действий пользователя в информационной среде. Для того чтобы исследовать статистическую взаимосвязь параметров, найдем математическую меру корреляции - коэффициент корреляции для исследуемых параметров. Для

исследования будем применять линейный коэффициент корреляции (коэффициент корреляции Пирсона) (7).

$$R=\frac{m*\sum_{i=1}^{m} xy-(\sum_{i=1}^{m} x)*(\sum_{i=1}^{m} y)}{(\sqrt{(m\sum_{i=1}^{m} x^2-(\sum_{i=1}^{m} x)^2)*(m\sum_{i=1}^{m} y^2-(\sum_{i=1}^{m} y)^2)}} \quad (7)$$

где m – число статистических наблюдений,

x и y – случайные величины.

Коэффициент Пирсона подходит при работе с выборкой, в которой 2 массива данных, он достаточно распространён, например, данный коэффициент применяется при расчете корреляции в программе Microsoft Excel.

Первыми параметрами исследуем количество неуспешных аутентификаций (массив x) и время входа в систему (массив y) таблица 8. В первый массив вносим значения экспертных оценок для количества неуспешных аутентификаций (таблице 7), во втором массиве мы соотносим значения экспертных оценок для количества неуспешных аутентификаций с результатом экспертных оценок для времени входа (таблица 5). Отметим, что, как правило, аномальное количество неуспешных аутентификаций могло происходить в ночное или обеденное время, также как и вход в это время является аномальным, что в целом может говорить о возможных аутентификациях после брутфорса.

Таблица 8 - Массивы данных для нахождения коэффициента корреляции.

Массив x. (Результат экспертных оценок для количества неуспешных аутентификаций)	Массив y. (Результат экспертных оценок для времени входа)
1	1
0,8	0,8
0,3	0,3
0,55	0,6
0,3	0,4
0.1	0.1

Определим коэффициент корреляции (8) и постоим диаграмму рассеивания (рисунок 4):

$$R=\frac{m*\sum_{i=1}^{m} xy-(\sum_{i=1}^{m} x)*(\sum_{i=1}^{m} y)}{(\sqrt{(m\sum_{i=1}^{m} x^2-(\sum_{i=1}^{m} x)^2)*(m\sum_{i=1}^{m} y^2-(\sum_{i=1}^{m} y)^2)}}=0{,}99, \quad (8)$$

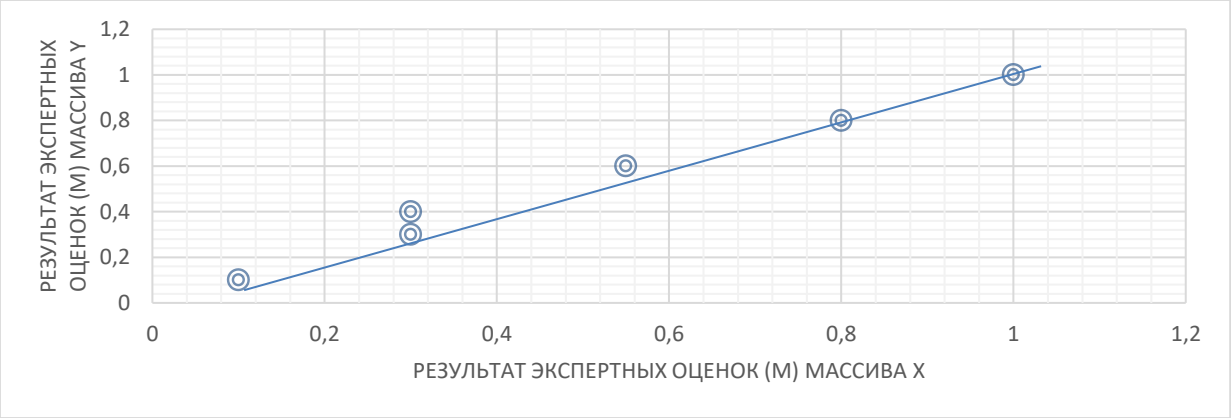

Рисунок 4 - Диаграмма рассеяния.

Корреляция – положительная линейная. Значительная корреляция между этими двумя параметрами говорит о том, что в данной выборке существует некоторая статистическая связь. На основании, данного исследования можем сделать вывод о том, что первым параметром, рассматриваемым в программе является количество неуспешных аутентификаций и если количество неуспешных аутентификаций аномально, то не имеет смысла оценивать все остальные параметры, необходимо как можно скорее передать оповещение специалисту по информационной безопасности.

Рассмотрим зависимость между временем входа (массив x) и используемыми директориями (массив y), таблица 9.

В первый массив вносим значения экспертных оценок для времени входа (таблица 5). Во второй массив заносим результаты экспертных оценок для используемых директорий, сопоставляя с временем их использования. (таблица 3). Отметим, что в нерабочее время использовались такие критичные директории, как "C:\Windows\Logs" и "C:\Windows\System", а в обеденное время фиксировался доступ директории C:\Windows\База данных клиентов.

Данный анализ говорит о том, что если произошла успешная аутентификация в нерабочее время, то с большей долей вероятности доступ будет производиться до критичной директории.

Таблица 9 - Массивы данных для нахождения коэффициента корреляции.

Массив x. (Результат экспертных оценок для времени входа)	Массив y. (Результат экспертных оценок для доступа до директории)
0,1	0,1
0,1	0,1
0,1	0,2
0,3	0,3
0,4	0,4
0,6	0,6
0,6	0,7
0,8	0,8
0,8	0,9
0,8	0,9
0,8	0,9
1.0	1.0
1.0	1.0

Определим коэффициент корреляции (9) и постоим диаграмму рассеивания (рисунок 5):

$$R=\frac{m*\sum_{i=1}^{m} xy-(\sum_{i=1}^{m} x)*(\sum_{i=1}^{m} y)}{(\sqrt{(m\sum_{i=1}^{m} x^2-(\sum_{i=1}^{m} x)^2)*(m\sum_{i=1}^{m} y^2-(\sum_{i=1}^{m} y)^2)}}=0{,}98 \quad (9)$$

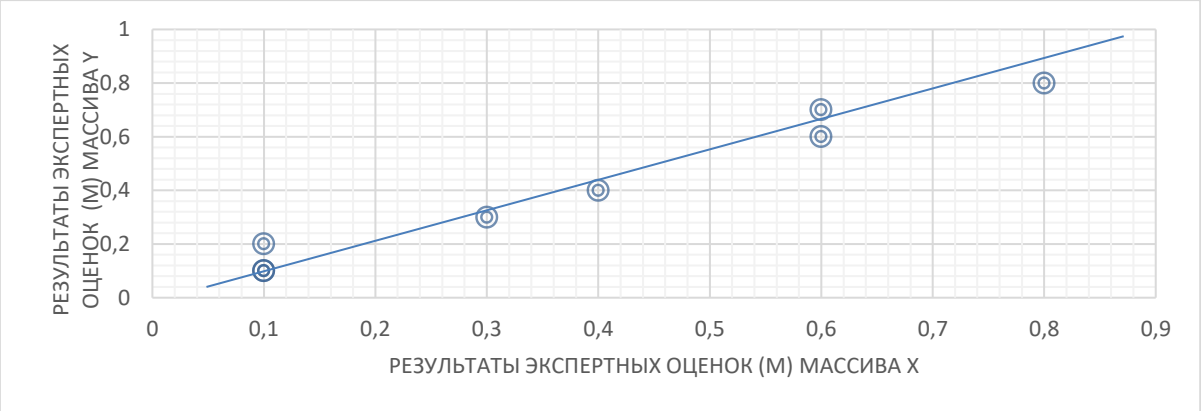

Рисунок 5 - Диаграмма рассеяния

Корреляция – положительная линейная. Значительная корреляция между этими двумя параметрами говорит о том, что в данной выборке существует некоторая статистическая связь. На основании, данного исследования можем сделать вывод о том, что вторым параметром, рассматриваемым в программе является время входа в систему и если время аномально, то не имеет смысла оценивать все остальные параметры, необходимо как можно скорее передать оповещение специалисту по информационной безопасности.

3.3 Составление правил и структурной схемы функционирования системы мониторинга действий пользователя в информационной системе

Для каждого параметра определим границы нормального, подозрительного и аномального поведения пользователя в информационной среде. Результаты представлены в таблице 10.

На основании полученных данных можно сделать следующие выводы.

Нормальным является поведение пользователя сотрудника, если он совершает следующие действия:

-количество неуспешных аутентификаций под УЗ сотрудника не превышает 6 попыток

- заходит в информационную среду в начале рабочего дня или после обеда;

- использует в своей работе директории, относящаяся к непосредственно его рабочим задачам.

Таблица 10 - Классификация поведения пользователя в информационной системе.

Поведение / Параметр	нормальное	подозрительное	аномальное
Использование директорий	$0.6 \leq \mu_A(x)$	$0.4 < \mu_A(x) < 0.6$	$\mu_A(x) < 0.4$
Время входа в информационную систему	$0.6 \leq \mu_B(t)$	$0.4 \leq \mu_B(t) < 0.6$	$\mu_B(t) < 0.4$
Количество неуспешных аутентификация	$0.55 < \mu_C(n)$	$0.3 < \mu_C(n) \leq 0.55$	$\mu_C(n) \leq 0.3$

Отличные от эталонного поведения действия будут рассматриваться как подозрительные или аномальные и требовать оповещения администратору, через почтовый модуль, детального изучения действий пользователя и блокировки пользователя в случае необходимости для предотвращения совершения несанкционированных действий.

На основании проведенного анализа были сформулированы нечеткие правила для разрабатываемой системы:

1.Если <использование директорий – аномальное> или <время входа в систему – аномальное> или <количество неуспешных аутентификаций – аномальное>, то <оповещение администратору и немедленная блокировка возможно скомпрометированной УЗ>.

2. Если <использование директорий – подозрительное> или <время входа в систему – подозрительное> или <количество неуспешных аутентификаций – подозрительно>, то <оповещение администратору>.

3. Если <использование директорий – нормальнон> или <время входа в систему – нормальное> или <количество неуспешных аутентификаций – нормальное>, то <действий не требуется>.

Исходя из полученных данных, сформулированных нечетких правил, а также эталона пользователя была разработана система анализа аномальных действий пользователя в информационной среде, структурная схема которой приведена на рисунке 6.

Работа системы требует накопления данных, на основании которых создается эталон нормального поведения пользователя. Затем в системе происходит сравнение поведения пользователя с эталоном по трем выделенным параметрам: доступ до директорий, времени входа в систему, количество неуспешных аутентификаций. При выявлении аномалий или подозрительного поведения система сигнализирует об отклонениях и, при необходимости, блокирует пользователя.

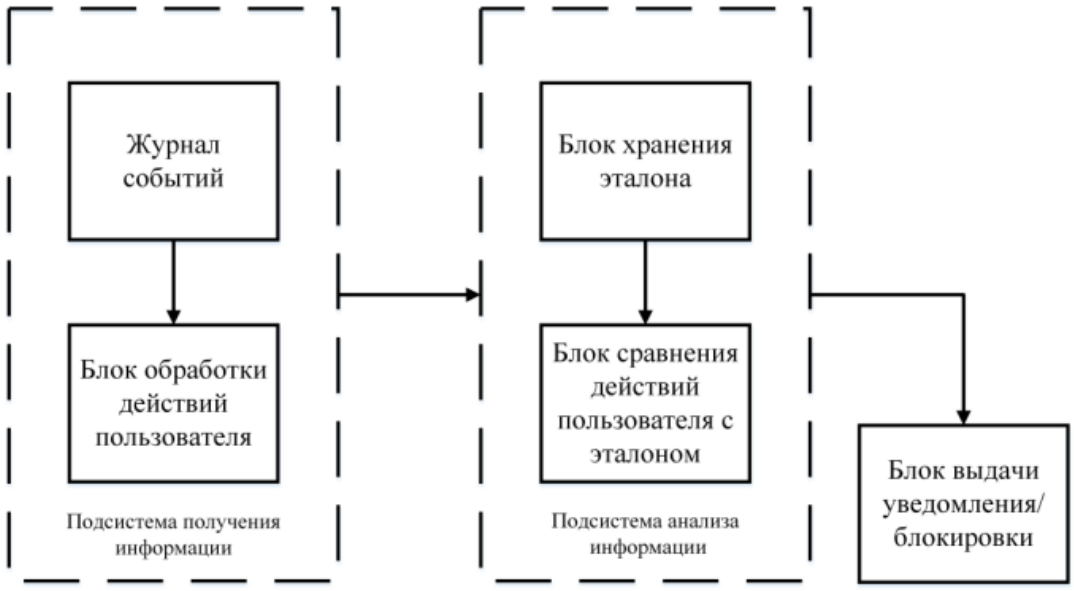

Рисунок 6 - Структурная схема системы анализа действий пользователя в информационной среде.

3.4 Программная реализация системы мониторинга действий в автоматизированной информационной системе

На основании проведенных исследований, составления правил функционирования системы была реализована программа система мониторинга действий пользователя в автоматизированной информационной системе, код для данной программы представлен в приложении А.

Ниже представлены скрины реализации интерфейса программы (рисунок 7, 8, 9, 10).

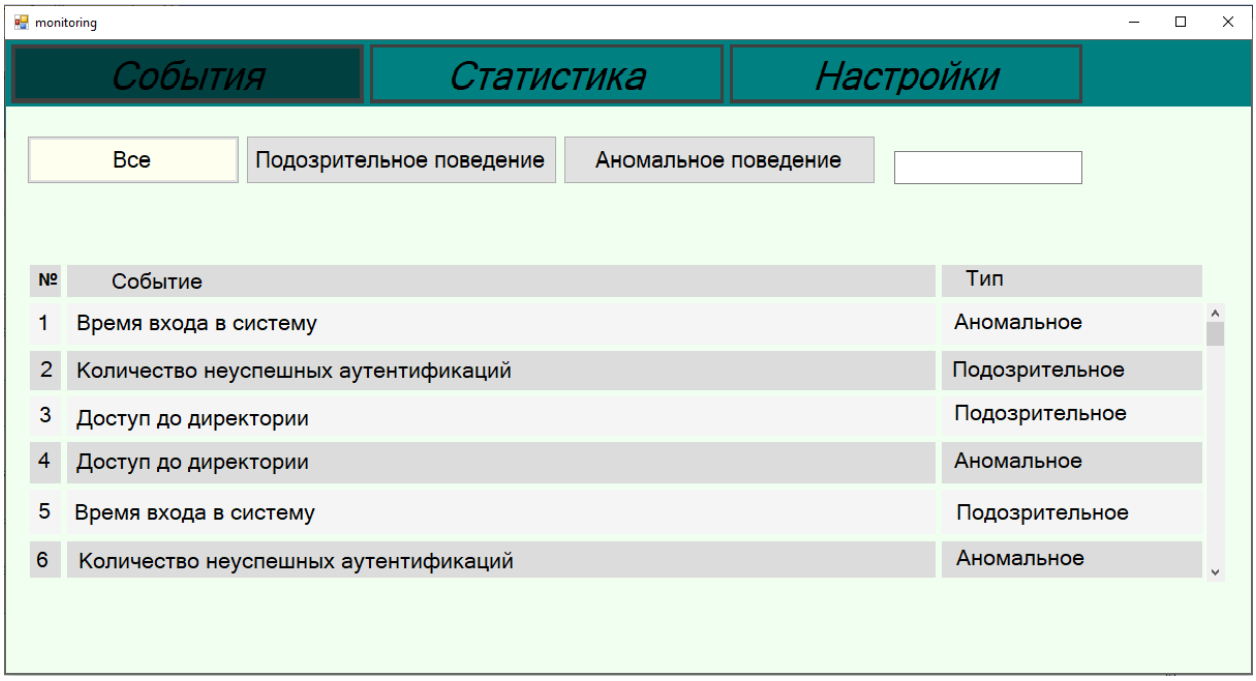

Рисунок 7 - Интерфейс программы.

В данной системе у администратора есть три вкладки «События, Статистика, Настройки».

Во вкладке «События» представлены все зарегистрированные системой события, с названием события и типом поведения. У администратора информационной безопасности есть возможность отсортировать события по типу поведения пользователя.

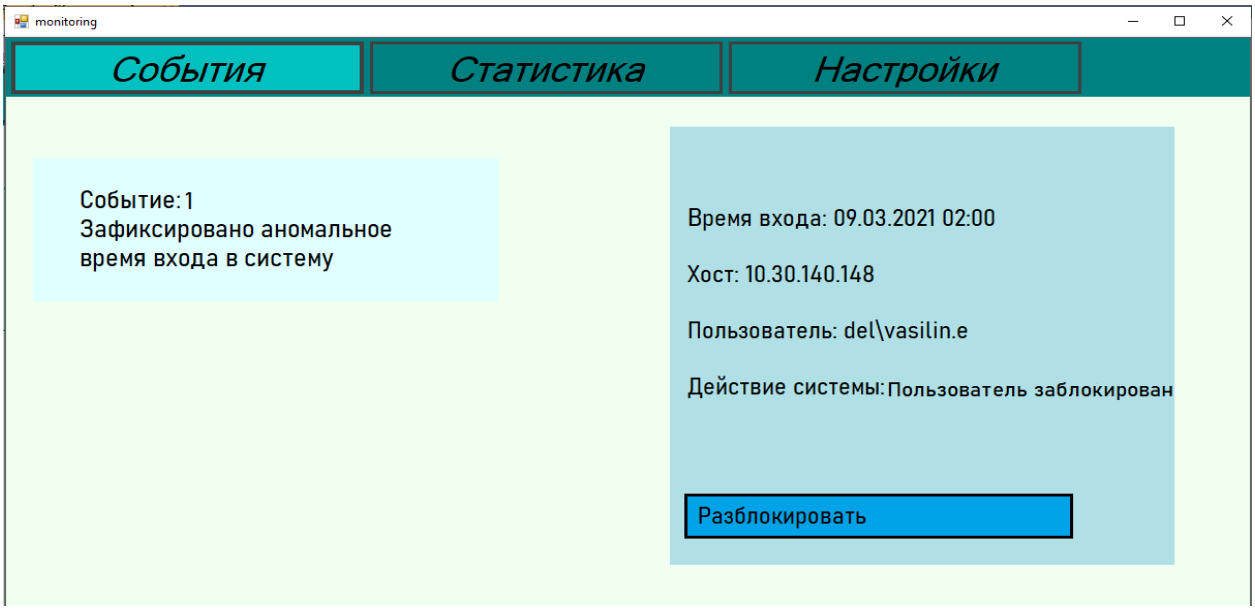

Рисунок 8 - Интерфейс программы.

При выборе зарегистрированного события информационной безопасности открывается полная информация о нем: номер, название, время регистрации, хост, пользователь и действия которая предприняла система. В случае если пользователь был заблокирован, у администратора безопасности есть возможность его разблокировать.

Рисунок 9 - Интерфейс программы.

При переходе во вкладку «Настройки» появляется возможность изменить значения границ функций принадлежности для каждого типа поведения.

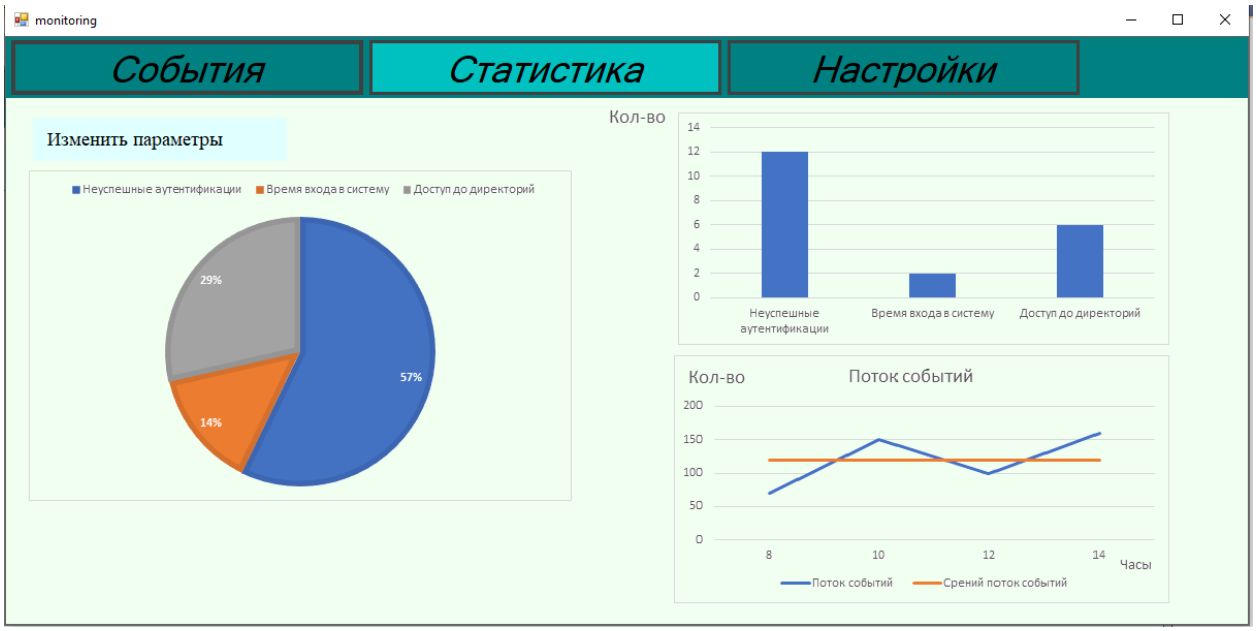

Рисунок 10 - Интерфейс программы.

Во вкладке «Статистика», можно увидеть статистику, собранную системой. В данном случае на круговой диаграмме представлено процентное соотношение сработок системы за весь период времени. На столбчатой диаграмме представлено количество сработок за неделю по каждому инциденты. На линейной диаграмме представлен поток событий за 6 часов, и выделен средний поток событий. Стоит отметить, что администратор может изменить временные интервалы за которые будут строиться диаграммы.

4. ТЕХНИКО-ЭКОНОМИЧЕСКОЕ ОБОСНОВАНИЕ РАЗРАБОТКИ

4.1Маркетинговое исследование

На основании проведенного сравнительного анализа существующих систем, выделим основные ключевые характеристики систем мониторинга.

1) Возможность сбора информации с различных источников
2) Количество ресурсов, затрачиваемых на эксплуатацию системы
3) Сложность внедрения
4) Возможность отслеживать большое количество параметров
5) Стоимость
6) Удобство интерфейса

Выставим баллы каждому параметру проанализированных систем от 1 до 10, где 10 самая высокая оценка, с точки зрения удобства для пользователей, 1 – самая низкая оценка.

Таблица 11. Маркетинговое сравнение.

Параметр / Система	DATAPK	FortiSiem	Symantec DLP Suite	Разрабатываемая система
Своевременное реагирования на угрозы	9	10	9	7
Количество ресурсов, затрачиваемых на эксплуатацию системы	4	2	3	9
Сложность внедрения	2	3	1	8
Возможность отслеживать большое количество параметров	8	8	7	5
Удобство интерфейса	7	8	7	6
Стоимость	1	2	1	

Так как система разрабатывается под небольшое предприятие с ограниченным количеством денежных и человеческих ресурсов, то ключевыми показателями при выборе системы для руководства предприятия являются, простота в эксплуатации и внедрении, стоимость, возможность отслеживать заданные параметры и удобства интерфейса. Стоимость данной системы будет рассчитана ниже. Однако мы уже можем отметить, что разрабатываемая система имеет преимущества по следующим параметрам: Сложность внедрения, количество ресурсов, затрачиваемых на эксплуатацию системы, также не сильно уступает и в удобстве интерфейса. На основании проведенного анализа, можно сделать вывод о том, что предприятие будет заинтересовано в такой разработке

4.2 Расчет затрат на реализацию проекта.

В данной работе предлагается разработка системы мониторинга действий пользователя в автоматизированной информационной системе.

Первая часть затрат связана с общими затратами (см. таблицу 12) на реализацию проекта, к данной категории относятся цена на электроэнергию, теплоэнергию и арендная плата.

Таблица 12 - Показатели энергозатрат ООО «Юрдел».

Показатель	Значение
$S_{пл}$, кв.м	500
$W_{тепл}$, руб/кв.м	73
$W_{э}$, руб/кВт*ч	4,3
$T_{разр.раб.}$,дней	28
$t_{дн}$,час	8
P, кВт	90

Общие затраты рассчитываем по формуле:

$$Зэн = Р * t_{дн} * Т_{разр.раб.} * Wэ + S_{пл} * (Т_{разр} / 365) * W_{тепл} \quad (10)$$

Р – суммарная мощность электроприборов, кВт;

$t_{дн}$ - продолжительность работы электроприборов в течение дня, час;

$Т_{разр.раб.}$ – продолжительность работ в рабочих днях;

Wэ – тариф на электроэнергию, руб/кВт*ч;

$W_{тепл}$ – тариф на тепловую энергию, руб/кв.м. в год.

$$З_{эн} = 90*8*28*4.3+ 500 *(28/365) *73 = 89488 \text{ рублей.} \quad (11)$$

Следующий вид затрат связан с заработной платой исполнителей данного проекта.

На этапе реализации данного проекта необходимо 3 вида специалистов.

1) Специалист по защите информации, который подготавливает описание задачи и описывает математическую модель.
2) 9 экспертов в области информационной безопасности, привлекаемые для опроса
3) 2 инженера – программиста, ответственных за программную реализацию проекта.

Заработная плата вычисляется по формуле:

$$З_{з/п} = З_{осн}(1+К_{доп})(1+К_{с.ф}.) \quad (12)$$

$З_{осн}$ - основная заработная плата специалистов, определяемая в зависимости от трудоёмкости и квалификации специалиста.

$К_{доп}$= 0,1 – коэффициент, учитывающий дополнительную зарплату.

$К_{с.ф}$ = 0,3 – коэффициент, учитывающий отчисления в социальные фонды.

Основная заработная плата вычисляется по формуле:

$$Зосн = З1_{час} * t1 + З2_{час} * t2 + З3_{час} * t3, \quad (13)$$

$З1_{час} =$ 220 р/час. Специалист отработал 18 дней по 8 часов (144 часа).

$З2_{час} =$ 150 р/час. Работали 9 специалистов, каждый из них по 3 часа. В сумме было отработано 27 часов.

$З3_{час} =$ 300 р/час. Работали 2 инженера – программиста 22 дня по 8 часов. В целом было отработано 352 часа.

Зосн = 220*144+150*27+300*352 = 141330 рублей.

$З_{з/п} =$ 141330 * (1+0,1) *(1+0,3) = 202 102 рублей.

Итого, затраты на разработку составляют:

$$Зр = З_{з/п} + З_{эн} \quad (14)$$

Зр = 202 102 рублей + 89488 рублей = 291590 рублей.

Затраты на реализацию проекта представлены на рисунке 12

Определим модель цены:

$$Ц = Зр+П+НДС, \quad (15)$$

где Зр – затраты на разработку

П – прибыль на разрабатываемую систему,

$$П = р*Зр/100 \quad (16)$$

НДС – налог на добавленную стоимость.

Рентабельность принимаем за 25%., налог на добавленную стоимость составляет 20%

П = 25 * 291590/100 = 72 898 рублей

НДС = 20* 291590/100 = 58 318 рублей

Ц = 291590 + 72 898 + 58318 = 422 806 рублей.

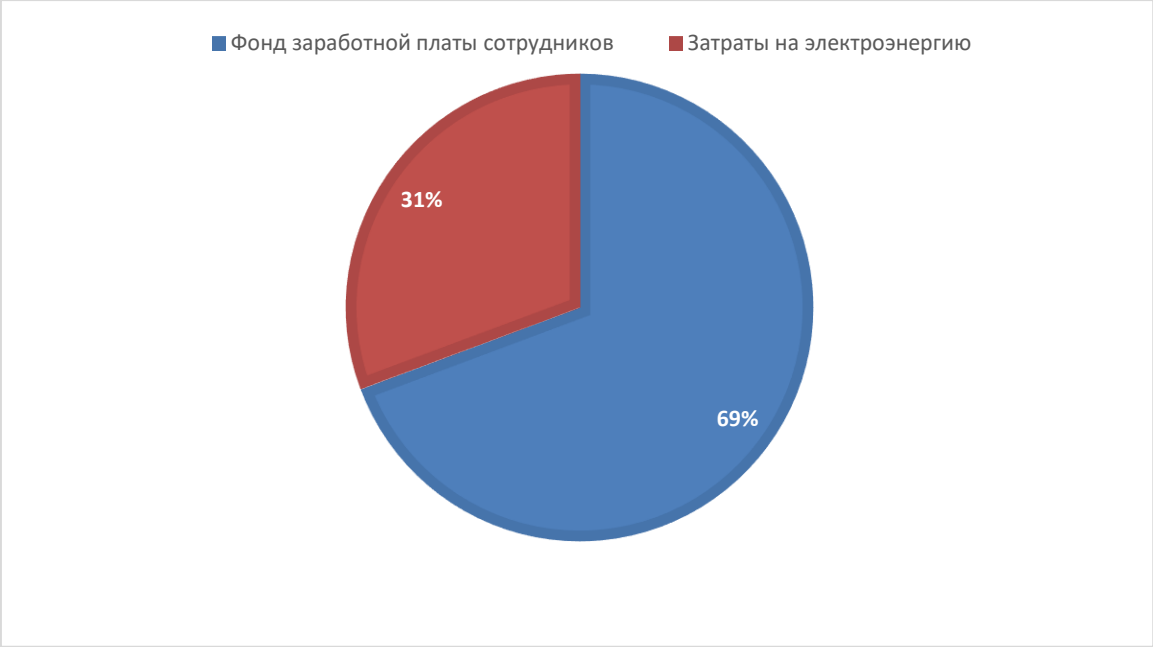

Рисунок 11 - Затраты на реализацию проекта.

Таким образом, можно сделать вывод о том, что стоимость данной системы значительно меньше стоимости существующих аналогов, что является одним из ключевых параметров при выборе системы мониторинга для предприятия ООО «Юрдел»

4.3 Расчёт затрат на эксплуатацию проекта

Основными статьями по расходами в эксплуатационный период будем считать расходы на специалиста по информационной безопасности и инженера – программиста. В обязанности специалиста по информационной безопасности входит своевременное реагирование на оповещения, которые выдает система.

В обязанности инженера – программиста входит отслеживание корректной работоспособности системы, а также написание дополнительных модулей для разрабатываемой системы, по желанию руководства предприятия.

Эксплуатационные расходы рассчитываются по формуле:

$$Э = З_{эс} + Р_r + А \quad (17)$$

$З_{эс}$ – фонд заработной платы обслуживающего персонала;

$Р_r$ – затраты на текущий ремонт и межремонтное обслуживание;

А – амортизационные отчисления.

$$З_{эс} = t_{э1} * З_{1час} \quad (18)$$

$t_{э1}$ = время, затрачиваемое сотрудником на поддержание работоспособности системы.

$t_{э1}$ = 200 р/час. Специалист по информационной безопасности тратит на работу с системой 30 минут в день. Работа осуществляется 365 дней в году. В год сотрудник тратит 183 часа на работу с данной системой

$$З_{эс} = 200 * 183 = 36\,600 \text{ рублей.}$$

К затратам на текущий ремонт отнесем работы по изменению программного кода. Данные работы вычисляются по формуле:

$$Р_r = S_{эл} + З_p. \quad (19)$$

$S_{эл\,(общ)}$ – стоимость заменяемых в процессе ремонта элементов;

$З_p$ – зарплата ремонтных рабочих.

В данной системе нет элементов, которые требуют замены или ремонта. Поэтому к затратам на текущий ремонт мы относим только заработную плату инженера программиста.

$$З_р = t_{р1} * З_{1час} \quad (20)$$

$t_{э2}$ = 300 р/час. Инженер-программист работает 1 день в месяц по 8 часов. (96 часов в год)

$$Р_r = З_р = 300 * 96 = 28\,800 \text{ рублей.}$$

Амортизационные отчисления вычисляем по формуле:

$$А = П_п * Н_а/100 \quad (21)$$

$П_п$ – стоимость разработки программного обеспечения

$Н_а$ – норма амортизационных отчислений, для ПО 33%;

$$А = 291590*33/100 = 96\ 195 \text{ рублей.}$$

Общая сумма эксплуатационных расходов(17):

$$Э = 36\ 600 + 28\ 800 + 96\ 195 = 161\ 595 \text{ рублей.}$$

4.4. Расчёт экономической эффективности проекта

Данный параграф посвящен расчету экономической эффективности на внедрение нового программного средства защиты информации – системы мониторинга действий пользователя в автоматизированной информационной системе на предприятии ООО «Юрдел».

В данном случае затраты носят инвестиционный характер. Для определения экономической эффективности инвестиций в данном проекте используется метод дисконтированных оценок. Дисконтирование применяется с целью сравнения возможных затрат и будущих доходов.

Так как предприятие осуществляет инвестиции за счет собственного бюджета в качестве обоснования пороговой процентной ставки стоит использовать прирост инфляции в Самарской области за 2020 г, который составил 4, 6 %. На основе данной пороговой процентной ставки рассматривается коэффициент дисконтирования.

$$K = \frac{1}{(1+r)^t} \quad (22)$$

t – число периодов, отделяющее момент

осуществления платежей или получение доходов от базового года.

r - прирост инфляции в Самарской области за 2020 год

Экономическая эффективность рассматривается на основании расчета:

- чистой дисконтированной стоимости
- внутренней нормы доходности
-срока полного возмещения инвестиций.
-прогнозируемого срока функционирования проекта (Т).

Расчёт чистой дисконтированной стоимости основан на сопоставлении величины исходных инвестиций (И) с общей суммой дисконтированных чистых денежных поступлений (ЧДП), обусловленных ими в течение прогнозируемого срока функционирования проекта (Т).

ЧДП для каждого i-го года эксплуатации рассчитывается по формуле:

$$ЧДП_i = \triangle П_i \pm \triangle Э_i \quad (23)$$

Где $\triangle П_i$ - прирост доходов предприятия;

В данной разработке прирост доходов предприятия осуществляется за счет сокращения ущерба от утечки информации.

$\triangle Э_i$ – изменение величины эксплуатационных издержек.

$$\triangle Э_i = (З_с - Э_н)$$

$З_с$ и $Э_н$ – это соответственно эксплуатационные издержки в существующем (до внедрения новой техники) и новом (после внедрения новой техники) вариантах.

Данная система позволяет снизить вероятные убытки от реализации угроз информационной безопасности примерно на 500 000 рублей.

Эксплуатационные расходы составляют 226 995 рублей.

В таблице 13 представлено изменение значения эксплуатационных издержек $\triangle Э_i$ за 5 лет.

Таблица 13 - Изменение значения эксплуатационных издержек.

Номер года	Эксплуатационные издержки до внедрения новой техники Зс руб.	Эксплуатационные издержки после внедрения новой техники $Э_н$, руб	Изменение величины эксплуатационных издержек $\triangle Э_i$, руб	Чистая дисконтированная стоимость без учёта инвестиций
0			-422 806	
1	500 000	161 595	338 405	323 523
2	500 000	161 595	338 405	310 463
3	500 000	161 595	338 405	296 846
4	500 000	161 595	338 405	284 374
5	500 000	161 595	338 405	270 724
Итого	2 500 000	807975	1 692 025	1 485 930

Чистая дисконтированная стоимость вычисляется по формуле:

$$ЧДС = \sum_{i=1}^{i} \frac{ЧДПi}{(1+r)^t} - И \quad (24)$$

ЧДС = 1 485 930 - 422 806 = 1 063 124 рублей.

Так как ЧДС > 0, то затраты оправданы.

Внутренняя норма доходности – это такая ставка процента, при которой ЧДС проекта равна 0. Смысл этого показателя при анализе эффективности инвестиций заключается в следующем: ВНД показывает ожидаемую доходность проекта и, следовательно, максимально допустимый относительный уровень расходов на данный проект. При расчете этого показателя используем метод последовательных итераций. Для этого необходимо найти два таких значения процентной ставки, при которых ЧДС меняет свое значение с + на -.

$$ВНД = r_1 + \frac{ЧДС_+(r2-r1)}{ЧДС_+ + |ЧДС_-|} \quad (34)$$

Где r_1 – процентная ставка, при которой ЧДС положительна (ЧДС+);

r2 – процентная ставка, при которой ЧДС отрицательна (ЧДС-).

при r_1 = 0,48 величина ЧДС+ = 513

- при r_2 = 0,47 величина ЧДС- = - 254

$$\text{ВНД} = \frac{32+5,13}{767} = 0,48$$

Таким образом ВНД больше процентной пороговой ставки 0,48 >0,046, следовательно затраты оправданы.

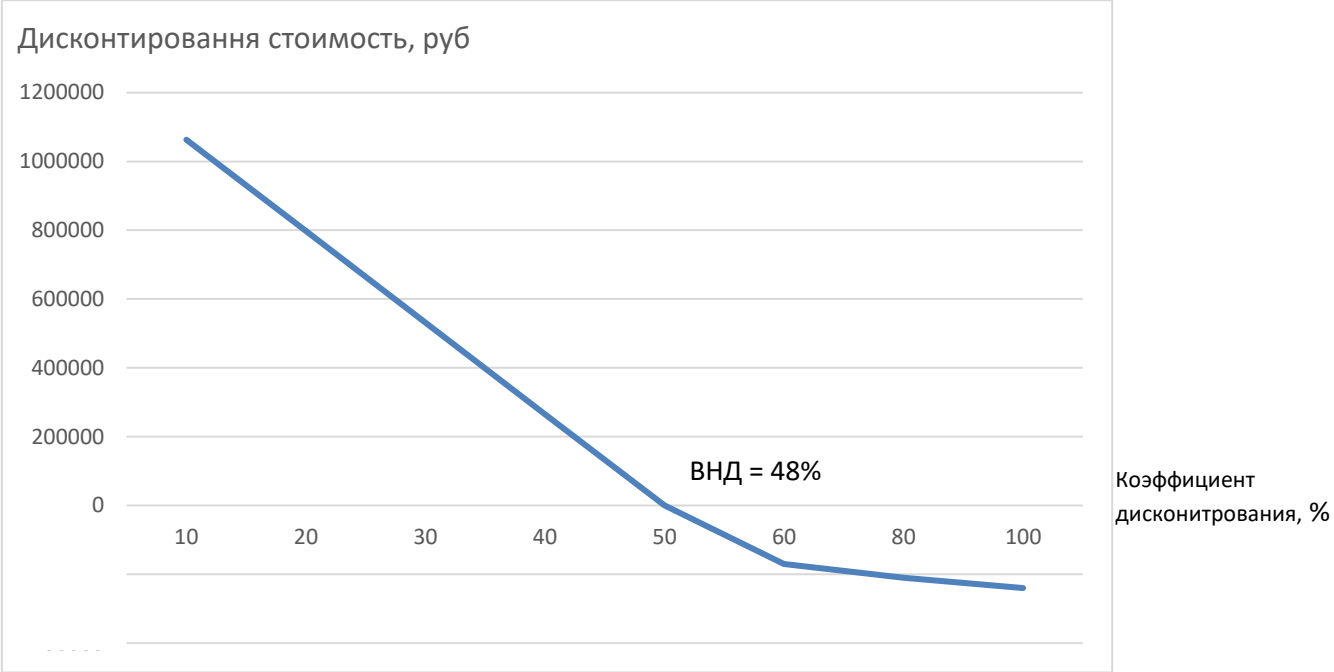

Рисунок 12 - Внутренняя норма доходности.

Срок полного возмещения инвестиций (СПВИ) показывает то количество лет, в течение которых инвестиции окупаются. Он даёт представление о рискованности производственных капитальных затрат.

СВПИ рассчитывается:

$$СПВИ = n + (И - \sum_{n=1}^{n} ЧДП_i)/ЧДП_{n+1}$$

Где n – число лет, за которое сумма чистых дисконтированных потоков денежных средств достигает величины, близкой к величине инвестиций, но ещё не покрывает их.

СПВИ сравнивается с допустим сроком, принятым инвестором, исходя из сроков возврата заёмных средств, сроков службы износа приобретаемого оборудования, “жизненного цикла” товара и т.д

СВПИ = 1 + (422 806 – 323 523)/ 310 463= 1,32 = 1 год 3 месяца 27 дней.

Можно сделать вывод о том, что вычисленное значение СВПИ соответствует допустимым срокам возмещения средств.

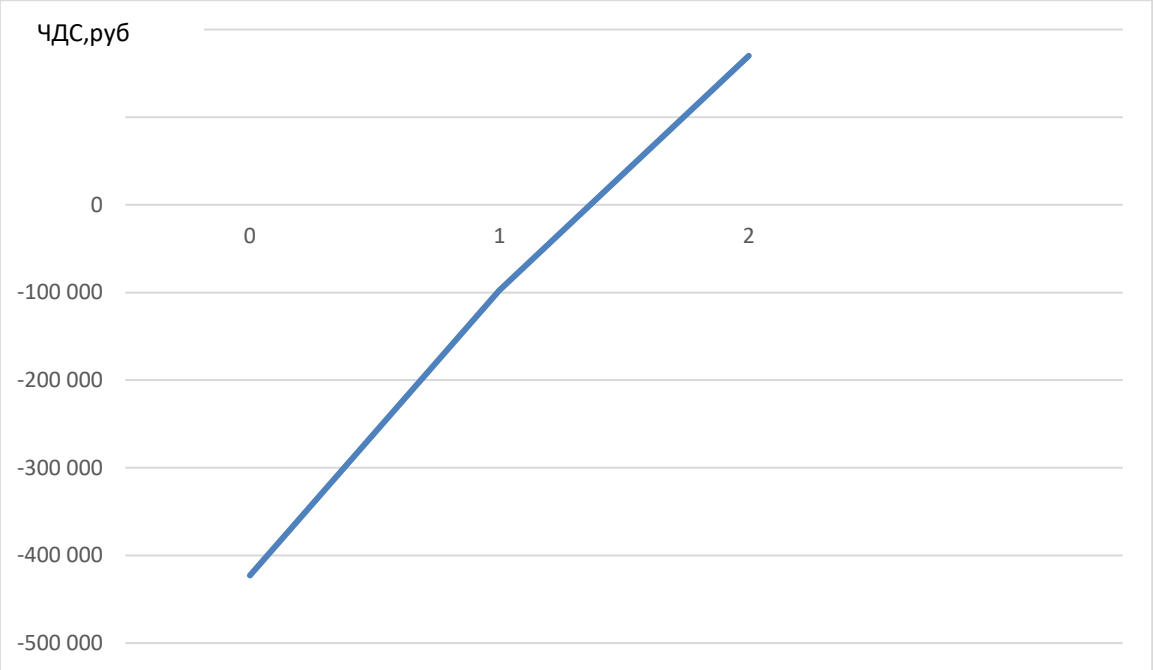

Рис 13 - Срок полного возмещения инвестиций.

5. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ЖИЗНЕДЕЯТЕЛЬНОСТИ

5.1 Постановка задачи

Необходимо проанализировать работу с персональными электронно – вычислительными машинами (ПЭВМ) в юридической фирме ООО «Юрдел». Анализируется система «человек – машина – среда».

5.2 Среда

Параметры микроклимата.

Существенное значение для комфортной работы с ПК имеют параметры микроклимата помещения, где работает человек. Микроклиматические параметры производственной среды — это сочетание температуры, относительной влажности и скорости движения воздуха.

Работа с ПЭВМ относятся к категории – 1а. К категории 1а относятся работы, производимые сидя и не требующие физического напряжения, при которых расход энергии составляет до 120 ккал/ч;

Оптимальными параметрами микроклимата для данной категории является температура воздуха 22 -24 ◦С, относительная влажность воздуха 40 – 60% скорость движения ветра 0,1 м/с в холодное время года и температура воздуха 22 -24 ◦С, относительная влажность воздуха 40 – 60% скорость движения ветра 0,1 м/с в холодное время года

Таблица 14 - Оптимальные параметры микроклимата

Период года	Темп. воздуха, гр. С, не более	Относит. Влажность воздуха, %	Скорость движения воздуха, м/с
Холодный	22-24	40 - 60	0,1
Теплый	23 - 25	40 - 60	0,2

Освещение на рабочем месте

В соответствии с нормами по освещению ниже перечислены требования.

- Освещенность на поверхности стола в зоне размещения рабочего документа должна быть 300 - 500 лк.

-Допускается установка светильников местного освещения для подсветки документов. Местное освещение не должно создавать бликов на поверхности экрана и увеличивать освещенность экрана более 300 лк.

-Необходимо ограничивать прямую блесткость от источников освещения, при этом яркость светящихся поверхностей (окна, светильники и др.), находящихся в поле зрения, должна быть не более 200 кд/кв.м.

-Необходимо ограничивать отраженную блесткость на рабочих поверхностях (экран, стол, клавиатура и др.) за счет правильного выбора типов светильников и расположения рабочих мест по отношению к источникам естественного и искусственного освещения, при этом яркость бликов на экране ВДТ и ПЭВМ не должна превышать 40 кд/кв.м и яркость потолка, при применении системы отраженного освещения, не должна превышать 200 кд/кв.м.

-Необходимо ограничивать неравномерность распределения яркости в поле зрения пользователя ПЭВМ, при этом соотношение яркости между рабочими поверхностями не должно превышать 3:1 - 5:1, а между рабочими поверхностями и поверхностями стен и оборудования 10:1.

-В качестве источников света при искусственном освещении должны применяться преимущественно люминесцентные лампы типа ЛБ. При устройстве отраженного освещения в производственных и административно-общественных помещениях допускается применение металлогалогенных ламп мощностью до 250 Вт. Допускается применение ламп накаливания в светильниках местного освещения.

-Общее освещение следует выполнять в виде сплошных или прерывистых линий светильников, расположенных сбоку от рабочих мест, параллельно линии зрения пользователя при рядном расположении ПЭВМ. При периметральном расположении компьютеров линии светильников должны

располагаться локализованно над рабочим столом ближе к его переднему краю, обращенному к оператору.

- Яркость светильников общего освещения в зоне углов излучения от 50 до 90 градусов с вертикалью в продольной и поперечной плоскостях должна составлять не более 200 кд/кв.м, защитный угол светильников должен быть не менее 40 градусов.
- Светильники местного освещения должны иметь не просвечивающий отражатель с защитным углом не менее 40 градусов.
-Коэффициент запаса (Кз) для осветительных установок общего освещения должен приниматься равным 1.4.

Для обеспечения нормируемых значений освещенности в помещениях использования ПЭВМ следует проводить чистку стекол оконных рам и светильников не реже двух раз в год и проводить своевременную замену перегоревших ламп.

Таблица 15 - Нормы освещенности помещений на уровне 80 см от пола.

Тип помещения	Комбинированное освещение, лк	Общее освещение, лк
Машинный зал	750	400
Помещения для персонала, осуществляющего техническое обслуживание ЭВМ.	750	400
Архивы, помещения для хранения носителей информации	-	300

Электробезопасность;

При эксплуатации ПЭВМ должны быть соблюдены следующие требования электробезопасности:

- сетевое электропитание устройств ПЭВМ должно производиться только от розеток типа "Европа" с заземляющими контактами;
- все электрические розетки, предназначенные для подключения к ним устройств ПЭВМ, должны иметь маркировку по напряжению. Значение номинального напряжения сети (220 В) необходимо наносить яркой краской, крупными символами (высотой не менее 50 мм) на стене или щите, возле или над розеткой;
- заземляющие контакты розеток должны иметь соединения с заземляющим контуром помещения или должны быть занулены. При занулении необходимо обратить особое внимание на создание надежного контакта нулевого провода с нулевой шиной сети электропитания. Запрещается использовать в качестве заземления радиаторы отопления, водопроводные трубы, молниеотводы.

Пожарная безопасность

Каждое из помещений, где производится эксплуатация устройств ПЭВМ, должно быть оборудовано первичными средствами пожаротушения и обеспечено инструкциями по их применению.

В качестве средств пожаротушения разрешается использование углекислотного огнетушителя типа ОУ-2, ОУ-5. Применение пенных огнетушителей не допускается, так как жидкость пропускает ток; - устройства ПЭВМ необходимо устанавливать вдали отопительных и нагревательных приборов (расстояние не менее 1 м и в местах, где не затруднена их вентиляция и нет прямых солнечных лучей). [6]

5.3 Машина

Электромагнитные излучения: при работе монитор испускает ряд излучений, которым подвергается человек, работающий за ЭВМ, и которые также подлежат нормированию. переменное электромагнитное, которое создает высокочастотный трансформатор строчной развертки, который размещается в задней или боковой части терминала. приводит к появлению вне монитора электростатического поля.

Таблица 16 - Допустимые значения параметров излучений, генерируемых Мониторами.

Электромагнитное излучение на расстоянии 0,5 м вокруг монитора по электрической составляющей	
5 Гц - 2 кГц	25 В/м
2 – 400 кГц	2,5 В/м
Электромагнитное излучение на расстоянии 0,5 м вокруг монитора по магнитной составляющей	
5 Гц - 2 кГц	250 нТл
2 - 400 кГц	25 нТл
Поверхностный электростатический потенциал	Не более 500 В

Акустический шум.

Печатающее оборудование, являющееся источником шума, необходимо устанавливать на звукопоглощающей поверхности автономного рабочего места пользователя. Если уровни шума от печатающего оборудования превышают нормируемые, оно должно быть расположено вне помещения с ПК. Помещения для выполнения основной работы с ПК не должны быть расположены рядом (смежно) с производственными помещениями с повышенным уровнем шума (мастерские, производственные цеха и т. п.).

При выполнении основной работы на мониторах и ПЭВМ (диспетчерские, операторские, залы вычислительной техники и т. д.), где работают инженерно-технические работники, уровень шума не должен превышать 60

дБА, в помещениях операторов ЭВМ (без дисплеев) — 65 дБА, на рабочих местах в помещениях, где размещаются шумные агрегаты вычислительных машин — 75 дБА.

Визуальные показатели видеодисплейного терминала (ВДТ).

Таблица 17 - Предельно допустимые значения визуальных параметров ВДТ, контролируемые на рабочих местах.

Параметры	Допустимые значения
Яркость белого поля	Не менее 35 кд/м^2
Неравномерность яркости рабочего поля	Не более ± 20 %
Контрастность (для монохромного режима)	Не менее 3 : 1
Временная нестабильность изображения (непреднамеренное изменение во времени яркости изображения на экране дисплея)	Не должна фиксироваться
Пространственная нестабильность изображения (непреднамеренные изменения положения фрагментов изображения на экране)	Не более 2×10^{-4L}, где L - проектное расстояние наблюдения, мм

Проектирование рабочих мест.

Так как целью разработки является разработка системы в уже существующее предприятие, то дополнительного проектировании рабочих мест не требуется.

Однако стоит упомянуть, что на данном предприятии конструкция рабочих мест соответствует всем гигиеническим требованиям, а именно:

- площадь на одно рабочее место с ПЭВМ составляет не менее 6,0 кв.м, С ВДТ на базе плоских дискретных экранов (жидкокристаллические, плазменные) - 4,5 кв.м., а объем - не менее 20 куб.м;
- помещения с ПЭВМ должны оборудоваться системами отопления, кондиционирования воздуха или эффективной приточно-вытяжной вентиляцией;
- запрещается применять для внутренней отделки интерьера помещений с ПЭВМ полимерные материалы (древесностружечные плиты, слоистый бумажный пластик, синтетические ковровые покрытия и др.). Полимерные материалы, используемые для отделки интерьера помещений с ПЭВМ, должны быть разрешены для применения органами и учреждениями Государственного санитарно-эпидемиологического надзора;
-поверхность пола в помещениях эксплуатации ПЭВМ должна быть ровной, без выбоин, нескользкой, удобной для очистки и влажной уборки, обладать антистатическими свойствами;
- рабочие места с ПЭВМ по отношению к световым проемам должны располагаться так, чтобы естественный свет падал сбоку, преимущественно слева;
- схема размещения рабочих мест с ПЭВМ должны учитывать расстояние между рабочими столами с видеомониторами (в направлении тыла поверхности одного видеомонитора и экрана другого видеомонитора), которое должно быть не менее 2,0 м, а расстояние между боковыми поверхностями видеомониторов - не менее 1,2 м;

- высота рабочей поверхности стола должна регулироваться в пределах 680-800 мм; при отсутствии такой возможности высота рабочей поверхности стола должна составлять 725 мм;

- рабочий стол должен иметь пространство для ног высотой не менее 600 мм, шириной - не менее 500 мм, глубиной на уровне колен - не менее 450 мм и на уровне вытянутых ног не менее 650 мм; - клавиатуру следует располагать 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; - оконные проемы в помещении ПЭВМ должны оборудоваться регулируемыми устройствами типа: жалюзи, занавесей, внешних козырьков и др.;

- рабочий стул (кресло) должен быть подъемно-поворотным и регулируемым по высоте и углом наклона сиденья и спинки, а также расстоянию спинки от переднего края сиденья. При этом регулировка каждого параметра должна быть независимой, легко осуществляемой и иметь надежную фиксацию;

- экран видеомонитора должен находиться от глаз пользователя на оптимальном расстоянии 600-700 мм, но не ближе 500 мм с учетом размеров алфавитно-цифровых знаков и символов;

- в помещениях с ПЭВМ ежедневно должна производиться влажная уборка;

- помещения с ПЭВМ должны быть оснащены аптечкой первой помощи и углекислотными огнетушителями. [3]

5.4 Человек

Виды трудовой деятельности разделяются на три группы:

группа А - работа по считыванию информации с экрана ПЭВМ с предварительным запросом;

группа Б - работа по вводу информации;

группа В - творческая работа в режиме диалога с ЭВМ.

Для видов трудовой деятельности устанавливаются 3 категории тяжести и напряженности работы с ПЭВМ, которые определяются:

- для группы А - по суммарному числу считываемых знаков за рабочую смену, но не более 60000 знаков за смену;
- для группы Б - по суммарному числу считываемых или вводимых знаков за рабочую смену, но не более 40000 знаков за смену;
- для группы В - по суммарному времени непосредственной работы с ПЭВМ за рабочую смену, но не более 6 часов за смену.

При 8-ми часовой рабочей смене и работе на ПЭВМ регламентированные перерывы следует устанавливать:

- для 1 категории работ через 2 часа от начала рабочей смены и через 2 часа после обеденного перерыва продолжительностью 15 минут каждый;
- для 2 категории работ через 2 часа от начала рабочей смены и через 1,5-2,0 часа после обеденного перерыва продолжительностью 10 минут через каждый час работы;
- для 3 категории работ через 1,5-2,0 часа от начала рабочей смены и через 1,5-2,0 часа после обеденного перерыва продолжительностью 20 минут каждый или продолжительностью 15 минут через каждый час работы.

При 12-ти часовой рабочей смене регламентированные перерывы должны устанавливаться в первые 8 часов работы аналогично перерывам при 8-ми часовой рабочей смене, а в течение последних 4 часа работы, независимо от категории и вида работ, каждый час продолжительностью 15 минут. [4]

ЗАКЛЮЧЕНИЕ

Вопрос обеспечения информационной безопасности на любом предприятии с каждым днём становится все более актуальным. Инциденты в области информационной безопасности в корпоративной сети предприятия могут повлечь за собой утечку информации. Вследствие чего предприятие может потерпеть серьёзные материальные и репутационные убытки и уступить на рынке конкурентам. Поэтому в процессе разработки системы защиты на предприятии крайне важно осуществлять регулярный мониторинг действий пользователя в информационной среде. Мониторинг информационной безопасности в информационных (автоматизированных) системах представляет собой процесс постоянного наблюдения и анализа результатов регистрации событий безопасности с целью выявления нарушений, угроз безопасности информации.

В представленной Выпускной Квалификационной Работе было исследовано поведение пользователя информационной среды на основании трех параметров, на основании полученных результатов разработана система мониторинга действий пользователя в автоматизированной информационной системе для предприятия ООО «Юрдел». В работе был сформирован эталон пользователя информационной среды, найдена корреляционная зависимость между параметрами информационной системы, разработана структурная схема системы анализа действия пользователя в информационной среде. Кроме того, были разработаны нечеткие правила для функционирования сисемы.

Система мониторинга разработана на языке программирования Python.

Система показала себя как стабильно функционирующая, устойчивая. Она соблюдает правила функционирования и отправляет уведомления в систему, а также блокирует пользователя в случае отклонений от эталонного поведения.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Федеральный закон "Об адвокатской деятельности и адвокатуре в Российской Федерации" от 31.05.2002 N 63-ФЗ (последняя редакция) http://www.consultant.ru/document/cons_doc_LAW_36945/

2. Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ (последняя редакция) /[Электронный ресурс]. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения 16.02.2021)

3. Гигиенические требования к видеодисплейным терминалам, персональным электронно-вычислительным машинам и организации работы санпин 2.2.2.542-96.

4. Гигиенические требования к персональным электронновычислительным машинам и организации работы. Санпин 2.2.2/2.4.1340-03.

5. ГОСТ 7.32-2017 Система стандартов по информации, библиотечному и издательскому делу. Отчет о научно-исследовательской работе. Структура и правила оформления . - М.: Стандартинформ, 2018. - 16 с.

6. Безопасность жизнедеятельности: Учебное пособие / Под общ. Ред. Н. К. Дёмика. – М.: Изд-во Рос. Экон. Акад., 2007. – с. ISBN 5–7307–060

7. Зуев В.Н., Ефимов А.Ю. Нейросетевой поведенческий анализ действий пользователя в целях обнаружения вторжений уровня узла // Программные продукты и системы. - 2019. Т. 32. Вып. 2. - С. 258–262.

8. Карпова Н.Е, Баранов А.С, Емелина А.А, Коновалов А.Е /Разработка системы анализа действий пользователя в информационной среде/ Динамика систем, механизмов и машин. – 2020 -Том 8, № 2. – С. 114

9. Карпова Н.Е, Баранов А.С, Емелина А.А, Коновалов А.Е /Исследование аномальных действий пользователя в информационной среде / Сборник научных трудов НГТУ. – 2020 – № 1–2 (97). – С. 26–39. – DOI: 10.17212/2307-6879-2020-1-2-26-39

10. Коробкова И.Л., Дьяков И.А. Основы теории нечетких множеств: Метод. Указания // Тамбов: Изд-во Тамб. Гос. Техн. Ун-та,. 2003. 24 с.

11. Корченко А. Г. Построение систем защиты информации на нечётких множествах. / МК-Пресс. 2006/. 320 с.

12. Привалов А.Н. Богатырёва Ю.И /иерархическая оценка компетентности в области информационной безопасности / научные ведомости ТГПУ м . Л .Н. Толстого. – 2012. № 13 (132). Выпуск 23/1 С. 194

13. Савинова В.М. Идентификация пользователей корпоративной системы с помощью поведенческого анализа с использованием модели

искусственной нейронной сети / В.М. Савинова, А.А. Бесхмельницкий, Е.С. Бабина, А.Д. Осадчая // Транспортное дело России. – 2017. №5. С. 65-68

14. Choi S., Yun J. H., Kim S. K. A Comparison of ICS Datasets for Security Research Based on Attack Paths //International Conference on Critical Information Infrastructures Security. – Springer, Cham, 2018. – P. 154-166

15. Karpova N., Panfilova I. Ensuring the Safety of Information Processes in Sociotechnical Systems Based on an Analysis of the Behavioral Characteristics of a Person as a Subject of Such a System // XXI International Conference Complex Systems: Control and Modeling Problems (CSCMP), Samara, 2019. P. 751–753

16. Lozano C.M., Lopez F., Lopez J. And others. Neural Networks for System Security. Proc. Of 5th European Congress on Intelligent Techniques and Soft Computing (Aachen, Germany).vol.1, pp. 410-414. (1997)

17. Obaidat M.S., Macchairolo D.T. A multilayer neural network system for computer access security. EEE Trans. On Syst., Man. And Cybern. Vol. 24, No 5. Pp. 806-813, (1994)

18. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных" (утв. 15.02.2008 фстэк рф) угрозы несанкционированного доступа к информации в информационной системе персональных данных /[Электронный ресурс]. Режим доступа: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/379-bazovaya-model-ugroz-bezopasnosti (дата обращения 15.04.2021)

19. Банк данных угроз безопасности информации) /[Электронный ресурс]. Режим доступа: https://bdu.fstec.ru/ (дата обращения 1.04.2021)

20. Классификация угроз информационной безопасности [Электронный ресурс]. – Режим доступа : http://it-ideas74.ru/articles/25-security-inform.html. (Дата обращения: 16.01.2021)

21. Обзор DATAPK — комплекса оперативного мониторинга и контроля защищённости АСУ ТП /[Электронный ресурс]. Режим доступа: https://www.anti-malware.ru/reviews/PAK-DATAPK [14] (дата обращения 17.02.2021)

22. Сапрыкина А./ Обзор fortisiem — система сбора и анализа событий информационной безопасности /[Электронный ресурс]. Режим доступа: https://www.anti-malware.ru/reviews/fortisiem (дата обращения 24.02.2021)

23. Средства защиты информации (СЗИ) [Электронный ресурс]. Режим доступа: https://it-security.admin-smolensk.ru/zinfo/szi/ (Дата обращения: 20.01.2021)

24. Сущность, состав и проблемы безопасности АСУ ТП/[Электронный ресурс]. Режим доступа: https://www.anti-malware.ru/reviews/PAK-DATAPK (дата обращения 28.03.2021)

25. Трещев Иван Андреевич/О классификации угроз безопасности конфиденциальной информации предприятия/[Электронный ресурс]. Режим доступа: https://mir-nauki.com/PDF/15KMN314.pdf (дата обращения 11.01.2021)

26. Doug White. Three Key Areas in Active Directory Security/ Security Weekly. [Электронный ресурс]. Режим доступа: https://securityweekly.com/2018/09/06/three-key-areas-in-active-directory-security/ (дата обращения 09.02.2021) (10)

27. Symantec Data Loss Prevention (DLP) Suite /[Электронный ресурс]. Режим доступа:https://www.symbuy.ru/symantec-data-loss-prevention-suite (дата обращения 28.01.2021) (16)

28. Tara Seals Fear of Insider Threats Hits an All-Time High, Infosecurity Magazine [Электронный ресурс] Режим доступа: https://www.infosecurity-magazine.com/news/fear-of-insider-threats-hits-an/ (дата обращения 15.03.2021)

ПРИЛОЖЕНИЕ А

Программный код для системы мониторинга действий пользователя в автоматизированной информационной системе.

```
import json

import pytz

from typing import Iterator

from datetime import datetime, timedelta

from typing import List, Tuple, Optional, Iterator, Union

self.count_entry_access = ["0-3", "4-6"]

        self.count_entry_access = ["7-10"]

        self.count_entry_fail = ["11-13", "14-17"]

       self.__count_exit = None;

        self.intervals = None;

class ActiveDirectoryLogs:

    def __init__(self) -> None:

        self.dt = ActiveDirectoryLogs.count_entry.ToString("4625")

        self. count_entry = ActiveDirectoryLogs.__te

        self.__count_entry = None;

        self.__for_session = None;

    DAY_ENTRY = datetime.datetime.now()

    __te = datetime.datetime.now().TimeOfDay

from demo.ActiveDirectoryLogs import ActiveDirectoryLogs
```

```
from demo.OurDat

self.day_entry_access = ["понедельник", "вторник", "среда", "четверг",
"пятница"]

        self.day_entry_access = ["понедельник", "вторник", "среда", "четверг",
"пятница"]

        self.day_entry_fail = ["суббота", "воскресенье"]

        self.__time_entry = None;

        self.__way_to_file = None;

        self.__time_exit = None;

        self.__for_session = None;

        self.intervals = None;

class ActiveDirectoryLogs:

    def __init__(self) -> None:

        self.dt = ActiveDirectoryLogs.DAY_ENTRY.ToString("dddd")

        self.time_entry = ActiveDirectoryLogs.__te

        self.__way_to_file = None;

        self.__time_exit = None;

        self.__for_session = None;

    DAY_ENTRY = datetime.datetime.now()

    __te = datetime.datetime.now().TimeOfDay

from demo.ActiveDirectoryLogs import ActiveDirectoryLogs

from demo.OurDataBase import OurDataBase
```

```
class Program:
    @staticmethod
    def main(args : typing.List[str]) -> None:
        odb = OurDataBase()
        adl = ActiveDirectoryLogs()
class OurDateBase:
    class ActiveDirectoryBase:
        def __init__(self) -> None:
            self.way_to_file = "C:\\Users\\*\\Documents\\Загрузки"
    class Program:
        def __init__(self) -> None:
            self.__odb = OurDateBase()
            self.__adb = OurDateBase.ActiveDirectoryBase()
        @staticmethod
        def main(args : typing.List[str]) -> None:
            pass
    def __init__(self) -> None:
        self.way_to_file = ["C: ", "C:\\Documents and Settings", "C:\Users\ шаблоны документов", ""C:\Documents and Settings\worker\Командировки", "C:\Windows\карточка сотрудника, ""C:\Documents and Settings\worker\Мои клиенты", "C:\Documents and Settings\worker\Текущие клиенты, "C:\Users\*\Documents\Загрузки, "C:\ProgramFiles", "C:\Windows\персональные данные
```

```
сотрудников, "C:\Windows\База данных клиентов, "C:\Windows\System",
"C:\Windows\Logs"]
class ActiveDirectoryBase:
    def __init__(self) -> None:
        self.way_to_file = "C:\\Users\\*\\Documents\\Загрузки"
from demo.ActiveDirectoryBase import ActiveDirectoryBase
from demo.OurDateBase import OurDateBase
class Program:
    def __init__(self) -> None:
        self.__odb = OurDateBase()
        self.__adb = ActiveDirectoryBase()
    @staticmethod
    def main(args : typing.List[str]) -> None:
class OurDataBase:
    def __init__(self) -> None:
        if (adl.dt == odb.day_entry_fail[0] or adl.dt == odb.day_entry_fail[1]):
            print("Аномальное поведение» в " + adl.dt, flush=True)
        else:
            print("Подозрительное поведение" + " " + adl.dt, flush=True)
            if (adl.time_entry <= odb.intervals[4] and adl.time_entry >= odb.inter-
vals[3]):
```

```
            print("Подозрительное поведение" + " 0,8 " + (adl.time_entry),
flush=True)
        elif (adl.time_entry <= odb.intervals[6] and adl.time_entry >= odb.inter-
vals[5]):
            print("Аномальное поведение" + " 0,8 " + (adl.time_entry), flush=True)
        elif (adl.time_entry <= odb.intervals[7] and adl.time_entry >= odb.inter-
vals[6]):
            print("Аномальное поведение" + " 0,6 " + (adl.time_entry), flush=True)
        elif (adl.time_entry <= odb.intervals[5] and adl.time_entry >= odb.inter-
vals[4]):
            print("Подозрительное поведение", flush=True)
        elif (adl.time_entry <= odb.intervals[3] or adl.time_entry >= odb.inter-
vals[7]):
            print("Аномальное поведение", flush=True)
class Events(ModuleInterface, LoggingHandler):
    __storage_port = 9200
    __api_storage_search = '/_search?timeout={}s&ignore_unavailable=true'
    def __init__(self, auth: Auth, settings: Settings):
        ModuleInterface.__init__(self, auth, settings)
        LoggingHandler.__init__(self)
        self.__storage_version = auth.get_storage_version()
        self.__storage_hostname = auth.get_creds().storage_hostname
        auth.disconnect()
```

```
self.__storage_session = Search(hosts=self.__storage_hostname,
port=self.__storage_port, timeout=self.settings.connection_timeout)

self.QueryBuilder = QueryBuilder(self.__storage_version, self.settings.stor-
age_events_timezone, self.settings.storage_bucket_size)

self.log.debug('status=success, action=prepare, msg="Events Module init"')

 def get_events_groupby(self, filters: dict, begin: int, end: int) -> Iterator[dict]:

self.log.debug('status=prepare, action=get_groups, msg="Try to exec query
with filter", '

            'hostname="{}", filter="{}" begin="{}", end="{}"'.for-
mat(self.__storage_hostname, filters, begin, end))

fields = filters.get('fields')

if filters is None or fields is None:

   raise Exception('Unsupported filters format "{}"'.format(filters))

query = self.QueryBuilder.build_agg_query(filters, fields, begin, end)

self.log.debug('status=prepare, action=build_query, msg="Generate query", '

            'hostname="{}" query="{}"'.format(self.__storage_hostname,
query))

indexes = ','.join(self.__get_indexes_list(begin, end))

timeout_report_gen = self.settings.connection_timeout * self.settings.connec-
tion_timeout_x

start_time = get_metrics_start_time()

response = self.__storage_session.search(index=indexes, body= query, size=0,
equest_timeout=timeout_report_gen, ignore_unavailable=True)
```

```
        took_time = get_metrics_took_time(start_time)
        self.__check_storage_response(es_response)
        if self.__is_empty_response(es_response):
            self.log.debug('status=success, action=get_groups, msg="Empty report", '
                           'hostname="{}", lines={}'.format(self.__storage_hostname, 0))
            yield {}
        converted_response = self.__convert_aggregation_response(es_response.get('aggregations', {}))
        base_schema = self.__make_return_schema(filters)
        for row in converted_response:
            schema = base_schema.copy()
            schema.update(row)
            yield schema
        line_counter = len(converted_response)
        self.log.info('status=success, action=get_groups, msg="Query executed, response have been read", '
                      'hostname="{}", lines={}'.format(self.__storage_hostname, line_counter))
        self.log.info('hostname="{}", metric=get_groups, took={}ms, objects={}'.format(self.__storage_hostname, took_time, line_counter))
    def get_events(self, filters: dict, begin: int, end: int) -> Iterator[dict]:
        self.log.debug('status=prepare, action=get_events, msg="Try to exec query with filter", '
```

```
                'hostname="{}", filter="{}" begin="{}", end="{}"'.format(self.__storage_hostname, filters, begin, end))
        line_counter = 0
        query = self.QueryBuilder.build_filter_query(filters, begin, end)
        indexes = ','.join(self.__get_indexes_list(begin, end))
        timeout_report_gen = self.settings.connection_timeout * self.settings.connection_timeout_x
        start_time = get_metrics_start_time()
        try:
            for hit in helpers.scan(self.__storage_session,
                                    query, scroll='{}s'.format(round(self.settings.connection_timeout/2)), index=indexes, size=self.settings.storage_batch_size, raise_on_error=False, request_timeout=timeout_report_gen, preserve_order=True):
                if (line_counter % self.settings.storage_batch_size) == 0:
                    self.log.debug('status=failed, action=get_events, msg="Get rows from storage {}", '
                                   'hostname="{}",'.format(line_counter, self.__storage_hostname))
                line_counter += 1
                yield hit
        except NotFoundError as nf_ex:
            if nf_ex.error == 'index_not_found_exception':
```

```
            self.log.error('status=failed, action=get_events, msg="{}", '
                           'hostname="{}",'.format(nf_ex.error, self.__storage_hostname))
            yield {}
        else:
            raise Exception(nf_ex.error)
    took_time = get_metrics_took_time(start_time)
    self.log.info('status=success, action=get_events, msg="Query executed, response have been read", '
                  'hostname="{}", lines={}'.format(self.__storage_hostname, line_counter))
    self.log.info('hostname="{}", metric=get_events, took={}ms, objects={}'.format(self.__storage_hostname, took_time, line_counter))
def __make_return_schema(self, filters):
    ret = {}
    field = filters.get('fields', '')
    field_list = field.split(',')
    for fld in field_list:
        fld_list = fld.strip().split(' as ')
        fld_name = fld.strip() if len(fld_list) == 1 else fld_list[1].strip()
        ret[fld_name] = ''
    return ret
def __get_indexes_list(self, begin: int, end: int) -> list:
```

```
        index_prefix = 'ptsiem_events_' if self.__storage_version == StorageVersion
else 'events_'

        begin_date = datetime.fromtimestamp(begin, tz=pytz.timezone(self.set-
tings.storage_events_timezone))

        end_date = datetime.fromtimestamp(end, tz=pytz.timezone(self.settings.stor-
age_events_timezone))

        ret = []

        for n in range(int((end_date - begin_date).days) + 1):

            ret.append(index_prefix + (begin_date + timedelta(n)).strftime('%Y-%m-
%d'))

        return ret

    def __convert_aggregation_response(self, aggs: dict) -> list:

        ret = []

        for k, v in aggs.items():

            if v.get('buckets') is not None:

                for b in v.get('buckets'):

                    key = None

                    cnt = None

                    sub = []

                    for i, j in b.items():

                        if i == 'key':

                            key = j
```

```
                if i == 'doc_count':
                    cnt = j
                if isinstance(j, dict):
                    sub += self.__convert_aggregation_response({i: j})
            if len(sub) == 0:
                ret.append({k: key, "count": cnt})
            for h in sub:
                if h.get('count') is not None:
                    h.update({k: key})
                else:
                    h.update({k: key, "count": cnt})
            ret += sub
        return ret
    def __is_empty_response(self, storage_response: dict) -> bool:
        if storage_response is None or len(storage_response) == 0:
            self.log.error('status=failed, action=report_read, msg="Storage return empty response", '
                           'hostname="{}"'.format(self.__storage_hostname))
            return True
        if self.__storage_version == StorageVersion:
            if storage_response.get('hits').get('total').get('value') == 0:
```

```
            return True
        if self.__storage_version == StorageVersion:
            if storage_response.get('hits').get('total') == 0:
                return True
        return False
    def __check_storage_response(self, storage_response: dict) -> None:
        if storage_response.get('error') is not None and storage_response.get('er-
ror').get('root_cause') is not None:
            error_msg = []
            for i in storage_response.get('error').get('root_cause'):
                error_msg.append(i.get('type'))
            self.log.error('hostname="{}", status=failed, action=exec_query, '
                           'msg="Storage return errors: {}"'.format(self.__storage_hostname,
','.join(error_msg)))
            storage_response.clear()
            return
        if storage_response.get('timed_out'):
            self.log.warning('hostname="{}", status=failed, action=exec_query, '
                             'msg="Storage return timed out for some shards. '
                             'Some data have been lost"'.format(self.__storage_hostname))
        elif storage_response.get('_shards').get('failed') != 0:
```

```
            self.log.warning('hostname="{}", status=failed, action=exec_query,
msg="Storage return failed shards. '
                             'Some data have been lost"'.format(self.__storage_hostname))
        for k, v in storage_response.get('aggregations', {}).items():
            if v.get('doc_count_error_upper_bound') != 0 or
v.get('sum_other_doc_count') != 0:
                self.log.warning('hostname="{}", status=failed, action=exec_query, '
                                 'msg=" return doc count error. '
                                 'Some data have been lost"'.format(self.__storage_hostname))
    def close(self):
        if self.__storage_session is not None:
            self.__storage_session.close()
```