

Министерство образования Республики Беларусь

Учреждение образования
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет информационных технологий и управления

Кафедра интеллектуальных информационных технологий

К защите допустить:
Заведующий кафедрой XXX
_____ Д. В. Шункевич

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
к дипломному проекту
на тему:

**СИСТЕМА УПРАВЛЕНИЯ И МОНИТОРИНГА
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОМПАНИИ**

БГУИР ДП 1-40 03 01 02 059 ПЗ

Студент

Е. В. Митрофанов

Руководитель

Г. В. Лихачёв

Консультанты:

от кафедры ИИТ

А. М. Соболь

по экономической части

В. В. Верняховская

Нормоконтролёр

В. В. Захаров

Рецензент

Минск 2022

Министерство образования Республики Беларусь
Учреждение образования
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет ИТиУ
Специальность 1-40 03 01

Кафедра ИИТ
Специализация 1-40 03 01 02

УТВЕРЖДАЮ

_____ Зав. кафедрой
«____» _____ 2022 г.

ЗАДАНИЕ
по дипломному проекту студента
Митрофанова Егора Витальевича
(фамилия, имя, отчество)

1. Тема проекта: Система управления и мониторинга информационной безопасности компании

утверждена приказом по университету от 10 мая 2022 г. № 1133-с

2. Срок сдачи студентом законченного проекта: 30 мая 2022

3. Исходные данные к проекту: AD Windows Server 2016, FortyWeb фаервол, FortMail, ПО Kaspersky, ПО Symantek, PAM, MaxPatrol, Falcongaze Secure Tower, сервера с ОС Linux, сервера С OCWindows 2008-2022, ОС IBM 400, сетевые экраны Cisco Asa, ExchangeServe с ОС Windows 2016

Назначение разработки: разработать систему управления и мониторинга информационной безопасности компании

4. Содержание пояснительной записки (перечень подлежащих разработке вопросов):

Введение

1 Анализ подходов к разработке системы управления и мониторинга информационной безопасности компании

2 Проектирование системы управления и мониторинга информационной безопасности компании

3 Разработка системы управления и мониторинга информационной безопасности компании

4 Технико-экономическое обоснование разработки и введения в эксплуатацию системы управления и мониторинга информационной безопасности компании

Заключение

5. Перечень графического материала (с точным указанием обязательных чертежей):

- 1 Жизненный цикл события информационной безопасности — формат А1
- 2 Источники сообщений об инцидентах информационной безопасности — формат А1
- 3 Структура системы мониторинга и управления информационной безопасности компании — формат А1
- 4 Блок-схема алгоритма обработки инцидентов информационной безопасности — формат А1
- 5 Схема базы данных — формат А1
- 6 Пользовательский интерфейс системы — формат А1
- 7 Компьютерная презентация

6. Содержание задания по технико-экономическому обоснованию.

- 1 Краткая характеристика системы управления и мониторинга информационной безопасности компании
- 2 Расчёт затрат на разработку системы управления и мониторинга информационной безопасности компании
- 3 Расчёт экономического эффекта

Задание выдал: _____ В. В. Верняховская

КАЛЕНДАРНЫЙ ПЛАН

№ п/п	Наименование этапов дипломного проекта	Объем этапа, %	Срок выполнения этапов	Примечание
1	Подбор и изучение литературы	10	12.02 – 19.04	
2	Изучение проблемной области, средств проектирования и разработки	10	20.02 – 19.04	
3	Определение требований к реализации	10	03.04 – 18.04	
4	Проектирование модели системы	15	23.03 – 05.04	
5	Разработка системы	30	05.04 – 20.05	
6	Расчет экономической эффективности проекта	5	23.03 – 02.05	
7	Оформление пояснительной записки	10	23.03 – 31.05	
8	Оформление графической части проекта	10	01.04 – 29.05	

Дата выдачи задания: 23.03.2022 г. Руководитель _____ А. М. Соболь

Задание принял к исполнению _____ Е. В. Митрофанов

РЕФЕРАТ

СИСТЕМА УПРАВЛЕНИЯ И МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОМПАНИИ / Е. В. Митрофанов. – БГУИР, 2022, – п.з. – 75с., чертежей (плакатов) — 6 л. формата А1.

Целью дипломного проекта является разработка программного продукта — системы управления и мониторинга информационной безопасности компании - для самостоятельного производства и собственного использования на предприятии. Предметом исследования является управление и мониторинг информационной безопасности компании.

В первом разделе пояснительной записки проведен анализ типовой структуры системы управления и мониторинга информационной безопасности компании и обзор аналогов.

В втором разделе описана модель системы управления и мониторинга информационной безопасности компании. Структурированы понятия, связанные с модулем, рассмотрены ее общая схема, определены основные её возможности, а также требования к системе.

В третьем разделе проведен выбор и описание инструментальных средств для реализации системы, описана реализация необходимой ее функциональности, а также графический интерфейс и принципы взаимодействия с ним.

В четвертом разделе приведено технико-экономическое обоснование разрабатываемого программного продукта.

Результатом дипломного проектирования является система управления и мониторинга информационной безопасности компании.

СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ УСЛОВНЫХ ОБОЗНАЧЕНИЙ	6
ВВЕДЕНИЕ	7
1 Анализ подходов к разработке системы управления и мониторинга информационной безопасности компании	9
1.1 Анализ поставленной задачи в рамках предметной области	9
1.2 Типовая структура системы управления и мониторинга информационной безопасности компании	10
1.3 Обзор аналогов ключевого компонента системы управления и мониторинга информационной безопасности компании	16
1.4 Вывод	18
2 Проектирование системы управления и мониторинга информационной безопасности компании	19
2.1 Требования к системе в целом	19
2.2 Требования к структуре и функционированию системы	19
2.3 Требования к надежности системы	20
2.4 Требования к защите от несанкционированного доступа в систему	20
2.5 Требования к функциональным характеристикам системы	21
2.6 Требования к модернизации	21
2.7 Технические требования к реализации	21
2.8 Вывод	22
3 Разработка системы управления и мониторинга информационной безопасности компании	23
3.1 Используемые составляющие системы управления и мониторинга информационной безопасности компании	23
3.2 Вывод	60
4 Технико-экономическое обоснование разработки и внедрения в эксплуатацию системы управления и мониторинга информационной безопасности компании	61
4.1 Характеристика разработанной системы управления и мониторинга информационной безопасности	61
4.2 Расчет инвестиций на разработку и внедрение в эксплуатацию системы управления и мониторинга информационной безопасности	61
4.3 Расчет экономического эффекта от использования системы управления и мониторинга информационной безопасности	66

4.4 Расчёт показателей экономической эффективности разработки и использования системы управления и мониторинга информационной безопасности	67
4.5 Вывод	70
ЗАКЛЮЧЕНИЕ	71
СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ	71

ПЕРЕЧЕНЬ УСЛОВНЫХ ОБОЗНАЧЕНИЙ

DB — DataBase (база данных);
DLP-системы — Digital Light Processing (система предотвращения утечки информации);
DoS-атака — Denial of Service (отказ в обслуживании);
HTML — HyperText Markup Language (язык гипертекстовой разметки);
HTTP — HyperText Transfer Protocol (протокол передачи гипертекста);
IDS — Intrusion Detection System (система обнаружения вторжений);
IP — Internet Protocol (Интернет-протокол);
IT — Information Technology (информационные технологии);
KAV — Kaspersky Antivirus (антивирус Касперского);
MS — Microsoft (Майкрософт);
SIEM — Security Information And Event Management (система мониторинга и корреляции событий информационной безопасности);
TDS — Threat Detection System (система обнаружения целевых атак и угроз в корпоративной сети);
UI — User Interface (пользовательский интерфейс);
UML — Unified Modeling Language (унифицированный язык моделирования);
XML — eXtensible Markup Language (расширяемый язык разметки);
АРМ — автоматизированное рабочее место;
БД — база данных;
ИБ — информационная безопасность;
ЛВС — локальная вычислительная сеть;
НДС — налог на добавочную стоимость;
ОС — операционная система;
СУБД — система управления базами данных.

ВВЕДЕНИЕ

В современном автомобилестроении особое внимание уделяется повышению безопасности и комфорта вождения. Одним из ключевых аспектов, влияющих на безопасность, является эффективное освещение дорожного полотна, особенно в условиях плохой видимости и при выполнении маневров, таких как повороты. Традиционные системы освещения, использующие статичное направление света фар, не всегда обеспечивают достаточную видимость на поворотах, что может привести к аварийным ситуациям. В связи с этим актуальной задачей становится разработка и внедрение систем, способных динамически изменять направление света фар в зависимости от угла поворота руля и скорости движения автомобиля.

В последние годы на рынке автомобильных технологий наблюдается активное развитие интеллектуальных систем освещения, таких как адаптивные фары (Adaptive Front-lighting System, AFS). Эти системы позволяют автоматически регулировать направление светового потока в зависимости от дорожной ситуации, что значительно улучшает видимость и снижает риск возникновения аварий. Однако, несмотря на очевидные преимущества, такие системы требуют точного управления и интеграции с другими электронными системами автомобиля, что делает их разработку сложной технической задачей.

Целью данного дипломного проекта является разработка блока управления направлением света фар автомобиля при поворотах. Данный блок должен обеспечивать автоматическую корректировку угла наклона фар в зависимости от угла поворота руля и скорости движения, что позволит улучшить освещение дорожного полотна в поворотах и повысить безопасность вождения.

Достижение поставленной цели реализуется посредством выполнения следующих задач:

- проведение анализа существующих решений в области адаптивных систем освещения и выявление их преимуществ и недостатков;
- разработка алгоритма управления направлением света фар на основе данных о угле поворота руля и скорости автомобиля;
- проектирование аппаратной части блока управления, включая датчики, исполнительные механизмы и микроконтроллер;
- разработка программного обеспечения для управления системой и проведение тестирования разработанного блока в условиях, приближенных к реальному.

Разрабатываемый блок управления направлением света фар может быть интегрирован в современные автомобили, оснащенные электронными системами управления. Это позволит повысить безопасность вождения, особенно в условиях недостаточной видимости, и улучшить комфорт для водителя.

В качестве инструментов для разработки будут использованы современные средства проектирования электронных систем, такие как CAD-программы для проектирования печатных плат, среды разработки программного обеспечения для микроконтроллеров, а также специализированное оборудование для тестирования и отладки.

Таким образом, данный проект направлен на создание инновационного решения, которое может быть внедрено в автомобильную промышленность для повышения безопасности и комфорта вождения.

1. АНАЛИЗ ПОДХОДОВ К РАЗРАБОТКЕ СИСТЕМЫ УПРАВЛЕНИЯ И МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОМПАНИИ

В данном разделе будет производиться обзор подходов для решения задач, поставленных в рамках разрабатываемой системы, их преимуществ и недостатков, а также причины выбора конкретных подходов.

1.1. Анализ поставленной задачи в рамках предметной области

Мониторинг и управление информационной безопасностью компании — неотъемлемая часть рабочего процесса службы информационной безопасности компании. В связи со стремительным развитием информационных технологий, активно развивается преступность с использованием данных технологий. Мошенники используют различные алгоритмы и инструменты для получения доступа к материальным средствам и персональным данным (логин/пароль от различных персональных кабинетов пользователя, паспортные данные, идентификационные номера, данные платёжных карт и т.д.) с целью их похищения. Для решения проблемы компрометации персональных данных в компаниях могут использоваться различные программные решения:

- антивирусные системы;
- фрод-мониторинг;
- межсетевые экраны (фаерволы);
- системы противодействия фишингу;
- системы администрирования доступов пользователей;
- системы защиты электронной почты;
- DLP-системы;
- СУБД.

Проблема мошенничества с использованием информационных технологий может быть решена внедрением и настройкой системы управления и мониторинга информационной безопасности компании. Такая система должна уметь:

- своевременно идентифицировать локальные атаки и реагировать на них;
- в режиме реального времени проверять все транзакции, выявлять подозрительные и блокировать их;
- своевременно идентифицировать сетевые атаки и реагировать на них;
- в режиме реального времени производить поиск фишинговых ресурсов и информировать администраторов системы о таковых;
- инкапсулировать информацию;

- в режиме реального времени сканировать трафик электронной почты, выявлять подозрительные письма, блокировать их, и информировать об этом сотрудников службы информационной безопасности компании;
- предоставлять возможность удаленно администрировать рабочие машины;
- защищать, хранить, и структурировать внутреннюю информацию компании.

1.2. Типовая структура системы управления и мониторинга информационной безопасности компании

Типовая структура системы управления и мониторинга информационной безопасности компании состоит из элементов, представленных на рисунке 1.1.



Рисунок 1.1 – Типовая структура системы управления и мониторинга информационной безопасности компании

Исходя из данных, представленных на рисунке 3.1, сделан вывод, что АРМ администратора безопасности обменивается информацией с сервером мониторинга информационной безопасности, который, в свою очередь, собирает информацию из сети передачи данных, состоящей из следующих агентов мониторинга:

- коммуникационное или сетевое оборудование (маршрутизаторы, коммутаторы, серверы доступа и другое);
- рабочие станции;
- серверы;
- средства защиты ИБ (системы выявления атак, межсетевые экраны, антивирусные системы и другие).

1.2.1. Коммуникационное или сетевое оборудование

Коммуникационное или сетевое оборудование — устройства, необходимые для работы компьютерной сети, например: маршрутизатор, коммутатор, концентратор, коммутационная панель и др. Можно выделить активное и пассивное сетевое оборудование.

Активное оборудование — это оборудование, содержащее электронные схемы, получающее питание от электрической сети или других источников питания (батарейки, аккумулятора, солнечной панели, генератора и т. д.) и выполняющее функции преобразования, усиления сигналов и иные. Это определяет способность такого оборудования обрабатывать сигнал по специальным алгоритмам. В сетях происходит пакетная передача данных. Каждый сетевой пакет, помимо передаваемых данных, содержит, также, техническую информацию: сведения о его источнике, цели, целостности информации и другие, позволяющие доставить пакет по назначению. Активное сетевое оборудование не только улавливает и передает сигнал, но и обрабатывает эту техническую информацию, перенаправляя и распределяя поступающие потоки в соответствии со встроенными в память устройства алгоритмами. Эта «интеллектуальная» особенность, наряду с питанием от сети, является признаком активного оборудования. Например, в состав активного оборудования включаются следующие типы устройств:

1 Сетевой адаптер — плата, которая устанавливается в компьютер и обеспечивает его подсоединение к локальной вычислительной сети.

2 Коммутатор (свитч) (многопортовый мост) — устройство с несколькими (4-32) портами, обычно используемое для объединения нескольких рабочих групп ЛВС.

3 Маршрутизатор (роутер) — используется для объединения нескольких рабочих групп ЛВС, позволяет осуществлять фильтрацию сетевого трафика, разбирая сетевые (IP) адреса.

4 Ретранслятор — используется для создания усовершенствованной беспроводной сети с большей площадью покрытия и представляет собой альтернативу проводной сети. По умолчанию устройство работает в режиме усиления сигнала и выступает в роли ретрансляционной станции, которая улавливает радиосигнал от базового маршрутизатора сети или точки доступа и передает его на ранее недоступные участки.

5 Медиаконвертер — устройство, как правило, с двумя портами, обычно используемое для преобразования среды передачи данных (коаксиал-витая пара, витая пара-оптоволокно).

6 Сетевой трансивер — устройство, как правило, с двумя портами, обычно используемое для преобразования интерфейса передачи данных.

Пассивное сетевое оборудование — оборудование, не получающее питание от электрической сети или других источников питания (батарейка, аккумулятор, солнечная панель, генератор, др) и выполняющее функции распределения или снижения уровня сигналов. Например, кабельная система: кабель (коаксиальный и витая пара), вилка/розетка, коммутационная панель, симметрирующие устройство, преобразующие электрический сигнал из симметричного в несимметричный и наоборот для коаксиальных кабелей и т. д. Также, к пассивному оборудованию иногда относят оборудование трассы для кабелей: кабельные лотки, монтажные шкафы и стойки, телекоммуникационные шкафы.

1.2.2. Рабочие станции

Рабочие станции — комплекс аппаратных и программных средств, предназначенных для решения определённого круга задач. Рабочая станция как место работы специалиста представляет собой полноценный компьютер или компьютерный терминал, набор необходимого ПО, по необходимости дополняемые вспомогательным оборудованием: печатающее устройство, внешнее устройство хранения данных на магнитных и/или оптических носителях, сканер штрих-кода и прочим. Также термином «рабочая станция» обозначают стационарный компьютер в составе локальной вычислительной сети по отношению к серверу. В локальных сетях компьютеры подразделяются на рабочие станции и серверы. На рабочих станциях пользователи решают прикладные задачи: работают в базах данных, создают документы, делают расчёты, играют в компьютерные игры. Сервер обслуживает сеть и предоставляет собственные ресурсы всем узлам сети, в том числе и рабочим станциям.

1.2.3. Серверы

Сервер — компьютер (или специальное компьютерное оборудование), выделенный из группы персональных компьютеров (или рабочих станций) для выполнения какой-либо сервисной задачи без непосредственного участия человека. Сервер и рабочая станция могут иметь одинаковую аппаратную конфигурацию, так как различаются лишь по участию в своей работе человека за консолью. Некоторые сервисные задачи могут выполняться на рабочей станции параллельно с работой пользователя. Такую рабочую станцию условно называют невыделенным сервером. Консоль и участие человека

необходимы серверам только на стадии первичной настройки, при аппаратно-техническом обслуживании и управлении в нештатных ситуациях (штатно, большинство серверов управляются удалённо). Для нештатных ситуаций серверы обычно обеспечиваются одним консольным комплектом на группу серверов

1.2.4. Средства защиты ИБ

Понятие «информационная безопасность» включает комплекс мер, направленных на предупреждение и устранение несанкционированного доступа, обработки, искажения, форматирования, анализа, несогласованного обновления, корректирования и уничтожения данных. Проще говоря, это комплекс действий, стандартов и технологий, необходимых для защиты конфиденциальных данных. Цель защиты информации – сохранить данные и целостность системы, минимизировать потери в случае искажения информационных сведений. Сотрудники отделов информационной безопасности компании с помощью специального ПО могут отследить любое действие в корпоративной системе – создание, изменение, удаление, копирование и распространение важных файлов. Для правильного внедрения средств обеспечения защиты конфиденциальной информации компании требуется соблюдать три основных принципа:

1 **Целостность.** Механизмы контроля должны работать в комплексе. Соблюдение принципа целостности обеспечивает отсутствие искажения данных и защиту от несанкционированных изменений.

2 **Конфиденциальность.** Введение мер контроля для создания адекватного уровня защиты данных, активов и информационной безопасности компании на различных этапах бизнес-операций, а также для устранения угрозы неправомерного доступа к корпоративной информации. Важно сохранять конфиденциальность при хранении информации, а также при передаче данных фирмам-посредникам, независимо от их степени важности.

3 **Доступность.** Обеспечение уполномоченных сотрудников нужной им информацией. Локальная сеть должна вести себя последовательно, чтобы в случае необходимости иметь доступ к цифровым данным. Важным моментом является восстановление системы после любых сбоев, когда речь идет о доступе к данным. Метод восстановления не должен негативно влиять на функциональность предприятия. Без соблюдения вышеперечисленных принципов защита информации невозможна.

На практике обеспечение информационной безопасности фирмы осуществляется с помощью следующих средств:

1 **Моральные средства защиты.** Под моральными средствами подразумевают нормы поведения и правила работы с информационными активами, сложившиеся по мере распространения и внедрения электронной тех-

ники в различных отраслях государства и общества в целом. По факту это необязательные требования в отличие от законодательно утвержденных. Однако их нарушение приведет к потере репутации человека и организации. К морально-этическим средствам защиты информации в первую очередь стоит отнести честность и порядочность сотрудников. В каждой организации есть свой свод правил и предписаний, направленный на создание здорового морального климата в коллективе. Механизмом обеспечения безопасности служит внутренний документ компании, учитывающий особенности деловых процессов и информационной структуры, а также устройство ИТ-системы.

2 Правовые средства защиты Они основываются на действующих в Российской Федерации законах, решениях и нормативных актах, устанавливающих правила обработки персональных данных, гарантирующих права и обязанности участникам при работе с информационными ресурсами в период их обработки и использования, а также возлагающих ответственность за нарушение этих постановлений, тем самым устранив угрозу несогласованного использования конфиденциальной информации. Такие правовые методики используются в качестве профилактических и предупреждающих действий. В основном это организованные пояснительные беседы с персоналом предприятия, пользующимся корпоративными электронными устройствами.

3 Организационные средства Это часть администрирования организации. Они регулируют функционирование системы обработки информации, работу штата организации и процесс взаимодействия работников с системой так, чтобы в большей степени устранить или предупредить угрозу информационной атаки либо уменьшить потери в случае их возникновения. Основной целью организационных мер является формирование внутренней политики в области сохранения в секрете конфиденциальных данных, включающей использование необходимых ресурсов и контроль за ними. Внедрение политики конфиденциальности включает реализацию средств контроля и технических устройств, а также подбор персонала службы внутренней безопасности. Возможны изменения в устройстве ИТ-системы, поэтому в реализации политики конфиденциальности должны участвовать системные администраторы и программисты. Персонал должен знать, почему проблемы сохранения коммерческой тайны столь важны. Все работники предприятия должны пройти обучение правилам работы с конфиденциальной информацией.

4 Физические средства защиты Это различные типы механических и электронно-механических устройств для создания физических препятствий при попытках нарушителей воздействовать на компоненты автоматизированной системы защиты информации. Это также технические устройства охранной сигнализации, связи и внешнего наблюдения. Средства физической безопасности направлены на защиту от стихийных бедствий, пандемий, военных действий и других внезапных происшествий.

5 Аппаратные средства защиты Это электронные устройства, инте-

грированные в блоки автоматизированной системы или спроектированных как независимые устройства, контактирующие с этими блоками. Их задачей является внутренняя защита структурных компонентов ИТ-систем – процессоров, терминалов обслуживания, второстепенных устройств. Реализуется это с помощью метода управления доступом к ресурсам (идентификация, аутентификация, проверка полномочий субъектов системы, регистрация).

6 Программные методы защиты Обеспечение сетевой безопасности осуществляется за счет специальных программ, которые защищают информационные ресурсы от несанкционированных действий. Благодаря универсальности, простоте пользования, способности к модифицированию программные способы защиты конфиденциальных данных являются наиболее популярными. Но это делает их уязвимыми элементами информационной системы предприятия. Сегодня создано большое количество антивирусных программ, брандмауэров, средств защиты от атак. Путем использования данных категорий программ, подходящим к используемым на предприятии информационным системам, создается комплексное обеспечение сетевой безопасности.

7 Технические способы защиты информационных данных Различные электронные устройства и специализированное оборудование, входящие в единый автоматизированный комплекс организации и выполняющие, как самостоятельные, так и комплексные функции сохранения персональных данных. К ним относятся персонализация, авторизация, верификация, ограничение доступа к активам пользователей, шифрование.

8 Криптографические методы защиты информации Этот метод основывается на способах кодировки и обеспечивает защиту конфиденциальной информации как с помощью программного обеспечения, так и аппаратными средствами защиты информации. Криптографический способ обеспечивает высокую степень эффективности СИЗ. Ее можно выразить в цифровом эквиваленте: среднее количество операций и время для разгадки ключей и расшифровки данных. Для защиты текстов при передаче используются аппаратные методы кодировки, для обмена информацией между ПК локальной сети используются также программные методики. При сохранении информации на магнитных носителях используются программные методы шифровки. Однако у них есть некоторые недостатки: затраты времени и мощности процессоров для шифрования информации, трудности с расшифровкой, высокие требования к обеспечению секретности ключей (угроза открытых ключей от подмены). Информация – это важнейшая часть современной действительности. Именно сейчас цифровые данные подвергаются растущему количеству угроз и нежелательных вторжений. DDoS-атаки, сетевой перехват данных, действие вирусного программного обеспечения и другие киберпреступления становятся более изощренными и набирают обороты. Поэтому следует как можно быстрее реализовать систему защиты информации, которая надежно

защитит конфиденциальную корпоративную информацию. Вопрос безопасности информации полностью лежит на плечах руководства организацией. При выборе соответствующих средств для защиты информации следует принять во внимание область деятельности компании, ее размеры, техническое оснащение, а также компетенции персонала в сфере соблюдения режима конфиденциальности.

1.3. Обзор аналогов ключевого компонента системы управления и мониторинга информационной безопасности компании

Ключевым компонентом в построении системы управления и мониторинга информационной безопасности компании является SIEM-система. Понятие SIEM (Security Information and Event Management) в наши дни достаточно размыто, можно представить, что это процесс, объединяющий сетевую активность в единый адресный набор данных. Сам термин был придуман Gartner в 2005 году, но с тех пор само понятие и все, что к нему относится, претерпело немало изменений. Первоначально аббревиатура представляла собой комбинацию двух терминов, обозначающих область применения ПО: SIM (Security Information Management) — управление информационной безопасностью и SEM (Security Event Management) — управление событиями безопасности.

Существует достаточно много SIEM решений на рынке ПО, рассмотрим несколько из них.

Security QRadar SIEM от IBM регистрирует события с тысяч конечных устройств и приложений, распределенных в сети. Эта система выполняет мгновенную нормализацию и выявляет связь между действиями над необработанными данными, чтобы отличить реальные угрозы от ложных срабатываний.

Плюсы:

1 обнаружение неправильного использования приложений, внутреннего мошенничества и современных небольших угроз, которые можно не заметить среди миллионов событий;

2 выполнение мгновенной нормализации событий и сопоставление их с другими данными, полученными в результате обнаружения угроз, создания отчетов о соответствии требованиям и проведения аудита;

3 сокращение числа событий и потоков с миллиардов до небольшого количества реальных нарушений и определение приоритетов для них в соответствии с угрозой для бизнеса;

4 использование опционального ПО IBM Security X-Force Threat Intelligence для определения действий, связанных с подозрительными IP-адресами, например, при подозрении во вредоносной активности.

Минусы:

- 1 отсутствие мобильных версий;
- 2 отсутствие интеграции с облачными сервисами;
- 3 стоимость.

KOMRAD от «НПО «Эшелон» — это SIEM-система, разработка российской компании ЗАО «НПО «Эшелон». Предназначена для оперативного оповещения и реагирования на внутренние и внешние угрозы безопасности автоматизированных систем, а также контроля выполнения требований по безопасности информации.

Особенности системы:

- 1 централизованный сбор и анализ данных журналов событий систем защиты информации, автоматизированных рабочих мест, серверов и сетевого оборудования;
- 2 удаленный контроль параметров конфигурации и работы отслеживаемых объектов;
- 3 оперативное оповещение и реагирование на внутренние и внешние угрозы безопасности автоматизированной системы;
- 4 контроль выполнения заданных требований по безопасности информации, сбор статистики и построение отчетов по защищенности;
- 5 поддержка технологии взаимодействия с источниками событий: Syslog, Syslog-*ng*, SNMPv2, SNMPv3, Opsec, HTTP, SQL, ODBC, WMI, FTP, SFTP, сокеты Unix/Linux, plain log, SSH, Rsync, Samba(NetBIOS), NFS, SDEE, RDEP, OPSEC, CPMI;
- 6 невысокая стоимость.

Недостатки:

- 1 невозможность масштабирования решения и создания системы мониторинга информационной безопасности произвольного масштаба;
- 2 невозможность разбора событий в произвольном формате с помощью регулярных выражений (RE2) для подключения нестандартных источников событий информационной безопасности.

Tibco Loglogic LogLogic SIEM является модульной системой, состоящей из нескольких частей. LogLogic MX — готовое решение для малого и среднего бизнеса. LogLogic ST — долгосрочное хранение событий. LogLogic SEM — корреляция и оповещение о событиях ИБ. LogLogic LX — моментальный поиск событий. Database Security Manager — активный мониторинг и обнаружение уязвимостей баз данных.

Достоинства:

- 1 сбор событий с более чем 340 источниками;
- 2 корреляция событий и оповещение в режиме реального времени;
- 3 моментальный поиск по данным за последние 90 дней;
- 4 хранение и поиск по данным за 10 лет.

1.4. Вывод

В данном разделе был проведен анализ подходов к разработке системы управления и мониторинга информационной безопасности компании, была установлена структура системы, которая должна максимально удовлетворять потребности пользователя, а именно: своевременно идентифицировать локальные атаки и реагировать на них; в режиме реального времени проверять все транзакции, выявлять подозрительные и блокировать их; своевременно идентифицировать сетевые атаки и реагировать на них; в режиме реального времени производить поиск фишинговых ресурсов и информировать администраторов системы о таковых; инкапсулировать информацию; в режиме реального времени сканировать трафик электронной почты, выявлять подозрительные письма, блокировать их, и информировать об этом сотрудников службы информационной безопасности компании; предоставлять возможность удаленно администрировать рабочие машины; защищать, хранить, и структурировать внутреннюю информацию компании.

2. ПРОЕКТИРОВАНИЕ СИСТЕМЫ УПРАВЛЕНИЯ И МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОМПАНИИ

2.1. Требования к системе в целом

В рамках дипломного проекта поставлена цель разработать систему, которая должна удовлетворять запросам пользователей. Исходя из этого, выделен ряд требований к разрабатываемой системе:

- система не должна оказывать влияние на функционирование систем, подлежащих мониторингу;
- система должна поддерживать возможность хранения событий за последние 365 дней;
- система должна поддерживать возможность быстрого доступа к событиям собранным в течение 90 дней;
- в системе должна быть предусмотрена возможность создания АРМ мониторинга с доступом с использованием веб-интерфейса;
- в системе должна быть предусмотрена возможность синхронизации времени, и маркировки всех событий по времени сервера управления данной системой;
- система должна быть гибкой к изменениям и добавлению новых возможностей и функционала.

2.2. Требования к структуре и функционированию системы

Система должна состоять из следующих структурных компонентов:

- сервер управления (ArcSight Manager);
- сервер коннекторов (агентов) (ArcSight Smart Agent);
- АРМ управления (ArcSight Console).

Сервер управления системы управления и мониторинга информационной безопасности компании должен выполнять следующие функции: обработку поступающих с агентов событий аудита; управление коннекторами; управление учётными записями пользователей системы; хранение получаемых событий (при этом события хранятся как на встроенных в сервер управления дисках, так и на отдельном дисковом хранилище, подключённом к серверу консолидации событий).

Сервер коннекторов системы мониторинга и управления информационной безопасности компании является компонентом системы, на котором функционирует специализированное ПО сбора событий.

При помощи АРМ управления осуществляется управление и контроль системы.

2.3. Требования к надежности системы

Проектируемая и внедряемая системы мониторинга и управления информационной безопасности компании не должна уменьшать показатели надёжности информационных систем компании. Уровень надёжности разрабатываемой системы должен обеспечивать режим круглосуточного функционирования системы. Процедуры регламентного обслуживания с указанием времени их проведения должны быть отражены в рабочей документации. Должны быть предусмотрены процедуры резервного копирования собираемых данных аудита на внешние носители.

2.4. Требования к защите от несанкционированного доступа в систему

Каждый пользователь должен иметь уникальный идентификатор (логин) и пароль для входа в систему. Должна быть предусмотрена обязательная предварительная регистрация пользователя уполномоченным лицом. Для доступа к журналам аудита в наблюдаемых системах должны создаваться технологические учётные записи, права доступа к данным, для которых присваиваются на основании принципа минимума привилегий. При использовании данных учётных записей, система получает только возможность работы с журналом аудита наблюдаемых систем, без возможности чтения и/или изменения хранимых в системах основных данных. Функционал системы не должен предоставлять возможность получения доступа к данным автоматизированной системы компании, обрабатывая только события аудита, не затрагивая сами данные автоматизированной системы компании. Реализация механизмов идентификации и аутентификации должна удовлетворять следующим требованиям: доступ пользователю к АРМ управления системой должен предоставляться пользователю только после предъявления уникального персонализированного идентификатора (имени) пользователя и проведения процедуры аутентификации на основе некоторой вводимой пользователем информации (пароль, ключи), при этом должна быть предусмотрена возможность смены такой информации по запросу пользователей периодической регламентной сменой пользовательских и административных паролей; должна быть обеспечена возможность определения авторства каждой операции проводимой в системе; при попытке подбора паролей при входе в АРМ системы (неправильный набор пароля три раза подряд), система должна блокировать работу пользователя. Система должна содержать средства управления правами доступа пользователей. Уровень доступа в системе должен быть определён по ролевому признаку (на основе дискретных правил). Должны быть доступны следующие роли: роль администратора системы; роль оператора системы. В системе должен быть предусмотрен механизм администрирова-

ния, предназначенный для выполнения функций по управлению системой. Выполнение административных функций в системе должно быть вынесено на прикладной уровень в виде отдельного АРМ или модуля администратора без возможности доступа к информации систем, подлежащим мониторингу. Должна быть исключена возможность удаления событий из системы, с использованием стандартных средств администрирования системы. Система регистрации событий должна протоколировать следующие действия: создание нового пользователя; назначение пользователю прав доступа к данным и функциям системы, а также изменение прав доступа; входы/выходы пользователей в/из системы; использование специальных полномочий (редактирование информации в базе данных, сторнирование проведенных операций и т.д.).

2.5. Требования к функциональным характеристикам системы

Проектируемая система должна осуществлять сбор событий из журналов событий информационной системы, подлежащих мониторингу, и сохранять результат обработки в централизованной базе данных. Также, система должна обеспечивать выполнение следующих требований: предоставлять функционал агрегации, нормализации и корреляции событий от источников. Параметры агрегации, нормализации и корреляции должны быть настраиваемыми; предоставлять функционал формирования отчётов по событиям, сохраненным в централизованной базе данных. Функционал формирования отчётов должен быть настраиваемым; учитывать подключение в дальнейшем объектов в других временных зонах и корректно обрабатывать переход на летнее/зимнее время; при подключении к источникам событий система должна подчиняться принципу использования наименьших привилегий.

2.6. Требования к модернизации

В системе должна быть предусмотрена возможность модернизации и обновления без потери и уменьшения производительности. Модель системы обязана иметь возможность адаптировать ее к изменяющимся условиям эксплуатации и обеспечивать возможность поэтапного обновления отдельных компонентов.

2.7. Технические требования к реализации

Реализация должна представлять собой систему управления и мониторинга информационной безопасности компании, предоставляющее функциональные возможности по обеспечению круглосуточной информационной безопасности компании.

Взаимодействие с системой должно осуществляться через глобальную сеть Интернет с использованием закрытых каналов передачи данных.

2.8. Вывод

В данном разделе спроектирована модель системы управления и мониторинга информационной безопасности компании. Определены возможности системы, выделены основные сценарии использования.

Разработаны требования к системе в целом, дальнейший план модернизации и дополнению функциональных возможностей, и основные требования к реализации конечной системы. Также сформированы требования к структуре и функционированию системы управления и мониторинга информационной безопасности компании.

Также, структурированы понятия, связанные с разрабатываемой системой. Разобрана архитектура системы и связь между её компонентами.

Разработаны требования к отчётности, планировке и основные требования к реализации конечной системы.

3. РАЗРАБОТКА СИСТЕМЫ УПРАВЛЕНИЯ И МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОМПАНИИ

Структура системы управления и мониторинга информационной безопасности компании отображена на рисунке 3.1



Рисунок 3.1 – Структурная схема системы управления и мониторинга информационной безопасности компании

3.1. Используемые составляющие системы управления и мониторинга информационной безопасности компании

3.1.1. Microsoft Active Directory

Службы Active Directory (AD) - решение от компании Microsoft позволяющее объединить различные объекты сети (компьютеры, сервера, принтеры, различные сервисы) в единую систему. В данном случае AD выступают в роли каталога (базы данных), в котором хранится информация о пользователях, ПК, серверах, сетевых и периферийных устройствах. Для реализации данного решения, необходим специальный сервер - контроллер домена. Именно он будет выполнять функции аутентификации пользователей и устройств в сети, а также выступать в качестве хранилища базы данных. При попытке использовать любой из объектов (ПК, сервер, принтер) сети, выполняется обращение к контроллеру домена, который либо разрешает это действие (есть необходимые права), либо блокирует его.

ЕДИНАЯ ТОЧКА АУТЕНТИФИКАЦИИ. Поскольку контроллер домена Active Directory хранит всю информацию об инфраструктуре и пользователях, вы легко можете использовать его для входа в систему. Так, все данные пользователей (логины и пароли) хранятся в единой базе данных, что существенно упрощает работу с ними. При авторизации все компьютеры обращаются к этой базе данных, благодаря чему вносимые изменения будут применены ко всем компьютерам сети. Также с помощью AD реализуются политики безопасности, благодаря которым можно ограничить (либо разрешить) доступ к определенным серверам.

УДОБНОЕ УПРАВЛЕНИЕ ПОЛИТИКАМИ. С помощью Active Directory можно поделить компьютеры на различные рабочие группы (организационные подразделения). Это существенно упрощает использование инфраструктуры в двух случаях:

1 Изменение существующих настроек группы. Поскольку настройки хранятся в единой базе данных, при их модификации, они будут применены для всех компьютеров, относящихся к этой группе.

2 Добавление нового пользователя. Он автоматически получает установленные для его группы настройки, что существенно ускоряет создание новой учетной записи.

В зависимости от пользователя (учетной записи, которая используется) и его группы можно ввести ограничение на использование функционала операционной системы. Например, можно ограничить установку приложений всем кроме администраторов.

МОНИТОРИНГ СОБЫТИЙ В MICROSOFT ACTIVE DIRECTORY. К системе управления и мониторинга информационной безопасности компании должны быть подключены ресурсы Active Directory и серверы под управлением Microsoft Windows. Мониторинг событий Active Directory и серверов под управлением MS Windows необходимо вести удалённо, используя агент SmartConnector for Windows Event Log — Unified, установленный на сервере агентов ArcSight. Учётная запись, используемая для сбора событий безопасности с сервера агента ArcSight, не должна иметь административных полномочий в метакаталоге Active Directory и на контролируемых серверах. Сбор событий безопасности должен производиться только из журнала безопасности серверов. Для этого пользователю, от имени которого осуществляется мониторинг событий безопасности с сервера агентов ArcSight, должны быть назначены полномочия для удалённого чтения журнала событий. Система мониторинга и управления информационной безопасности компании должна считывать записи аудита Windows о следующих событиях безопасности Active Directory:

- управление учётными записями пользователей, группами, ролями;
- попытки входа с неправильным паролем;
- попытка входа с заблокированным идентификатором;

- попытка доступа к неразрешённым правам и функциям;
- доступ и очистка журналов аудита;
- создание и удаление системных объектов;
- сигналы тревоги или сбоев в системе;
- доступ к файлам.

Должны быть настроены правила корреляции, позволяющие выявлять следующие нарушения безопасности (при условии предоставления штатной системой аудита достаточной информации):

- подбор пароля;
- создание пользователя с последующим удалением в течении не более двух часов;
- назначение пользователю прав доступа (напрямую или включением в группу) с последующим их удалением в течении не более двух часов;
- добавление административных прав доступа пользователю;
- последовательный вход под разными идентификаторами (третя и более) с одного АРМ в течении более двух часов;
- попытка параллельной аутентификации под одним идентификатором;
- отключения опций или функций аудита;
- доступ к файлам, содержащим данные платёжных карт.

Администратор безопасности должен иметь возможность задавать временной интервал и количество отказов, вызывающих создание инцидента.

3.1.2. Система ORACLE Database 10g

Oracle Database 10g — база данных, разработанная специально для работы в сетях распределенных вычислений. Oracle Database 10g предназначена для эффективного развертывания на базе различных типов оборудования, от небольших серверов до Oracle Enterprise Grid мощных многопроцессорных серверных систем, от отдельных кластеров до корпоративных распределенных вычислительных систем.

Oracle Database 10g позволяет пользователям виртуализировать использование аппаратного обеспечения - серверов и систем хранения данных. Oracle Database 10g обладает технологиями, которые позволяют администраторам надежно хранить и быстро распределять и извлекать данные для пользователей и приложений, работающих в сетях Grid. Oracle Database 10g значительно повышает производительность обработки данных и включает в себя удобные средства администрирования.

Oracle Database 10g предоставляет возможность автоматической настройки и управления, которая делает ее использование простым и экономически выгодным. Ее уникальные возможности осуществлять управление всеми данными предприятия - от обычных операций с бизнес-информацией до динамического многомерного анализа данных (OLAP), операций с документами

формата XML, управления распределенной/локальной информацией - делает ее идеальным выбором для выполнения приложений, обеспечивающих обработку оперативных транзакций, интеллектуальный анализ информации, хранение данных и управление информационным наполнением. Некоторые ключевые возможности Oracle Database 10g:

1 Real Application Cluster (RAC) обеспечивает работу одного экземпляра базы данных на нескольких узлах grid, позволяя управлять нагрузкой и гибко масштабировать систему в случае необходимости.

2 Automatic Storage Management (ASM) позволяет автоматически распределять данные между имеющимися ресурсами систем хранения данных, что повышает отказоустойчивость системы и снижает общую стоимость владения (TCO).

3 Производительность. Oracle Database 10g позволяет автоматически управлять уровнями сервиса и тиражировать эталонные конфигурации в рамках всей сети.

4 Простые средства разработки. Новый инструмент разработки приложений HTML DB позволит простым пользователям создавать эффективные приложения для работы с базами данных в короткие сроки.

5 Самоуправление. Специальные механизмы Oracle Database 10g позволяют самостоятельно перераспределять нагрузку на систему, оптимизировать и корректировать SQL-запросы, выявлять и прогнозировать ошибки.

6 Большие базы данных. Теперь максимальный размер экземпляра базы данных Oracle может достигать 8 экзабайт.

7 Недорогие серверные системы. Oracle Database 10g может использовать недорогие однопроцессорные компьютеры или модульные системы из "серверов-лезвий".

8 В новой версии базы данных реализована поддержка переносимых табличных пространств, система управления потоками данных Oracle Streams и модель распределенных SQL-запросов. Для переноса существующих баз данных в среду Grid в них не потребуется вносить изменений, что позволяет быстро начать использовать все преимущества Oracle Database 10g.

МАСШТАБ ИНФОРМАЦИОННОЙ СИСТЕМЫ И РЕДАКЦИИ СУБД ORACLE. Ядром СУБД является сервер базы данных, который поставляется в одной из четырех редакций (Oracle Database 10g Enterprise Edition, Oracle Database 10g Standard Edition, Oracle Database 10g Standard Edition One, Oracle Database 10g Personal Edition) в зависимости от масштаба информационной системы, в рамках которой предполагается его применение. Для систем масштаба крупной организации предлагается продукт Oracle Database Enterprise Edition (корпоративная редакция), для которого имеется целый набор опций, архитектурно и функционально расширяющих возможности сервера. Продукт Oracle Database Standard Edition (стандартная редакция) ориентирован на организации среднего масштаба или подразделения в составе крупной ор-

ганизации. В рамках десятой версии СУБД Oracle стала доступной еще одна редакция - Standard Edition One, соответствующая функциональным возможностям Standard Edition, но доступная для лицензирования на компьютерах с числом процессоров не более двух. Персональная редакция (Personal Edition) предназначена, как следует из названия, для персонального применения. В стандартной и персональной редакциях основной акцент сделан на невысокую стоимость, простоту установки и сопровождения. При этом все варианты сервера Oracle имеют в своей основе один и тот же код и функционально идентичны, за исключением дополнительных модулей и опций, которые необходимы для специфических конфигураций. Основное преимущество такого подхода к построению СУБД - это идентичность кода для всех вариантов сервера баз данных. Для всех компьютерных платформ и архитектур существует единая СУБД Oracle, поставляемая в различных версиях, которая предоставляет одинаковую базовую функциональность вне зависимости от платформы.

ПОДДЕРЖИВАЕМЫЕ КОМПЬЮТЕРНЫЕ ПЛАТФОРМЫ И АРХИТЕКТУРЫ. Одной из основных характеристик СУБД Oracle является функционирование системы на большинстве платформ, и в том числе на больших ЭВМ, UNIX-серверах, персональных компьютерах и так далее. Другой важной характеристикой является поддержка Oracle всех возможных вариантов архитектур, в том числе симметричных многопроцессорных систем, кластеров, систем с массовым параллелизмом, архитектур майнфреймов. Очевидна значимость этих характеристик для современных организаций, где эксплуатируется множество компьютеров различных моделей и производителей. В таких условиях фактором успеха является максимальная типизация предлагаемых решений, ставящая своей целью существенное снижение стоимости владения программным обеспечением. Унификация систем управления базами данных - один из наиболее значимых шагов на пути достижения этой цели.

Поддержка Oracle большинства популярных компьютерных платформ и архитектур достигается за счет жесткой технологической схемы разработки кода СУБД. Разработку серверных продуктов выполняет единое подразделение корпорации Oracle, изменения вносятся централизовано, после этого все версии подвергаются тщательному тестированию в базовом варианте, а затем переносятся на все платформы, где также детально проверяются. Возможность переноса Oracle обеспечивается специфической структурой исходного программного кода сервера баз данных. Приблизительно 80% программного кода Oracle - это программы на языке программирования C, который (с известными ограничениями) является платформонезависимым. Примерно 20% кода, представляющее собой ядро СУБД, реализовано на машинно-зависимых языках, и эта часть кода перерабатывается для различных платформ. СУБД Oracle скрывает детали реализации механизмов управления дан-

ным на каждой из платформ, что дает основание говорить о практически полной унификации базового программного обеспечения. Дополнительно к этому, архитектура Oracle позволяет переносить прикладные системы, реализованные на одной платформе, на другие платформы без изменений как в структурах баз данных, так и кодов приложений.

КЛАССЫ ПРИЛОЖЕНИЙ. СУБД Oracle в одинаковой степени оптимизирована и для приложений оперативной обработки транзакций, и для аналитических приложений. На практике это означает, что один и тот же продукт (например, Oracle Database Enterprise Edition) можно с успехом использовать и как сервер оперативных баз данных, обрабатывающий интенсивный поток относительно простых и коротких транзакций, поступающих от множества пользователей, так и в качестве сервера хранилища данных, который позволяет концентрировать большие объемы данных и выполнять над ними сложные аналитические вычисления.

ШИРОКИЙ СПЕКТР ТИПОВ ДАННЫХ. Oracle опирается на стандарт SQL-3, позволяющий описывать определения новых типов объектов, состоящих из атрибутов (скалярных - то есть других типов, множеств объектов, ссылок на объекты) и обладающих ассоциированными с ним методами. Любая колонка таблицы может содержать данные базовых или сложных типов, поддерживаются также вложенные таблицы и массивы объектов переменной длины. Одна из отличительных особенностей Oracle - возможность хранения и обработки различных предопределенных типов данных. Данная функциональность интегрирована в ядро СУБД и поддерживается модулем interMedia в составе Oracle Database. Он обеспечивает работу с текстовыми документами, включая различные виды поиска, в том числе контекстного; работу с графическими образами более 20-ти форматов; работу с аудио- и видео информацией. СУБД Oracle не просто предоставляет расширенный набор встроенных типов данных, но и позволяет конструировать новые типы данных со спецификацией методов доступа к ним. Это означает, что разработчики получают в руки не просто систему для хранения и обработки атрибутивных данных в виде таблиц, а инструмент, позволяющий строить структурированные типы данных, непосредственно отображающие сущности предметной области.

КОМПОНЕНТЫ И МОДУЛИ ORACLE DATABASE. Модуль interMedia обеспечивает поддержку всех типов данных, в том числе выполнение операций поиска по большим текстовым документам различных форматов.

Компонент Oracle Enterprise Manager представляет собой универсальное средство администрирования баз данных, снаженное удобным графическим интерфейсом и позволяющее администратору баз данных выполнять широкий спектр операций над множеством баз данных Oracle, включая создание, модификацию и удаление любых объектов внутри каждой из них.

Модуль Distribution Option позволяет эффективно работать с распределенными базами данных и обеспечивает двухфазную фиксацию транзакций

к нескольким базам данных.

Модуль Advanced Replication Option позволяет выполнять репликацию данных в широком диапазоне возможностей, включая синхронную, асинхронную, каскадную и другие типы репликации.

Начиная с версии 8, СУБД Oracle является объектно-реляционной системой. Модуль Objects Option поддерживает объектно-ориентированные возможности: объектные типы, коллекции, массивы, вложенные таблицы, ссылки на объекты и большие бинарные объекты (BLOB).

За счет включения в сервер Oracle модуля 64 Bit Option, Oracle Database работает не только на 32-разрядных, но и на 64-разрядных компьютерах, что существенно расширяет его возможности как по скорости обработки данных, так и по объемам обрабатываемых данных.

Oracle Advanced Queuing (AQ) - встроенный в Oracle Database механизм хранения и обработки очередей сообщений. Компонент AQ относится к классу MOM (Message Oriented Middleware). Наличие такого компонента позволяет построить на базе сервера полнофункциональную инфраструктуру для обработки сообщений и исключает необходимость приобретения для этой цели дополнительных средств третьих фирм (таких как IBM MQ Series), обеспечивая, в то же время, связь с ними в неоднородных средах за счет продукта Oracle Messaging Gateway. AQ обеспечивает асинхронный режим обмена сообщениями между приложениями. AQ предлагает два режима рассылки сообщений: одна точка ко многим (point-to-multipoint) и публикация-подписка (publish/subscribe). AQ позволяет задавать приоритеты сообщений, задавать порядок сообщений в очереди (FIFO или на основе приоритета), группировать сообщения, определять правила доставки и время жизни сообщения, автоматически преобразовывать формат сообщения, получать по электронной почте асинхронные уведомления о прибытии интересующего сообщения, передавать сообщения через HTTP(S). Начиная с версии Oracle8i в состав сервера (во все редакции) включена виртуальная Java-машина (JServer Enterprise Edition).

Oracle Database снабжен всеми необходимыми средствами для подключения клиентских рабочих мест по протоколу Net8 (модуль Networking Kit), для обеспечения работы клиентов по технологии OLE (модуль Objects for OLE), набором ODBC-драйверов (ODBC Driver) и библиотеками для разработки программ на языках третьего уровня, использующих для доступа к базе данных Oracle Call Level Interface (OCI). Oracle Call Interface поддерживает разработку программ с применением вызовов низкоуровневых функций для доступа к базам данных. Это позволяет создавать эффективные программы, требующие минимальных ресурсов. Возможность разработки оптимизированных по скорости и используемой памяти приложений достигается за счет использования вызовов функций, которые предоставляют полный контроль за выполнением операторов SQL и PL/SQL.

Компонент Oracle Objects for OLE предоставляет возможность доступа к базам данных Oracle приложений, разработанных на C++, Microsoft Visual Basic, OLE 2.0. Полная поддержка языка макроопределений в Visual Basic позволяет получать данные из баз данных Oracle непосредственно в электронных таблицах Microsoft Excel.

ORACLE WORKFLOW. Oracle Workflow - это средство для автоматизации стандартных бизнес-процедур организации, ориентированное на разработчиков корпоративных приложений, основанных на технологиях Oracle.

Oracle Workflow предлагает инфраструктуру и средство проектирования (Workflow Builder) для автоматизации прохождения информации произвольного типа, формализации сложных бизнес-правил и включения пользователя в процесс принятия решения. Разработка приложений для управления потоками работ начинается с проектирования алгоритма процесса в графической среде Workflow Builder. Процесс состоит как из стандартных действий, таких как точки входа, выхода, ветвления, уведомления, вложенного процесса, так и действий, специфических для конкретного приложения, функциональность которых реализуется разработчиками. После того, как описания процессов сохранены в репозитории, они могут быть использованы приложениями через программный интерфейс. Дополнительные возможности включают рассылку почтовых уведомлений о результатах работы процесса и представление форм интерактивного взаимодействия пользователей с автоматизированным процессом, например, для получения подтверждений или контроля исполнения поручений.

ORACLE LITE. Oracle Database Lite (ODL) - программный продукт для создания инфраструктуры систем мобильных приложений. В состав продукта входит все необходимое для разработки, установки и управления приложениями для мобильных устройств на всех популярных сейчас ОС: Linux, Unix, Palm OS, Microsoft Windows CE/PPC, и Microsoft Windows NT/2000/XP. Основная задача предлагаемой инфраструктуры - обеспечение надежной и безопасной синхронизации данных между корпоративной базой данных Oracle Database и мобильными клиентами. После первого сеанса синхронизации пользователи, работая на компьютерах, где не было установлено никакого специального программного обеспечения, получают работающие приложения и базу данных ODL с актуальными корпоративными данными. При следующих сеансах связи пользователям передается только измененная информация. ODL - небольшая, но полнофункциональная реляционная база данных, специально спроектированная для работы на мобильных устройствах, в которой полностью реализованы механизмы транзакций, ссылочной целостности и спецификации языка SQL.

Бизнес-логика - хранимые процедуры и триггеры - разрабатывается на Java. Mobile Server - это расширение Oracle AS 10g, этот компонент обеспечивает взаимодействие мобильных приложений с Oracle Database 10g или с

различными Интернет-приложениями. При синхронизации данных, в случае разрыва соединения, передача информации на мобильные устройства возобновится после восстановления связи именно с той точки, где она прервалась. Применение Mobile Server обеспечивает гарантированную доставку данных. Информация, которая передается по сети и хранится в базе данных, может быть зашифрована по алгоритмам FIPS-140, удовлетворяющим стандартам AES. Синхронизация данных между базой данных Oracle Lite 10g и Oracle Database осуществляется по протоколам TCP/IP, HTTP, CDPD, 802.11b Wireless LAN, PPP, GPRS, HotSync, ActiveSync. Программный интерфейс Open Transport API дает возможность использовать любой беспроводной транспортный протокол для синхронизации. Мобильные приложения разрабатываются с помощью Mobile Development Kit на языках программирования C, C++, Java, Visual Basic, с использованием ActiveX Data Objects (ADO), в инструментальных средах Oracle JDeveloper 10g, Microsoft Visual Studio.Net 2003, Microsoft EVT 3.0, Borland Delphi, Sybase Power Builder, Metroworks CodeWarrior 8+, Rapid Software Formation. Приложения, работающие на мобильных устройствах, имеют доступ к Oracle Lite 10g через различные программные интерфейсы (JDBC, ODBC, ADOCE, ADO.Net, SODA Stateless Object Database Access).

Уникальная опция ODL - Web-to-Go дает возможность приложениям, работающим через Web-навигатор, переключаться с режима прямого соединения на режим автономной работы. Пользователь в таком случае, синхронизировав локальные данные с информацией на корпоративном сервере, продолжает работать и при разрыве соединения.

МОНИТОРИНГ СОБЫТИЙ В СИСТЕМЕ ORACLE 10G. К системе управления и мониторинга информационной безопасности компании необходимо подключить СУБД Oracle. Мониторинг событий данной СУБД необходимо осуществлять удаленно, используя агент SmartConnector for Oracle Audit DB, установленный на сервере агентов ArcSight. Система управления и мониторинга информационной безопасности компании должна считывать записи аудита Oracle о следующих событиях безопасности СУБД Oracle:

- управление учётными записями пользователей, группами, ролями;
- попытки входа с неправильным паролем;
- попытка входа с заблокированным идентификатором;
- попытка доступа к объектам СУБД.

Должны быть настроены правила корреляции, позволяющие выявлять следующие нарушения безопасности (при условии предоставления штатной системой аудита достаточной информации):

- подбор пароля;
- создание пользователя с последующим удалением в течении не более двух часов;
- назначение пользователю прав доступа (напрямую или включением в группу) с последующим их удалением в течении не более двух часов;

- добавление административных прав доступа пользователю;
- последовательный вход под разными идентификаторами (тремя и более) с одного АРМ в течении более двух часов;
- отключения опций или функций аудита;
- доступ к таблицам, содержащим данные платёжных карт.

Администратор безопасности должен иметь возможность задавать временной интервал и количество отказов.

3.1.3. Система антивирусной защиты Symantec Endpoint Protection

Symantec Endpoint Protection — это программное обеспечение, для эффективной защиты конечных точек ИТ-инфраструктуры компаний. Данное решение обеспечивает усиленную защиту, предотвращая информационные атаки на физические и виртуальные среды. На рисунке 3.2 представлен интерфейс системы Symantec Endpoint Protection.



Рисунок 3.2 – Интерфейс системы Symantec Endpoint Protection

Прозрачное внедрение необходимых инструментов безопасности в один агент с единой консолью управления, добавляет Symantec Endpoint Protection полезные функции, которые абсолютно не влияют на производительность системы. Использование сети Global Intelligence Network позволяет оперативно получать информацию о новых угрозах и реагировать на них в автоматическом режиме.

Основные функции Symantec Endpoint Protection:

1 Эффективная защита от вирусов и шпионских программ. Решение обеспечивает эффективную защиту от вирусов, руткитов, червей, ботов, троянских и шпионских программ, а также, от новых угроз.

2 Превентивное определение угроз. Благодаря технологиям Insight и SONAR, программное обеспечение распознает новые и быстро меняющиеся программы, содержащие вредоносный код, а также, ранее неизвестные угрозы.

зы и блокирует их работу.

3 Управление на основе интеллекта. Автоматизация процессов и централизованное управление предоставляют достоверные сведения об угрозах и мгновенно реагируют на них.

4 Новейшая защита от сетевых угроз. Функция блокировки общих точек уязвимости и защита браузера обеспечивают эффективную защиту от сетевых атак и несанкционированной загрузки приложений, межсетевой экран выполняет свою работу на основании установленных правил.

Основные возможности Symantec Endpoint Protection:

1 Технология SONAR 3 анализирует запущенные программы, определяет и блокирует вредоносный код, как в известных, так и новых, ранее неизвестных угрозах в режиме реального времени.

2 Решение Symantec Insight позволяет классифицировать файлы на безопасные и подверженные угрозам и более точно обнаруживать программы, содержащие вредоносный код на уровне персональных компьютеров, ноутбуков, которые работают на платформах Windows и Mac, а также, серверов и шлюзов. Данная технология является нечто большим, нежели обычный антивирус.

3 Почти 100% выявление спама и предотвращение утечки данных, благодаря расширенной фильтрации содержимого файлов, которая позволяет определять и блокировать перемещение важной информации по электронной почте и посредством мгновенных сообщений.

4 Более точный анализ, базирующийся на глобальной мировой гражданской сети анализа угроз, обеспечивает четкое представление локальной и сетевой ситуации с угрозами.

5 Системы защиты для виртуальных сред осуществляют надежную защиту виртуальной инфраструктуры, выявляют виртуальные клиенты и управляют ими в автоматическом режиме.

6 Защита веб-шлюзов от различных сетевых угроз.

МОНИТОРИНГ СОБЫТИЙ В СИСТЕМЕ АНТИВИРУСНОЙ ЗАЩИТЫ SYMANTEC ENDPOINT PROTECTION. К системе управления и мониторинга информационной безопасности компании необходимо подключить сервер антивирусной защиты Seserver. Мониторинг событий в системе антивирусной защиты Symantec Endpoint Protection выполняется удалённо, с использованием агента Smart Connector for Symantec Endpoint Protection DB, установленного на сервере агентов ArcSight.

Система управления и мониторинга информационной безопасности компании должна фиксировать следующие события безопасности системы Symantec Endpoint Protection:

- события обнаружения вирусов;
- события обновлений антивирусных баз;
- события запуска/остановки клиентских модулей;

- события изменения конфигурации;
- обнаружение рисков безопасности;
- журналирование сетевого трафика (при наличии соответствующих политик в ПО Symantec Endpoint Protection);
- обнаружение вредоносного ПО.

Должны быть настроены правила корреляции, позволяющие выявлять следующие нарушения безопасности: обнаружение вирусных эпидемий и выявление нарушений политики антивирусной защиты.

3.1.4. Система антивирусной защиты Kaspersky Business Security

В связи со стремительным развитием информационных технологий Все большее коммерческих операций выполняется в электронной форме, поэтому необходимо следить за безопасностью каждого устройства, находящегося в сети. Программное решение Kaspersky Business Security объединяет в себе многоуровневые технологии с гибким управлением в облаке и централизованными средствами контроля программ, веб-контроля и контроля устройств для решения вышеуказанной задачи. Также, данное ПО решает следующие задачи:

- 1 защита от новейших угроз, в том числе от безфайловых вирусов;
- 2 укрепление безопасности рабочих мест и снижение уязвимости к кибератакам;
- 3 повышение производительности и защита сотрудников с помощью инструментов контроля;
- 4 защита серверов и рабочих мест без ущерба для производительности;
- 5 защита различных платформ – Windows, Mac, Linux, iOS и Android;
- 6 простое управление безопасностью из единой консоли.

МОНИТОРИНГ СОБЫТИЙ В СИСТЕМЕ АНТИВИРУСНОЙ ЗАЩИТЫ KASPERSKY BUSINESS SECURITY. К системе управления и мониторинга информационной безопасности компании должны быть подключены серверы антивирусной защиты Kaspersky Business Security. Мониторинг событий в системе антивирусной защиты Kaspersky Business Security выполняется удалённо, с использованием агента FlexConnector для KAV 8, установленного на сервере агентов ArcSight. Система управления и мониторинга информационной безопасности компании должна фиксировать следующие события безопасности системы Kaspersky Business Security:

- события обнаружения вирусов;
- события обновлений антивирусных баз;
- события запуска/остановки клиентских модулей;
- события изменения конфигурации.

Должны быть настроены правила корреляции, позволяющие выявлять следующие нарушения безопасности (при условии предоставления штатной системой аудита достаточной информации): обнаружение вирусных эпидемий и выявление нарушений политики антивирусной защиты.

3.1.5. Сервера MS Forefront UAG

Microsoft Forefront Unified Access Gateway (UAG) — это программный пакет, обеспечивающий безопасный удаленный доступ к корпоративным системам для удаленных сотрудников и деловых партнеров. Его услуги включают обратный прокси-сервер, виртуальную частную сеть (VPN), DirectAccess и службы удаленных рабочих столов. UAG является частью предложения Microsoft Forefront. Microsoft прекратила выпуск продукта в 2014 году, хотя функция прокси веб-приложения в Windows Server 2012 R2 и более поздних версиях предлагает некоторые из своих функций.

МОНИТОРИНГ СОБЫТИЙ В СЕРВЕРАХ MS FOREFRONT UAG. К системе управления и мониторинга информационной безопасности компании должны быть подключены серверы MS Forefront UAG. Мониторинг событий выполняется удалённо, с использованием агента FlexConnector для MS Forefront UAG, установленного на сервере агентов ArcSight. Система управления и мониторинга информационной безопасности компании должна фиксировать следующие события прокси-серверов MS Forefront UAG: фильтрация сетевых пакетов и доступ к сети Интернет.

Должны быть настроены компоненты системы управления и мониторинга информационной безопасности компании, позволяющие выявлять следующие показатели (при условии предоставления штатной системой аудита достаточной информации):

- основные получатели трафика;
- основные отправители трафика;
- основные запрошенные URL;
- основные пропущенные/заблокированные запросы;
- доступ к серверам, содержащим данные платёжных карт.

3.1.6. Прокси-сервер Squid

В корпоративных сетях довольно обычна ситуация, когда, с одной стороны, множество пользователей на разных компьютерах пользуются ресурсами сети Интернет, при этом обеспечить надлежащий уровень безопасности на этих компьютерах одновременно довольно сложно. Ещё сложнее заставить пользователей соблюдать некий «корпоративный стандарт», ограничивающий возможности использования Интернет (например, запретить использование определённого типа ресурсов или закрыть доступ к некоторым адресам).

Простейшим решением будет разрешить только определённые методы доступа к Интернет (например, по протоколам HTTP и FTP) и определить права доступа абонентов на одном сервере, а самим абонентам разрешить только обращение к этому серверу по специальному прокси-протоколу (поддерживается всеми современными браузерами). Сервер же, после определения прав доступа, будет транслировать (проксировать) приходящие на него HTTP-запросы, направляя их адресату. Допустим, несколько пользователей с нескольких компьютеров внутренней сети просматривают некоторый сайт. С точки зрения этого сайта их активность представляется потоком запросов от одного и того же компьютера.

МОНИТОРИНГ СОБЫТИЙ В ПРОКСИ-СЕРВЕРЕ SQUID. К системе управления и мониторинга информационной безопасности компании необходимо подключить сервер Squid. Мониторинг событий выполняется удалённо, с использованием агента FlexConnector для Squid SAMS, установленного на сервере агентов ArcSight. Система управления и мониторинга информационной безопасности компании должна фиксировать следующие события прокси-серверов Squid: доступ к сети Интернет.

Должны быть настроены компоненты системы управления и мониторинга информационной безопасности компании, позволяющие выявлять следующие показатели (при условии предоставления штатной системой аудита достаточной информации):

- основные пользователи-генераторы трафика;
- основные сайты-генераторы трафика;
- основные запрошенные URL;
- объём полученной и отправленной информации.

3.1.7. СУБД MS SQL Server

Microsoft SQL Server — это ПО, которое работает на различных устройствах, таких как: персональный компьютер, ноутбук, виртуальная машина, сервер и даже "облако". К MS SQL Server можно подключаться локально или по сети, отправить команду по специальному протоколу TDS и, соответственно, получить ответ. Также, данная СУБД позволяет хранить и обрабатывать большой объём информации. Все что она делает это открывает сетевой порт, принимает запрос пользователя и даёт на данный запрос ответ. При работе в локальной сети, необходимо установить ПО MS SQL Server на каждую рабочую машину.

Центральным аспектом в MS SQL Server, как и в любой СУБД, является база данных. База данных представляет хранилище данных, организованных определенным способом. Нередко физически база данных представляется файлом на жестком диске, хотя такое соответствие необязательно. Для хранения и администрирования баз данных применяются системы управления базами данных или СУБД. И как раз MS SQL Server является одной из таких СУБД.

Также, бывают различные виды SQL-сервером. На сегодняшний день наиболее популярными являются следующие СУБД:

1 MS SQL server — многопользовательский программный продукт, разработанный компанией Microsoft, обладающий высокой производительностью и отказоустойчивостью, тесно интегрированный с ОС Windows. Этот сервер поддерживает удаленные подключения, работает с многими популярными типами данных, дает возможность создавать триггеры и хранимые данные, имеет практические и удобные утилиты для настройки.

2 Oracle Database server — СУБД, предназначенная для создания, консолидации и управления базами данных в облачной среде. Используя этот сервер, можно как автоматизировать обычные бизнес-операции, так и выполнять динамический многомерный анализ данных, проводить операции с документами xml-формата и управлять разделенной и локальной информацией.

3 IBM DB2 - семейство СУБД для работы с реляционными базами данных, признанное самым производительным, имеющим высокие технические показатели и возможности масштабирования. SQL-серверы этой группы характеризуются мультиплатформенностью, способностью к мгновенному созданию резервных копий и восстановлению БД, реорганизации таблиц в онлайн-режиме, разбиению баз данных, определению пользователями новых типов данных.

4 MySQL - СУБД, разработанная и поддерживаемая компанией Oracle. В основном она используется локальными или удаленными клиентами, позволяя им работать с таблицами разных типов, поддерживающих полнотекстовый поиск или выполняющих транзакции на уровне отдельных записей.

5 PostgreSQL - СУБД с открытым исходным кодом, работающая с объектно-

реляционными (поддерживающими пользовательские объекты) базами данных. Также PostgreSQL предназначена для создания, хранения и извлечения сложных структур данных. Она поддерживает самые различные типы данных (среди них - числовые, текстовые, булевы, денежные, бинарные данные, сетевые адреса, xml и другие).

При работе с MS SQL Server был выявлен ряд положительных свойств системы, таких как: производительность, так как SQL Server работает очень быстро; надежность и безопасность, так как SQL Server предоставляет шифрование данных; простота, так как с данной СУБД относительно легко работать и вести администрирование.

МОНИТОРИНГ СОБЫТИЙ В СУБД MS SQL SERVER. К системе управления и мониторинга информационной безопасности компании необходимо подключить серверы СУБД MS SQL Server. Мониторинг событий безопасности выполняется удалённо, с использованием агента SmartConnector for Microsoft SQL Server Multiple Instance Audit DB, установленного на сервере агентов ArcSight. Для выявления событий, свидетельствующих о нарушении ИБ, должен быть включён аудит событий в контролируемых базах MS SQL Server. Система управления и мониторинга информационной безопасности компании должна считывать записи аудита MS SQL Server о следующих события безопасности:

- вход пользователя в СУБД;
- выход пользователя из СУБД;
- ошибка аутентификации при подключении к СУБД;
- создание пользователя СУБД;
- использование привилегий администратора при работе с СУБД;
- доступ к объектам СУБД.

На рисунке 3.3 продемонстрирована схема источников данных в системе мониторинга и управления информационной безопасностью банка.



Должны быть настроены правила корреляции, позволяющие выявлять следующие нарушения безопасности (при условии предоставления штатной системой аудита достаточной информации):

- подбор пароля;
- создание пользователя с последующим удалением в течении не более двух часов;
- добавление административных прав доступа пользователю;
- последовательный вход под разными идентификаторами (три и более) с одного АРМ в течении не более двух часов;
- доступ к таблицам, содержащим данные платёжных карт.

3.1.8. Система OpenWAY

Система OpenWAY используется для эмиссии и эквайринга карт, маршрутизации транзакций и омни-канальных платежей. С помощью данного ПО собирается, обрабатывается, и хранится информация о платежах. Также, на основании собранной информации можно сформировать отчёт.

МОНИТОРИНГ СОБЫТИЙ В СИСТЕМЕ OPENWAY. К системе управления и мониторинга информационной безопасности компании необходимо подключить системы OpenWAY. Мониторинг событий безопасности выполняется удалённо, используя агент FlexConnector for OpenWAY, установленный на сервере агентов ArcSight. Система управления и мониторинга информационной безопасности компании должна считывать записи аудита системы OpenWAY о следующих событиях безопасности:

- управление учётными записями пользователей, группами, ролями;
- выход пользователя из СУБД;
- использование привилегий администратора при работе с системой (доступ к журналам аудита, их очистка);
- попытка входа с неправильным паролем;
- попытка входа с заблокированным идентификатором;
- доступ к объектам.

Должны быть настроены правила корреляции, позволяющие выявлять следующие нарушения безопасности (при условии предоставления штатной системой аудита достаточной информации):

- подбор пароля;
- создание пользователя с последующим удалением в течении не более двух часов;
- назначение пользователю прав доступа (напрямую или включением в группу) с последующим их удалением в течении не более двух часов;
- добавление административных прав пользователю;
- последовательный вход под разными идентификаторами (три и более) с одного АРМ в течении не более двух часов;

- отключение опций или функций аудита;
- доступ к объектам, содержащим данные платёжных карт.

Администратор безопасности должен иметь возможность задавать временной интервал и количество отказов.

3.1.9. Операционная система Linux

Операционная система Linux — это семейство ОС, работающих на основе одноименного ядра, которое включает в себя множество различных дистрибутивов, как для общего пользования, так и для узкого применения. Над дистрибутивами операционной системы Linux работает большая децентрализованная команда активичтов, поэтому данная ОС распространяется абсолютно бесплатно и с открытым исходным кодом. На рисунке 3.4, рисунке 3.5 и рисунке 3.6 представлены интерфейсы различных дистрибутивов операционной системы Linux.



Рисунок 3.4 – Интерфейс операционной системы Linux Ubuntu



Рисунок 3.5 – Интерфейс операционной системы Linux Alpine



Рисунок 3.6 – Интерфейс операционной системы Kali Linux

МОНИТОРИНГ СОБЫТИЙ В ОПЕРАЦИОННОЙ СИСТЕМЕ LINUX.
К системе управления и мониторинга информационной безопасности компании необходимо подключить серверы под управлением ОС Linux. Мони-

торинг событий в ОС Linux необходимо осуществлять удалённо, используя агент ArcSight Syslog Daemon, установленный на сервере агентов ArcSight. Система управления и мониторинга информационной безопасности компании должна фиксировать следующих событиях безопасности ОС Linux:

- вход пользователя в систему;
- создание пользователя;
- использование привилегий администратора при работе с системой (доступ к журналам аудита, их очистка);
- изменение уровня привилегий пользователя;
- доступ к файлам.

Должны быть настроены правила корреляции, позволяющие выявлять следующие нарушения безопасности (при условии предоставления штатной системой аудита достаточной информации):

- подбор пароля;
- создание пользователя с последующим удалением в течении не более двух часов;
- назначение пользователю прав доступа (напрямую или включением в группу) с последующим их удалением в течении не более двух часов;
- добавление административных прав пользователю;
- последовательный вход под разными идентификаторами (три и более) с одного АРМ в течении не более двух часов;
- отключение опций или функций аудита;
- доступ к объектам, содержащим данные платёжных карт.

Администратор безопасности должен иметь возможность задавать временной интервал и количество отказов.

3.1.10. SIEM - система ArcSight ESM от Micro Focus

Процесс мониторинга является одним из основных процессов в области информационной безопасности. Для достижения максимального эффекта мониторинг необходимо производить круглосуточно. Также, целью процесса является непрерывная регистрация, анализ и контроль событий безопасности. Под событием безопасности понимается событие, о котором просигнализировало некоторое средство защиты. Средством защиты выступает программно-аппаратный комплекс, утвержденный на предприятии. Сообщения об инциденте информационной безопасности поступают оператору безопасности, который оценивает данное сообщение и принимает решение о дальнейших действиях.

На рисунке 3.7 представлен интерфейс сетевого монитора SIEM ArcSight.



Рисунок 3.7 – Интерфейс сетевого монитора SIEM ArcSight

На рисунке 3.8 представлен интерфейс менеджера событий SIEM ArcSight.



Рисунок 3.8 – Интерфейс менеджера событий SIEM ArcSight

Результаты процесса мониторинга передаются в процесс разрешения инцидентов для идентификации инцидентов ИБ и их обработки. Под инцидентом ИБ понимается событие безопасности, которое привело (либо может привести) к негативным последствиям. Также события безопасности являются исходными данными при анализе эффективности системы и могут помочь оценить соответствие функционирования системы требованиям ИБ.

На рисунке 3.9 представлена схема жизненного цикла события в ArcSight.



Рисунок 3.9 – Схема жизненного цикла события в ArcSight

Задача регистрации подразумевает сбор событий безопасности от средств защиты и их независимое (вынесенное за пределы контролируемых средств защиты) хранения. Доступ к журналам регистрации осуществляется только администраторами безопасности.

Эффективная система мониторинга должна объединять события, собираемые со всех используемых защитных средств, в единую управляемую систему информационной безопасности, оставлять только те, в которых может содержаться полезная информация. Как показывает практика, из миллиона генерируемых записей интерес для администратора безопасности представляют сотни, если не десятки из них.

Вышеперечисленные проблемы способна решить система мониторинга, предоставляющая эффективные средства для анализа событий безопасности, а именно:

- фильтрации данных;
- приоритизации данных;
- нормализации данных;
- агрегирования данных;
- корреляции данных.

На рисунке 3.10 представлен интерфейс активного канала системы мониторинга SIEM ArcSight.

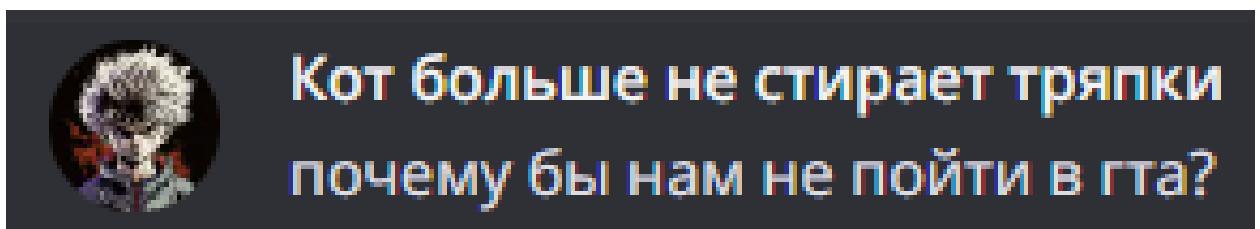


Рисунок 3.10 – Интерфейс активного канала системы мониторинга SIEM ArcSight

Основной целью системы мониторинга событий информационной безопасности в автоматизированной системе является непрерывная регистрация, анализ и контроль событий безопасности.

Событие безопасности — событие, зафиксированное некоторым средством.

Регистрация событий безопасности — перемещение данных журналов из устройств безопасности или их систем управления в единую базу данных.

Анализ событий безопасности — состоит из следующих составных частей: фильтрация данных, приоритизация данных, нормализация данных, агрегация данных, корреляция данных.

Контроль событий безопасности — включает в себя отображение зафиксированных событий безопасности на единой консоли в режиме реального времени, оповещение администраторов безопасности о зафиксированных событиях и формирование отчётов.

В качестве системы, которая бы смогла реализовать рассмотренные выше задачи, рассматривается система корреляции событий ArcSight ESM, которая позволяет собирать и анализировать сообщения о нарушениях безопасности, поступающих от систем обнаружения вторжений, межсетевых экранов, операционных систем, приложений, антивирусных систем и т.д. Данная информация собирается в едином центре, обрабатывается и подвергается анализу в соответствии с заданными правилами по обработке событий, связанных с безопасностью. Результаты анализа в режиме реального времени предоставляются операторам, администраторам и руководящему составу компании в удобном виде для принятия решений по управлению сети.

Программный продукт ArcSight позволяет реализовать рассмотренные выше задачи. Данный продукт состоит из трёх логических уровней: уровень агентов, уровень серверных и дополнительных модулей и уровень взаимодействия с пользователем.

На рисунке 3.11 представлен интерфейс графической формы активного листа SIEM ArcSight.

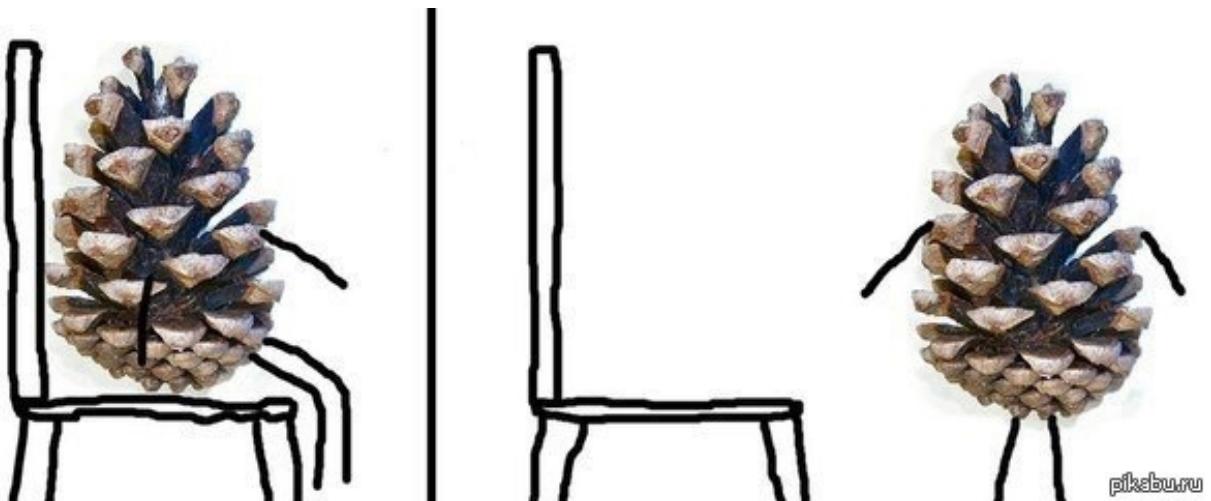


Рисунок 3.11 – Интерфейс графической формы активного листа SIEM ArcSight

Активный лист в SIEM ArcSight предназначен для отображения событий информационной безопасности в реальном времени. Также, активный лист обеспечивает возможность построения зависимостей между событиями с дальнейшим отображением полученной информации.

На рисунке 3.12 изображена блок-схема алгоритма реагирования на инциденты.

РОБЕРТ
ГАЛЛЕРІЯ



В фазе нормализации и агрегирования события безопасности собираются со всех систем обнаружения вторжений: межсетевых экранов, операционных систем, приложений и антивирусных систем, и приводятся к единому формату сообщений в XML. Сформированные сообщения затем коррелируются между собой, используя мощные механизмы корреляции, основанные как на статистических методах корреляции, так и на задаваемых правилах. И, наконец, ArcSight ESM выдает полученные результаты на основанную на технологии Java, интуитивно понятную централизованную консоль,ирующую в режиме реального времени.

ArcSight ESM помогает администраторам безопасности сфокусироваться на реальных угрозах безопасности, обеспечивая их средствами, позволяющими оперативно устранять угрозы безопасности сети. Также, данная SIEM-система поддерживает сбор данных с маршрутизаторов, систем предотвращения вторжений, и производит корреляцию этих данных с информацией, получаемой от межсетевых экранов, серверов, баз данных и многих приложений. В данный момент число типов поддерживаемых устройств — более 200 (показатель больший, чем у Cisco MARS и SIMS вместе взятых).

Ниже приведен перечень основных механизмов функционирования системы ArcSight ESM с подробных описанием.

1 Фильтрация данных — устранение избыточной информации, основываясь на критериях заданных администратором или определенных в системе.

2 Нормализация данных — приведение данных от различных средств защиты к единому виду, единым показателям значимости события. Нормализация также подразумевает устранение избыточной информации, т.е. устранение повторяющихся данных о событии, полученных от разных средств защиты, исключение противоречивости в их хранении.

3 Агрегирование данных — объединение однотипных событий в одно, другими словами это процесс группировки событий по одному или нескольким критериям, то есть последовательность однотипных событий заменяется одним, где в поле "количество" стоит количество агрегированных событий. Некоторые события, например сканирование портов, вызывают генерацию большого количества событий от одного или нескольких устройств. Реально происходит одно событие — сканирование портов.

Механизм агрегации позволяет сгруппировать серию событий и получить одно сообщение, что сильно упрощает анализ и экономит память. В системе возможна группировка по многим параметрам, среди которых:

- устройство, сгенерировавшее сообщение;
- адрес источника;
- адрес получателя;
- порт источника;
- порт получателя;

- внешний тип сообщения;
- внутренний тип сообщения;
- направление;
- процесс;
- имя пользователя.

Агрегация может производиться на множестве внутренних сообщений, а также на множестве сообщений устройств, что повышает точность преобразования. Возможна настройка параметров агрегации (время и критерии сравнения) для каждого типа сообщений.

4 Корреляция данных — способ выявления комплексных атак, т.е. атак, которые не могут быть обнаружены с использованием известных сигнатур IDS, так как фактически состоит из комплекса сигнатур, которые по отдельности не говорят о реальной атаке. Корреляция событий безопасности позволяет также проводить анализ событий на предмет выявления наличия комплекса событий, свидетельствующего об аномальном поведении, реализации угроз, к примеру, обнаружение подбора паролей. Возможны следующие варианты корреляции данных:

- корреляция с данными об операционной системе (например, обнаружение Unix-атаки направленной на ресурс под управлением ОС Windows не является угрозой и может быть проигнорировано администратором);
- корреляция атак и уязвимостей (если при проведении предварительного сканирования ресурсов было определено что определенный узел уязвим к определенному виду атак, то при обнаружении такой атаки направленной на данный ресурс событию будет присвоена высокая степень критичности, при определённой ранее неуязвимости узла — низкая степень критичности);
- анализ шаблона атаки (позволяет сделать вывод о применении того или иного средства реализации атаки);
- сопоставление данных (несколько однотипных событий за заданный период времени объединяются в одно, например, подбор пароля).

В системе ArcSight реализовано два механизма корреляции — статистический и корреляция, основанная на правилах.

Статистическая корреляция — встроенный эвристический механизм, позволяющий производить оценку рисков активов без использования предопределённых правил, основываясь только на данных, полученных от устройств. Администратор системы имеет возможность задать индивидуальные параметры ресурсов, связанные с анализом рисков (значимость, уязвимость, доступность пользователям). В любой момент времени можно сгенерировать отчёты, содержащие значение рисков ресурсов. Причину каждого значения риска можно определить, создав связанные детализированные отчёты.

Корреляция, основанная на правилах — механизм выявления события, соответствующего появлению последовательности событий, удовлетворяющей определенным правилам. В системе созданы правила для наиболее типичных

атак, но имеется возможность создания собственных.

Результатом работы системы корреляции является вывод следующих сообщений:

- вероятно удачная атака (узел уязвим);
- вероятно неудачная атака (узел не уязвим);
- вероятно неудачная атака (блокированы некоторые пакеты, составляющие атаку);
- вероятно неудачная атака (атака не применима к данной операционной системе);
- неудачная атака (узел блокировал атаку);
- воздействие неизвестно (узел не сканировался);
- воздействие неизвестно (операционная система не определена);
- воздействие неизвестно (уязвимость не определена);
- воздействие неизвестно (корреляция не проводилась).

Также в результате работы системы корреляции возможно получение некоторого объединения событий:

- атака со скомпрометированного узла;
- распределенная DoS-атака;
- неудачная попытка входа на множество узлов;
- доступ к ресурсу со взломанного узла;
- удачная попытка входа на взломанный узел;
- попытка взлома просканированного узла;
- скоординированная атака;
- атака с одного узла на множество;
- атака через промежуточный узел.

5 Приоритизация данных — автоматическое присваивание событиям соответствующего уровня, исходя из заданных администратором или определенных в системе критерииев.

6 Категоризация — каждое внутреннее сообщение системы проходит сопоставление с предопределенными значениями и получает какой-либо статус. Например, категория Outcome, может принимать значение Success или Failure. Категоризация расширяет возможности системы генерации отчетов и представления данных на консоли.

7 Визуализация — отображение консолидированных данных в реальном времени на консоли после процессов нормализации, агрегации и корреляции.

Система ArcSight ESM состоит из нескольких раздельно устанавливаемых компонентов, которые совместно обрабатывают события информационной безопасности. К основным компонентам системы мониторинга на базе ПО ArcSight ESM относятся:

- агенты ArcSight SmartConnector;
- модуль ArcSight Manager;
- база данных ArcSight Database;
- консоль управления ArcSight Console;
- web интерфейс ArcSight Web.



Рисунок 3.13 – Схема коммуникации модулей ArcSight

Агенты ArcSight SmartConnectors осуществляют сбор и первичную обработку сообщений информационной безопасности, поступающих от различных источников. Агенты выполняют нормализацию, фильтрацию, агрегацию, первичную категоризацию сообщений и передачу обработанных сообщений в модуль управления ArcSight Manager.

Агенты могут устанавливаться на выделенный сервер агентов и собирать события ИБ удаленно, или непосредственно на контролируемые системы.

При установке нового агента, он регистрируется в модуле управления и всё дальнейшее взаимодействие с модулем управления осуществляется по зашифрованному каналу. Агент передает принятые и обработанные сообщения ИБ модулю управления пакетами по 100 событий или каждую секунду, что наступает раньше.

Для получения событий ИБ с нестандартных или не поддерживаемых ArcSight ESM систем используются программируемые агенты ArcSight FlexConnectors.

Модуль управления (ArcSight Manager) сохраняет обработанную информацию в базе данных (ArcSight DataBase) и обрабатывает события ИБ с помощью механизма корреляции, который оценивает события с учётом сетевой модели и информации о уязвимостях, оценивая тем самым угрозы в реальном времени. Для этого модуль управления содержит большое количество предварительных настроек фильтров, правил, отчётов, мониторов данных, инструментальных консолей, сетевых моделей, которые используются сразу после установки ArcSight ESM. В тоже время все предопределённые настройки могут изменяться и настраиваться под определённые нужды.

База данных (ArcSight DataBase), кроме обработанных сообщений информационной безопасности, хранит информацию о конфигурации системы мониторинга, пользователях системы мониторинга, группах, правах, правилах и отчётах. Сервер базы данных функционирует на базе Oracle 10. БД Oracle устанавливается и настраивается автоматически при установке ArcSight ESM.

SmartStorage Partition Management — модуль управления разделами (партициями) базы данными. БД разделяется на разделы оперативного хранения, разделы среднесрочного хранения, долговременного хранения, и разделы offline хранения.

Консоль управления (ArcSight Console) выполняется на АРМ администратора ArcSight ESM и предназначена для:

- визуального контроля событий информационной безопасности;
- создания и настройки фильтров и правил обработки сообщений;
- описание правил оповещения;
- генерации отчётов;
- административных действий по созданию пользователей ArcSight ESM и прав.

Интерфейс и набор инструментальных средств консоли управления зависит от роли использующего его пользователя.

Интерфейс ArcSight Web представляет из себя web-сервер, который обеспечивает безопасный интерфейс к модулю управления ArcSight Manager с помощью web проводника. ArcSight Web предназначен для пользователей, которым нужно иметь доступ к ArcSight ESM извне защищенной сети организации.

В системе ArcSight применяется ролевая модель доступа. Роли позволяют описывать различные уровни доступа пользователей к системе и их зоны ответственности, предоставляя различные инструментальные средства.

В ArcSight используются следующие роли:

1 Администратор — осуществляет установку и общую работоспособность системы;

2 Автор — моделирует сеть, разрабатывает системные ресурсы, а также шаблоны отчётов и статьи базы данных;

3 Оператор — отвечает за мониторинг событий и первичное расследование инцидентов;

4 Аналитик — отвечает за детальное расследование и исправление инцидентов по запросам от операторов;

5 Менеджер безопасности — отвечает за управление и работы в Центре безопасности;

6 Бизнес-пользователь — использует ArcSight, чтобы устанавливать и передавать системные условия.

3.2. Вывод

В рамках третьей главы были описаны используемые при разработке языки программирования и инструменты, существующие компоненты программного модуля, возможности пользователей и интерфейс. Обозначены планы на будущее в рамках реализации данного программного средства. Выполнено функциональное тестирование, показавшее что все функции реализованы и работают корректно.

4. ТЕХНИКО-ЭКОНОМИЧЕСКОЕ ОБОСНОВАНИЕ РАЗРАБОТКИ И ВНЕДРЕНИЯ В ЭКСПЛУАТАЦИЮ СИСТЕМЫ УПРАВЛЕНИЯ И МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОМПАНИИ

4.1. Характеристика разработанной системы управления и мониторинга информационной безопасности

Система управления и мониторинга информационной безопасности компании является самостоятельной разработкой и будет использоваться для собственных нужд.

В рамках разрабатываемой системы были поставлены задачи автоматизации и/или упрощения процесса управления и мониторинга информационной безопасности компании. Благодаря системе управления и мониторинга информационной безопасности компании планируется уменьшить затраты на заработную плату специалистов по информационной безопасности компании, а так же улучшить качество обнаружения и предотвращения инцидентов информационной безопасности.

4.2. Расчет инвестиций на разработку и внедрение в эксплуатацию системы управления и мониторинга информационной безопасности

Расчет затрат на разработку системы управления и мониторинга информационной безопасности в данном случае будет состоять из следующих пунктов:

- затраты на комплектующие изделия;
- затраты на основную заработную плату разработчиков;
- затраты на дополнительную заработную плату разработчиков;
- затраты на материалы для монтажа системы;
- затраты на монтаж технической составляющей системы;
- отчисления на социальные нужды;
- прочие затраты (амortизационные отчисления, расходы на электроэнергию, командировочные расходы, арендная плата за офисные помещения и оборудование, расходы на управление и реализацию и т.п.);
- плановая прибыль, включаемая в цену системы управления и мониторинга информационной безопасности.

1 Затраты на комплектующие изделия. Включаются затраты на приобретение в порядке производственной кооперации готовых покупных изделий и полуфабрикатов, используемых для комплектования изделий.

Расчет затрат на комплектующие изделия представлен в таблице 4.1.

Таблица 4.1 – Расчет затрат на комплектующие изделия

Наименование комплектующего изделия или полуфабриката	Количество на единицу, шт.	Цена за единицу, руб.	Сумма, руб.
1. Сервер HP ProLiant DL165R07	1	3937,5	3937,5
2. Оперативная память 2GB	2	141,4	282,8
3. Жесткий диск HP 160GB	2	92,2	184,4
4. Сервер HP ProLiant DL180	1	2812,0	2812,0
5. Процессор ProLiant DL160	1	1100	1100
6. Оперативная память 2GB	8	106,1	848,8
7. Корзина HP DL180G6	1	115,3	115,3
8. Жесткий диск HP 1TB	14	700	9800
9. Блок питания HP 750W	1	325	325
Всего			19405,8
Всего с учётом транспортно-заготовительных расходов			21346,4

2 Затраты на основную заработную плату команды разработчиков. Основная заработная плата исполнителей проекта определяется по формуле:

$$Z_o = K_{\text{пр}} \cdot \sum_{i=1}^n Z_{qi} \cdot t_i,$$

где n – количество исполнителей, занятых разработкой конкретного системы управления и мониторинга информационной безопасности;

$K_{\text{пр}}$ – коэффициент премий (1,5);

Z_{qi} – часовая заработка i -го исполнителя (руб.);

t_i – трудоемкость работ, выполняемых i -м исполнителем (ч).

Расчет основной заработной платы представлен в таблице 4.2.

3 Затраты на дополнительную заработную плату команды разработчиков включает выплаты, предусмотренные законодательством о труде (оплата трудовых отпусков, льготных часов, времени выполнения государственных обязанностей и других выплат, не связанных с основной деятельностью исполнителей), и определяется по формуле:

$$Z_d = \frac{Z_o \cdot H_d}{100},$$

где H_d – норматив дополнительной заработной платы(20 %);

Z_o – затраты на основную заработную плату (руб.).

Таблица 4.2 – Расчет основной заработной платы

№	Наименование должности разработчика	Вид выполнляемой работы	Месячная заработка плата, руб.	Часовая заработка плата, руб.	Трудоемкость работ, ч.	Зарплата по тарифу, руб.
1	2	3	4	5	6	7
1	Руководитель проекта	анализ системы	1300,00	8,125	100	812,5
2	Специалист по информационной безопасности	разработка системы	1100	6,875	200	1375
3	Системный архитектор	разработка архитектуры взаимодействия компонентов системы	900	5,625	70	393,75
4	Специалист по тестированию программного обеспечения	тестирование полномасштабной системы	800	5	40	200
Итого						2781,25
Премия(50%)						1390,625
Итого затраты на основную заработную плату разработчиков						4171,875

Дополнительная заработная плата составит:

$$Z_d = \frac{4171,875 \cdot 20}{100} = 834,375 \text{ руб.}$$

4 Расчет затрат на материалы для монтажа системы осуществляются в табличной форме и представлены в таблице 4.3

5 Затраты на монтаж технической составляющей системы. Расчет заработной платы на монтаж системы осуществляется в табличной форме и представлен в таблице 4.4.

Таблица 4.3 – Расчет затрат на материалы для монтажа

Наименование материала	Единица измерения	Норма расхода	Цена за единицу	Сумма, руб.
1. Кабель сетевой UTP-CAT5E	м	30	3	90
2. Короб декоративный белый	м	10	2,5	25
3. Коннекторы RJ-45	шт	55	1,5	82,5
4. Шкаф серверный напольный 42U ЦМО ШТК-С-2	шт	1	1900	1900
5. Розетка электрическая белая	шт	5	3	15
6. Розетка компьютерная белая внешняя	шт	2	8	16
7.1. Кабель КМВЭВ1х2х0,75	м	10	3,2	32
Всего				2160,5
Всего с учетом транспортных расходов				2592,6

Таблица 4.4 – Расчет заработной платы на монтаж системы

Наименование категории работника и должности	Численность исполнителей, чел.	Месячная заработка, руб.	Дневная заработка, руб.	Трудоемкость работ, дн.	Сумма, руб.
1. Главный инженер	1	1000	47,6	2	95,2
2. Электромонтер	1	800	38	3	114,2
Итого					204,5
Премия(40%)					83,8
Всего основная заработка					288,3

Дополнительная заработка платы составит:

$$Z_d = \frac{288,3 \cdot 20}{100} = 57,7 \text{ руб.}$$

6 Отчисления в фонд социальной защиты и обязательного страхования (в фонд социальной защиты населения и на обязательное страхование) определяются в соответствии с действующими законодательными актами определяются по формуле:

$$P_{coz} = \frac{(Z_o + Z_d) \cdot H_{coz}}{100},$$

где H_{coz} – норматив отчислений в фонд социальной защиты населения и на обязательное страхование (34,6 %).

$$P_{coz} = \frac{(4171,875 + 834,375 + 288,3 + 57,7) \cdot 34,6}{100} = 1851,88 \text{ руб.}$$

7 Прочие затраты включаются в себестоимость разработки системы управления и мониторинга информационной безопасности в процентах от затрат на основную заработную плату команды разработчиков определяются по формуле:

$$P_{pr} = \frac{Z_o \cdot H_{pr}}{100},$$

где H_{pr} – норматив прочих затрат (70 %).

$$P_{pr} = \frac{4460,2 \cdot 70}{100} = 3122,12 \text{ руб.}$$

8 Общая сумма затрат на разработку системы управления и мониторинга информационной безопасности находится путем суммирования всех рассчитанных статей затрат, и определяется по формуле:

$$Z_p = Z_k + Z_o + Z_d + P_{coz} + P_{pr},$$

$$Z_p = 21346,4 + 4171,875 + 346 + 834,375 + 1732,1625 + 2920,312 = 31351,12 \text{ руб.}$$

9 Отпускная цена системы управления и мониторинга информационной безопасности определяется по формуле:

$$\Pi_{pc} = Z_p,$$

$$\Pi_{pc} = 31351,12 \text{ руб.}$$

Формирование цены системы управления и мониторинга информационной безопасности на основе затрат представлено в таблице 4.5.

Таблица 4.5 – Формирование цены на основе затрат на разработку системы управления и мониторинга информационной безопасности

Статья затрат	Сумма, руб.
Затраты на комплектующие изделия	21346,4
Основная заработка плата команды разработчиков	4171,875
Дополнительная заработка плата команды разработчиков	834,375
Затраты на материал для монтажа	2592,6
Основная заработка плата на монтаж системы	288,3
Дополнительная заработка плата на монтаж системы	57,7
Отчисления в фонд социальной защиты и обязательного страхования	1851,88
Прочие затраты	3122,12
Итого	34265,25

4.3. Расчет экономического эффекта от использования системы управления и мониторинга информационной безопасности

Использование системы управления и мониторинга информационной безопасности в первую очередь централизует и нормализует поступление информации со всевозможных источников-объектов системы безопасности, тем самым облегчая и улучшая работу отдела информационной безопасности. Быстрый анализ инцидентов и реагирование на них понижает вероятность утечек данных, проникновений злоумышленников во внутреннюю сеть организации и повышает производительность отдела безопасности путем снижения трудоемкости ряда процессов. Использование системы скажется на высвобождении рабочего времени персонала, который, впоследствии, станет обслуживать систему. Экономический эффект при использовании системы будет рассчитываться следующим образом.

Экономия затрат на заработную плату при использовании системы управления и мониторинга информационной безопасности для организаций-заказчика определяется по формуле:

$$\mathcal{E}_{зп} = K_{пр} \cdot (t_p^{\text{без пс}} - t_p^{\text{с пс}}) \cdot T_ч \cdot N_{пп} \cdot \left(1 + \frac{H_{д}}{100}\right) \cdot \left(1 + \frac{H_{но}}{100}\right),$$

где $N_{пп}$ – плановый объем работ;

$t_p^{\text{без пс}}, t_p^{\text{с пс}}$ – трудоемкость выполнения работы до и после внедрения системы управления и мониторинга информационной безопасности (ч.);

$T_ч$ – часовая тарифная ставка, соответствующая разряду выполняемых работ (3,75 руб./ч.);

$K_{\text{пр}}$ – коэффициент премий (1,5);
 H_d – норматив дополнительной заработной платы (20%);
 $H_{\text{но}}$ – ставка отчислений от заработной платы, включаемых в себестоимость (34,6%).

$$\mathcal{E}_3 = 1,5 \cdot (7 - 4) \cdot 3,75 \cdot 750 \cdot \left(1 + \frac{20}{100}\right) \cdot \left(1 + \frac{34,6}{100}\right) = 20442,375 \text{ руб.}$$

Экономический эффект при использовании системы управления и мониторинга информационной безопасности будет рассчитываться по формуле:

$$\Delta\Pi_{\text{ч}} = (\mathcal{E}_3 - \Delta Z_{\text{тек}}) \cdot (1 - H_{\Pi}),$$

где \mathcal{E}_3 – экономия текущих затрат, полученная в результате применения системы управления и мониторинга информационной безопасности (руб.);

$\Delta Z_{\text{тек}}$ – прирост текущих затрат, связанных с использованием системы управления и мониторинга информационной безопасности (15% отпускной стоимости системы);

H_{Π} – ставка налога на прибыль, в соответствии с действующим законодательством (18%).

$$\Delta\Pi_{\text{ч}} = (20442,375 - 6511,08) \cdot (1 - 0,18) = 11423,67 \text{ руб.}$$

4.4. Расчёт показателей экономической эффективности разработки и использования системы управления и мониторинга информационной безопасности

Так как сумма инвестиций больше суммы годового экономического эффекта, то экономическая целесообразность инвестиций в разработку и использование программного продукта осуществляется на основе расчёта и оценки следующих показателей:

- чистый дисконтированный доход (ЧДД);
- срок окупаемости инвестиций ($T_{\text{ок}}$);
- рентабельность инвестиций ($T_{\text{и}}$).

Так как приходится сравнивать разновременные результаты (экономический эффект) и затраты (инвестиции в разработку программного продукта), необходимо привести их к единому моменту времени – началу расчётного периода, что обеспечивает их сопоставимость. Для этого необходимо использовать дисконтирование путём умножения соответствующих результатов и затрат на коэффициент дисконтирования соответствующего года t , который определяется по формуле

$$\alpha_t = \frac{1}{(1 + E_h)^t}$$

где E_h — норма дисконта (в долях единиц), равная или больше средней процентной ставки по банковским депозитам, действующей на момент осуществления расчётов, 0,12;

t — порядковый номер года периода реализации инвестиционного проекта (предполагаемый период использования разрабатываемого ПО пользователем и время на разработку).

$$\alpha_t = \frac{1}{(1 + 0,12)} = 0,8928$$

Чистый дисконтированный доход рассчитывается по формуле

$$ЧДД = \sum_{t=1}^n (P_t - Z_t) \cdot \alpha_t$$

где n — расчётный период, лет;

P_t — результат (экономический эффект — прибыль или чистая прибыль), полученный в году t , р.;

Z_t — затраты (инвестиции — затраты на разработку (модернизацию) или на приобретение и внедрение ПО) в году t , р.

Расчёт показателей эффективности инвестиций представлен в таблице 4.6

Таблица 4.6 – Расчёт чистого дисконтированного дохода и срока окупаемости инвестиций в разработку и внедрения программно-аппаратного комплекса, р.

Наименование показателя	Усл. обоз.	Расчетный период, год			
Результат		1-ый	2-ой	3-ий	4-ый
1. Прирост результата(чистой прибыли)	P _t	11423,67	11423,67	11423,67	11423,67
2.Коэффициент дисконтирования	α _t	1	0,8928	0,7971	0,7118
3.Результат с учетом фактора времени	P _t α _t	11423,67	10199,05	9104,66	8131,37
Затраты (инвестиции)					
4.Инвестиции в разработку ПО	3	31351,12	-	-	-
5.Инвестиции с учетом фактора времени	3 _t α _t	31351,12	-	-	-
6.Чистый дисконтированный доход по годам	ЧДД _t	-19927,45	10199,05	9104,66	8131,37
7.ЧДД нарастающим итогом	ЧДД	-19927,45	-9728,4	-623,74	+7507,63

Рентабельность инвестиций определяется по формуле

$$P_i = \frac{\Pi_{ср}}{3} \cdot 100\%$$

где $\Pi_{ср}$ – среднегодовая величина чистой прибыли за расчётный период, р., которая определяется по формуле

$$\Pi_{ср} = \frac{\sum_{t=1}^n \Pi_{ct}}{n}$$

$$\Pi_{ср} = \frac{45694,68}{4} = 11423,67 \text{ руб.}$$

где Π_{ct} – чистая прибыль, полученная в году t , р.

$$P_i = \frac{11423,67}{43891,6} \cdot 100\% = 26\%$$

4.5. Вывод

В результате технико-экономического обоснования разработки и внедрения в эксплуатацию системы управления и мониторинга информационной безопасности были получены следующие значения показателей эффективности:

1 прирост среднегодовой чистой прибыли организации-заказчика составит 11423,67 руб.;

2 затраты на разработку системы управления и мониторинга информационной безопасности для организации-заказчика окупятся на четвертый год его использования без учета фактора времени и на пятый с учетом фактора времени;

3 инвестиции на разработку системы управления и мониторинга информационной безопасности будут экономически эффективными, т.к. рентабельность инвестиций составляет 26 %.

Таким образом, разработка и применение системы управления и мониторинга информационной безопасности является эффективной и данные инвестиции осуществлять целесообразно.

ЗАКЛЮЧЕНИЕ

В ходе дипломного проектирования разработана система управления и мониторинга информационной безопасности компании. Данная система предназначается для собственного использования.

Проанализированы подходы и средства для разработки системы управления и мониторинга информационной безопасности компании. Также, были рассмотрены аналоги данной системы, представленные на рынке. Информация, полученная в ходе анализа, помогла конкретизировать цели и задачи, поставленные при дипломном проектировании.

Спроектирована архитектура системы управления и мониторинга информационной безопасности компании. Данная архитектура легла в основу разрабатываемой системы.

Проведено тестирование разработанной системы. Результаты тестирования показали, что отдельные блоки и вся система в целом работает корректно и без сбоев.

Реализована система управления и мониторинга информационной безопасности компании. Реализация осуществлялась с использованием подходов и средств, рассмотренных на этапе анализа.

Выполнено технико-экономическое обоснование разработки и внедрения в эксплуатацию системы управления и мониторинга информационной безопасности компании. По данным, полученным в ходе технико-экономического обоснования, система рентабельна и окупается на пятый год эксплуатации.

Разработанная система используется для круглосуточного мониторинга информационной безопасности компании. Также, данная система используется для управления инфраструктурой информационной безопасности компании.

Система управления и мониторинга информационной безопасности компании гибкая. Имеет большой потенциал к модернизации путём внедрения новых или более совершенных модулей.

Цель дипломного проекта достигнута, поставленные задачи решены в полном объёме.

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

- [1] Денисенко, В. В. Компьютерное управление технологическим процессом, экспериментом, оборудованием / В. В. Денисенко. — М.: Горячая линия–Телеком, 2014. — 608 с.
- [2] Антимиров, В. М. Проектирование аппаратуры систем автоматического управления : учебное пособие : в 2 ч. Ч. 1 : Создание САУ / В. М. Антимиров. — Екатеринбург : Изд-во Урал. ун-та, 2015. — 92 с.
- [3] Проектирование АСУ ТП [Электронный ресурс]. — Режим доступа: http://arman-engineering.ru/info_center/articles/888. — Дата доступа: 30.03.2018.
- [4] Горовой, В. Г. Экономическое обоснование проекта по разработке программного обеспечения / В. Г. Горовой, А. В. Грицай, В. А. Пархименко. — Минск : БГУИР, 2018. — 12 с.
- [5] Доманов, А. Т. СТП 01-2017. Стандарт предприятия. Дипломные проекты (работы). Общие требования / А. Т. Доманов, Н. И. Сорока. — Минск : БГУИР, 2017. — 169 с.
- [6] SIEM система Micro Focus ArcSight [Электронный ресурс]. — Режим доступа: <https://www.anti-malware.ru/reviews/Micro-Focus-ArcSight>. — Дата доступа: 14.04.2019.
- [7] SIEM система Kaspersky [Электронный ресурс]. — Режим доступа: <https://www.anti-malware.ru/reviews/Kaspersky-Unified-Monitoring-and-Analysis-Platform>. — Дата доступа: 26.03.2017.
- [8] Родичев, Ю. А. Нормативная база и стандарты в области информационной безопасности. / Ю. А. Родичев. — 2017. — 256 с.
- [9] Е. К. Баранова, А. В. Бабаш. Информационная безопасность и защита. / А. В. Бабаш Е. К. Баранова. — 2017. — 324 с.
- [10] Microsoft Active Directory [Electronic resource]. — Mode of access: <https://www.lepide.com/blog/what-is-active-directory-and-how-does-it-work/>. — Date of access: 17.05.2018.
- [11] Cisco MARS Wikipedia [Electronic resource]. — Mode of access: https://en.wikipedia.org/wiki/Cisco_Security_Monitoring,_Analysis,_and_Response_System. — Date of access: 08.08.2019.

[12] Cisco MARS [Electronic resource]. — Mode of access: <https://manualzz.com/doc/30336013/user-guide-for-cisco-security-mars-local-and-global-contr>. — Date of access: 12.11.2017.

[13] Talamantes, J. The Social Engineer's Playbook: A Practical Guide to Pre-texting / J. Talamantes. — Kindle edition. — 2014. — 148 P.

[14] Системы информационной безопасности [Электронный ресурс]. — Режим доступа: <https://habr.com/ru/company/roi4cio/blog/528770/>. — Дата доступа: 30.04.2018.

[15] Information security audit article [Electronic resource]. — Mode of access: https://en.wikipedia.org/wiki/Information_security_audit. — Date of access: 25.11.2017.

[16] Нестеров, С. А. Основы информационной безопасности. / С. А. Нестеров. — 2016. — 324 с.

[17] Бирюков, А. А. Информационная безопасность. Защита и нападение / А. А. Бирюков. — 2-е изд. — 2017. — 245 с.

[18] Бондарев, В. Введение в информационную безопасность автоматизированных систем. / В. Бондарев. — 2016. — 310 с.

[19] Система информационной безопасности MaxPatrol SIEM [Электронный ресурс]. — Режим доступа: https://www.anti-malware.ru/reviews/MaxPatrol_SIEM. — Дата доступа: 25.10.2016.

[20] Pdl [Electronic resource]. — Mode of access: <http://www.agat.by/products/defence-products/technology/pdl/>. — Date of access: 25.03.2018.

[21] Introduction to DCE [Electronic resource]. — Mode of access: http://www-01.ibm.com/software/network/dce/library/publications/dceaix_22/a3u2s/A3U2SM21.htm. — Date of access: 25.03.2018.

[22] Peterson, M. T. Dce: A Guide to Developing Portable Applications / M. T. Peterson. — 1st edition. — Computing McGraw-Hill, 1995. — 608 P.

[23] Hu, W. Guide to Writing DCE Applications / W. Hu, D. Magid, J. Shirley. Osf Distributed Computing Environment. — 2st edition. — O'Reilly Media, 1992. — 459 P.

[24] 10 Introduction to OMG IDL [Electronic resource]. — Mode of access: <https://mhanckow.students.wmi.amu.edu.pl/corba/IDL.html>. — Date of access: 17.05.2018.

[25] Microsoft Interface Definition Language [Electronic resource]. — Mode of access: <https://msdn.microsoft.com/en-us/library/windows/desktop/aa367091>. — Date of access: 17.05.2018.

[26] MIDL (Microsoft Interface Definition Language) [Electronic resource]. — Mode of access: [https://ru.bmstu.wiki/MIDL_\(Microsoft_Interface_Definition_Language\)](https://ru.bmstu.wiki/MIDL_(Microsoft_Interface_Definition_Language)). — Date of access: 17.05.2018.

<i>Обозначение</i>	<i>Наименование</i>	<i>Дополнительные сведения</i>						
<u>Текстовые документы</u>								
БГУИР ДП 1-40 03 01 02 059 ПЗ	Пояснительная записка	69 с.						
	Отзыв руководителя							
	Рецензия							
	<u>Графические документы</u>							
ГУИР.87059-01 90 01-1	Жизненный цикл события информационной безопасности	Формат А1						
ГУИР.87059-01 91 01-1	Источники сообщений об инцидентах информационной безопасности	Формат А1						
ГУИР.87059-01 92 01-1	Структура системы управления и мониторинга информационной безопасности компании	Формат А1						
ГУИР.87059-01 93 01-1	Блок-схема алгоритма обработки инцидентов информационной безопасности	Формат А1						
ГУИР.87059-01 94 01-1	Схема базы данных	Формат А1						
ГУИР.87059-01 95 01-1	Пользовательский интерфейс системы	Формат А1						
	<u>Текст программы</u>	CD-диск						
	<i>БГУИР ДП 1- 40 03 01 02 059 Д1</i>							
<i>Изм.</i>	<i>Л.</i>	<i>№ докум.</i>	<i>Подп.</i>	<i>Дата</i>	<i>Система управления и мониторинга информационной безопасности компании Ведомость дипломного проекта</i>	<i>Лит</i>	<i>Лист</i>	<i>Листов</i>
<i>Разраб.</i>		<i>Митрофанов</i>				T	69	69
<i>Пров.</i>		<i>Лихачёв</i>						
<i>Т.контр.</i>		<i>Соболь</i>						
<i>Н.контр.</i>		<i>Захаров</i>						
<i>Утв.</i>		<i>Шункевич</i>						