

Федеральное агентство связи  
федеральное государственное бюджетное образовательное учреждение  
высшего образования  
«Сибирский государственный университет телекоммуникаций  
и информатики»  
(СибГУТИ)

Кафедра \_\_\_\_\_ БиУТ \_\_\_\_\_

Допустить к защите зав. кафедрой

\_\_\_\_\_ /С.Н. Новиков /

**ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА  
СПЕЦИАЛИСТА**

Исследование и организация процесса мониторинга событий информационной  
безопасности

Пояснительная записка

Студент \_\_\_\_\_ / Н.А. Анжин \_\_\_\_\_ /

Факультет \_\_\_\_\_ АЭС \_\_\_\_\_ Группа \_\_\_\_\_ АБ-56 \_\_\_\_\_

Руководитель \_\_\_\_\_ / Г.В. Попков \_\_\_\_\_ /

Рецензент \_\_\_\_\_ / \_\_\_\_\_ /

Консультанты:

– по экономическому обоснованию

\_\_\_\_\_ / И.С. Мухина \_\_\_\_\_ /

– по безопасности жизнедеятельности

\_\_\_\_\_ / Н.Н. Симакова \_\_\_\_\_ /

Рецензент: \_\_\_\_\_ / \_\_\_\_\_ /

Новосибирск 2021

Инд. № подл.	Подп. и дата	Взам. инв. №	Инд. № дубл.	Под. и дата

Федеральное агентство связи  
федеральное государственное бюджетное образовательное учреждение  
высшего образования  
«Сибирский государственный университет телекоммуникаций и информатики»  
(СибГУТИ)

**КАФЕДРА**

## Безопасность и управление в телекоммуникациях

## ЗАДАНИЕ

## НА ВЫПУСКНУЮ КВАЛИФИКАЦИОННУЮ РАБОТУ СПЕЦИАЛИСТА

СТУДЕНТА Н.А. Анжина ГРУППЫ АБ-56

«УТВЕРЖДАЮ»

« 28 » июля 2020 г.

Зав. кафедрой БиУТ

\_\_\_\_\_ / С.Н. НОВИКОВ /

Новосибирск 2020

1. Тема выпускной квалификационной работы специалиста: \_\_\_\_\_

Исследование и организация процесса мониторинга событий информационной безопасности

утверждена приказом по университету от «28» июля 2020 г. № 4/1011о-20

2. Срок сдачи студентом законченной работы «  » 2021 г.

3. Исходные данные по проекту (эксплуатационно-технические данные, техническое задание):

Международный и национальный стандарты ISO/IEC 27001:2013 и ГОСТ Р ИСО/МЭК 27001-2006

Национальный стандарт ГОСТ Р ИСО/МЭК 18044-2007;

CMU/SEI-2004-TR-015.

4. Содержание расчетно-пояснительной записки (перечень подлежащих разработке вопросов)	Сроки выполнения по разделам
Введение	05.02.2021 г.
1. Организационная часть мониторинга инцидентов ИБ	08.02.2021 г.
2. Программно-техническая часть мониторинга инцидентов ИБ	15.03.2021 г.
3. Внедрение системы мониторинга ИБ компании	09.04.2021 г.
4. Безопасность жизнедеятельности	03.05.2021 г.
5. Технико-экономическое обоснование работы	07.05.2021 г.
6. Заключение	18.05.2021 г.
7. Список литературы	29.05.2021 г.
8. Приложения	31.05.2021 г.

Консультанты по ВКР (с указанием относящихся к ним разделов):

1. Раздел по технико-экономическому обоснованию

---

---

---

---

2. Раздел по безопасности жизнедеятельности

---

---

---

---

Дата выдачи задания

« 01 » сентября 2020 г.

\_\_\_\_\_/ Г.В. Попков /

(подпись, Ф.И.О. руководителя)

Задание принял к исполнению

« 01 » сентября 2020 г.

\_\_\_\_\_/ Н.А. Анжин /

(подпись, Ф.И.О. студента)



Федеральное агентство связи  
федеральное государственное бюджетное образовательное учреждение  
высшего образования  
«Сибирский государственный университет телекоммуникаций и информатики»  
(СибГУТИ)

**ОТЗЫВ**

о работе студента Н.А. Анжина в период подготовки выпускной квалификационной работы по теме «Исследование и организация процесса мониторинга событий информационной безопасности»

---

---

---

---

---

---

---

---

---

---

Работа имеет практическую ценность  
Работа внедрена  
Рекомендую работу к внедрению  
Рекомендую работу к опубликованию  
Работа выполнена с применением ЭВМ

<input type="checkbox"/>
<input type="checkbox"/>
<input type="checkbox"/>
<input type="checkbox"/>
<input type="checkbox"/>

Тема предложена предприятием  
Тема предложена студентом  
Тема является фундаментальной  
Рекомендую студента в магистратуру  
Рекомендую студента в аспирантуру

<input type="checkbox"/>
<input type="checkbox"/>
<input type="checkbox"/>
<input type="checkbox"/>
<input type="checkbox"/>

Руководитель выпускной квалификационной работы специалиста

Доц. каф. БиУТ, к.т.н.

Попков Глеб Владимирович

«\_» июня 2021 г.

С Отзывом ознакомлен

/Н.А. Анжин/

«\_» июня 2021 г.

## Уровень сформированности компетенций у студента

Н.А. Анжина

Компетенции		Уровень сформированности компетенций		
		высокий	средний	низкий
1		2	3	4
Профессиональные	ПК-1 - способностью осуществлять анализ научно-технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности телекоммуникационных систем			
	ПК-5 - способностью проектировать защищенные телекоммуникационные системы и их элементы, проводить анализ проектных решений по обеспечению заданного уровня безопасности и требуемого качества обслуживания, разрабатывать необходимую техническую документацию с учетом действующих нормативных и методических документов			
	ПК-7 - способностью осуществлять рациональный выбор средств обеспечения информационной безопасности телекоммуникационных систем с учетом предъявляемых к ним требований качества обслуживания и качества функционирования			
	ПК-12 - способностью выполнять технико-экономические обоснования, оценивать затраты и результаты деятельности организации в области обеспечения информационной безопасности			

## АННОТАЦИЯ

Выпускной квалификационной работа студента Н.А. Анжин  
по теме Исследование и организация процесса мониторинга событий  
информационной безопасности

Объём работы – 86 страниц, на которых размещены 4 рисунков и 4 таблиц. При написании работы использовалось источников.

Ключевые слова: \_\_\_\_\_

Работа выполнена на: кафедре БиУТ СибГУТИ

Руководитель: доц. каф. БиУТ Попков Г.В.

Целью работы Исследование и организация процесса мониторинга событий  
информационной безопасности

Решаемые задачи: анализ существующего состояния объекта проектирования,  
разработка системы защиты информации, выбор оборудования и программного  
обеспечения, безопасность жизнедеятельности, технико-экономическое  
обоснование работы

Основные результаты: \_\_\_\_\_



## Graduation thesis abstract

The paper consists of \_ pages, with figures and tables/charts/diagrams. While writing the thesis reference sources were used.

Keywords: information protection system, access control system, video surveillance system, antivirus protection, security policy, authentication

The thesis was written at BIUT department SibSUTIS  
(name of organization or department)

Scientific supervisor associate professor of the BiUT Solonskaya Oxana

The goal/subject of the paper is modernize the information security system in the enterprise

Tasks: analysis of the existing state of the design object, development of an information protection system, selection of equipment and software, life safety, technical and economic justification of work

Results modernized information security system in the enterprise

# ОГЛАВЛЕНИЕ

Введение .....	4
1 Исследование и применение мониторинга инцидентов ИБ .....	5
1.1 Постановка задачи .....	5
1.2 Исследование информационно-технологической инфраструктуры телекоммуникационной компании Х.....	5
1.3 Основные подходы в организации мониторинга ИБ.....	10
1.3 Анализ регламентирующих документов .....	14
1.4 Исследование центра обеспечения безопасности.....	16
1.5 Вывод .....	27
2 Исследование и анализ программно-аппаратных систем мониторинга инцидентов ИБ .....	28
2.1 Постановка задачи .....	28
2.2 Исследование и применение SIEM-систем .....	28
2.3 Анализ основных принципов работы и характеристик SIEM-системы ..	30
2.4 Анализ используемых средств защиты информации.....	33
2.5 Вывод .....	44
3 Внедрение системы мониторинга ИБ компании .....	45
3.1 Постановка задачи .....	45
3.2 Анализ и выбор SIEM-системы .....	45
3.3 Развертывание SIEM-системы в телекоммуникационной компании....	54
Заключение .....	63
4 Безопасность жизнедеятельности.....	64
4.1 Постановка задачи .....	64
4.2 Характеристика трудовой деятельности специалиста ИБ .....	64

Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Инв. № подл.	Взам. инв. №	Инв. № дубл.						



Введение

В настоящее время для обеспечения информационной безопасности предприятия важное значение имеют технологии проактивной защиты информации, нацеленные на упреждение нарушений информационной безопасности и осуществляющие мониторинг, менеджмент информационной безопасности.

Технологии проактивной защиты основываются на своевременном, оперативном сборе данных и метаданных о событиях безопасности, которые фиксируются в записях журналов аудита компьютерной инфраструктуры, хранении данных в специализированном хранилище и последующей обработке, включающей процедуры классификации, корреляции, моделирования, выработки предупреждений и решений по противодействию атакам, а также другие наиболее эффективные оперативные процедуры восстановления и надежное сохранение безопасности информации. Другими словами, осуществляется управление инцидентами и, в частности, мониторинг инцидентов информационной безопасности.

Цель данной выпускной квалификационной работы является разработка системы проведения мониторинга инцидентов информационной безопасности для телекоммуникационной компании. Для этого необходимо решить следующие задачи:

- рассмотреть основные подходы в организации мониторинга инцидентов ИБ ;
- провести анализ программно-технической части мониторинга инцидентов ИБ;
- выполнить внедрение системы мониторинга ИБ для телекоммуникационной компании;
- анализ безопасности жизнедеятельности;
- технико-экономическое обоснование проекта.

Подпись и дата	
Инв. № дубл.	
Взам. инв. №	
Подпись и дата	
Инв. № подл.	

# 1 Исследование способов и применения мониторинга инцидентов ИБ

## 1.1 Постановка задачи

Задача первой главы заключается в исследовании основных подходов в организации мониторинга инцидентов информационной безопасности, также необходимо провести анализ регламентирующих документов и рассмотреть необходимость в составе компании центра управления инцидентами.

## 1.2 Исследование информационно-технологической инфраструктуры компании

Рассматриваемая в данной работе компания является оператором связи и предоставляет услуги мобильной связи и мобильного интернета на региональном уровне.

Структура телекоммуникационной компании включает в себя следующие объекты:

- Центр обработки данных (ЦОД);
- Главный офис компании;
- Филиалы.

Общая структурная схема сети исследуемой компании представлена на рисунке 1.1

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата						
Изм.	Лист	№ докум.	Подпись	Дата	ФАЭС.10.05.02.056					Лист
										5

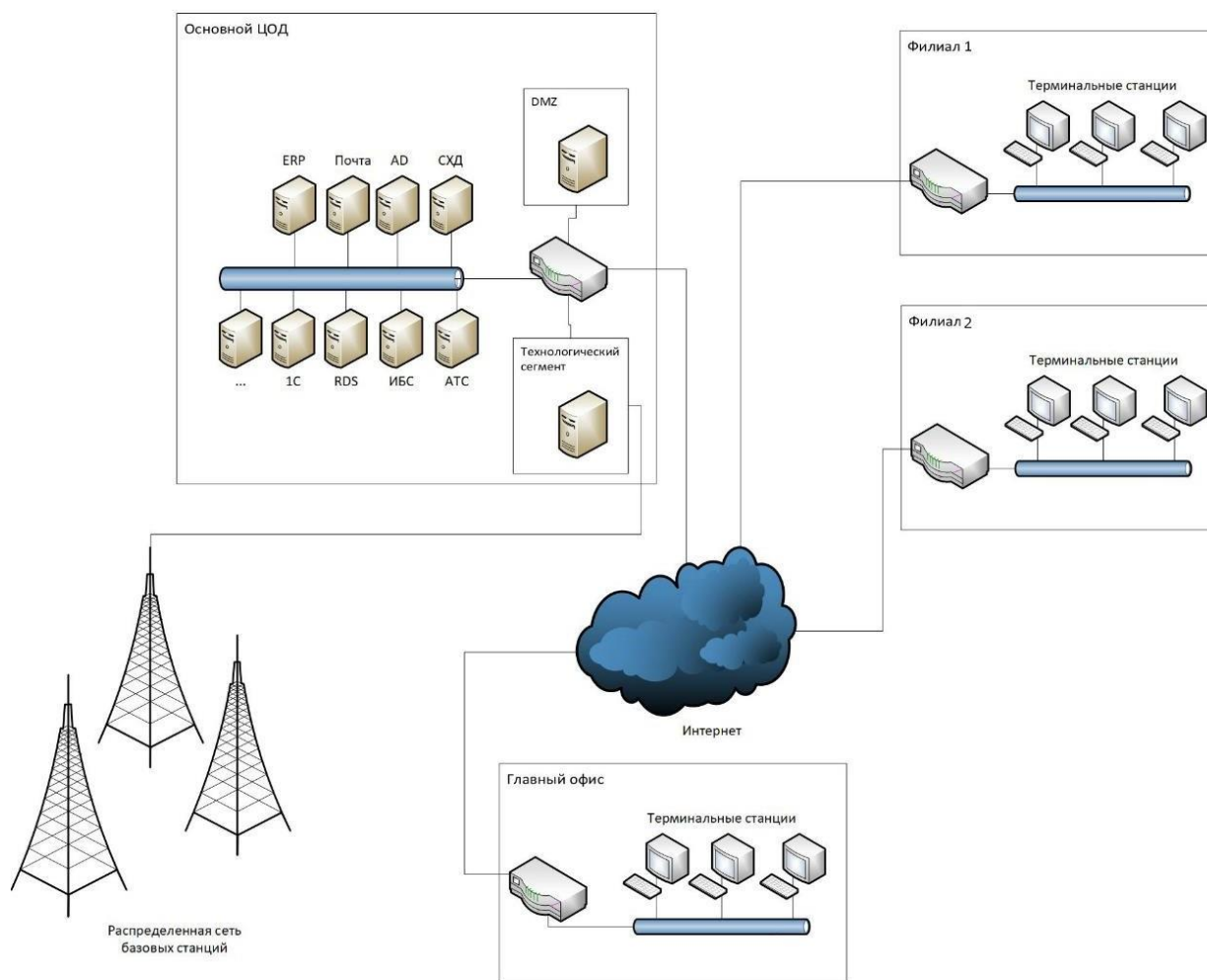


Рисунок 1.1 - Структурная схема сети.

Рассмотрим подробнее инфраструктуру каждого объекта.

### 1. Центр обработки данных.

Основное назначение цод - централизованное хранение данных, повышение надежности всей информационной инфраструктуры и обеспечение связи между цод и пользователями.

Цод содержит набор серверов, которые обеспечивают работу следующих логических подсистем:

- Информационно-биллинговая система;
- Бэк-офис;
- Демилитаризованная зона (DMZ);
- Технологический сегмент.

Инв. № подл.	Подпись и дата
Взам. инв. №	Инв. № дубл.
Подпись и дата	
Инв. № подл.	

Изм.	Лист	№ докум.	Подпись	Дата

ФАЭС.10.05.02.056

## Информационно-биллинговая система

Информационно-биллинговая система – это программно-аппаратный комплекс, предназначенный для автоматизации задач обслуживания и предоставления услуг абонентам оператора связи.

### Основные функции ибс:

- Сбор, обработка и ввод в базу данных первичной информации о предоставленных услугах и их оплате;
- Абонентский учет;
- Регистрация и контроль платежей;
- Ведение нормативно-справочной информации по услугам, тарифам, категориям абонентов;
- Тарификация и расчет платежей по предоставленным услугам связи;
- Формирование счетов абонентов;
- Информационно-справочное обслуживание абонентов и пользователей ИБС;
- Формирование документов статистической отчетности и информационно-аналитических документов по оказанным услугам категориям абонентов и прочее;
- Возможность управления коммутационным оборудованием сети оператора связи в части активизации или блокировки абонентского номера или услуг.

Данная система реализована в рамках архитектуры клиент-сервер. Вся информация, подлежащая учету в ибс, хранится на сервере базы данных в под. Клиентами сервера базы данных выступают подсистемы ибс, которые разделяются на три группы: клиентские приложения, серверные подсистемы и системы, взаимодействующие с внешними устройствами. Доступ к базе данных удаленных пользователей осуществляется через выделенные каналы связи.

Информационно – биллинговая система является важным объектом защиты информации, так как в ней содержатся данные о клиентах, заключенных

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата						
Изм.	Лист	№ докум.	Подпись	Дата	ФАЭС.10.05.02.056					Лист
										7

контрактах абонентами, а также о стоимости передачи информации по разным каналам и направлениям.

Бэк-офис

Бэк-офис включает в себя отделы компании, которые выполняют административные, обслуживающие функции и составляют корпоративную сеть компании. Цод содержит офисные серверы, на которых располагаются офисные системы, используемые на рабочих местах сотрудниками компании.

Можно выделить 4 основных типа серверов, обеспечивающих работу бэк-офиса компании:

- 1. Терминальные серверы, обеспечивающие функционирование службы удаленных рабочих столов;
- 2. Серверы приложений, включающие в себя офисное программное обеспечение, систему управления предприятием и специализированное программное обеспечение для бухгалтерского и финансового учета.
- 3. Серверы хранения данных, предназначенные для предоставления пользователям доступ к файлам, которые необходимы им для работы, ограничивая несанкционированный доступ к данным.
- 4. Вспомогательные системы, такие как прокси-сервер, почтовые серверы и т. Д.

Нарушение работоспособности данных серверов может повлечь за собой полную или частичную невозможность функционирования того или иного подразделения бэк-офиса и, как следствие, нарушение непрерывности бизнес-процессов компании.

Демилитаризованная зона

Демилитаризованная зона реализована для размещения внешних веб-ресурсов компании. Данный сегмент сети содержит набор серверов, на которых располагаются общедоступные сервисы, а именно сайт компании, «личный кабинет» клиента и другие обслуживающие сервисы и предоставляет доступ к ним как организации, так и ее клиентам.

Подпись и дата	
Инв. № дубл.	
Взам. инв. №	
Подпись и дата	
Инв. № подл.	





автоматизированные рабочие места сотрудников компании на базе тонкого клиента, что позволяет организовывать экономичные и отказоустойчивые рабочие места.

На данных рабочих местах сотрудниками осуществляется доступ к виртуальному рабочему столу через службу удаленных рабочих столов. Таким образом, в компании полностью отсутствует факт локального расположения файлов и приложений на устройствах сотрудников.

Доступ к ЦОД, а также сети интернет осуществляется через маршрутизатор и коммутаторы доступа.

3. Филиалы.

ИТ-инфраструктура филиалов компании реализована аналогично инфраструктуре главного офиса. Службы удаленных рабочих столов обеспечивает высокую производительность программ для сотрудников филиалов, которым необходим доступ к централизованным хранилищам данных.

Функционирование арм и серверов происходит под управлением операционной системы Windows.

Связь между сегментами осуществляется по каналам организации, составляющим виртуальную частную сеть (VPN).

1.3 Основные подходы в организации мониторинга инцидентов информационной безопасности

Мониторинг – это систематическое или непрерывное наблюдение за объектом с обеспечением контроля и/или измерения его параметров, а также проведение анализа с целью предсказания изменчивости параметров и принятия решения о необходимости и составе корректирующих и предупреждающих действий.[4]

Мониторинг инцидентов информационной безопасности — это процесс проверки всех событий безопасности, получаемых от различных источников, и обнаружение инцидентов информационной безопасности. Мониторинг

Подпись и дата	
Инв. № дубл.	
Взам. инв. №	
Подпись и дата	
Инв. № подл.	

					ФАЭС.10.05.02.056	Лист 10
Изм.	Лист	№ докум.	Подпись	Дата		

инцидентов информационной безопасности является одним из ведущих процессов в системе управления инцидентами информационной безопасности организации. Все основные процессы данной системы можно представить в виде PDCA-цикла. Его название – аббревиатура, сокращение от английских слов: Plan – планируй, Do – выполняй, Check – проверяй, Act – действуй. Стандарт ГОСТ Р ИСО/МЭК 27001-2006 описывает модель PDCA как основу функционирования всех процессов системы управления информационной безопасностью. Аналогично данной модели ГОСТ Р ИСО/МЭК ТО 18044-2007 подразделяет управление инцидентами информационной безопасности на 4 отдельных этапа:

- планирование и подготовка;
- использование;
- анализ;
- улучшение.[3]

Инв. № подл.	Подпись и дата				Инв. № дубл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата	
Изм.	Лист	№ докум.	Подпись	Дата	ФАЭС.10.05.02.056					Лист
										11

Основное содержание этих этапов показано на рисунке 1.



Рисунок 1 - Этапы управления инцидентами ИБ.[3]

Исходя из данной схемы мониторинг инцидентов информационной безопасности выполняется на этапе Использование и позволяет решать следующие задачи в системе управления инцидентами ИБ:

- сбор данных для дальнейшего управления инцидентами информационной безопасности;
- обеспечение непрерывного процесса выявления любых событий, которые способны повлиять на безопасность организации;
- обеспечение процесса быстрого реагирования на инциденты информационной безопасности и выявления причины возникновения инцидента в процессе расследования;

Изм.	Лист	№ докум.	Подпись	Дата	<p style="text-align: center; font-size: 1.2em;">ФАЭС.10.05.02.056</p>	<p style="text-align: right;">Лист 12</p>
Изм.	Лист	№ докум.	Подпись	Дата		
Изм.	Лист	№ докум.	Подпись	Дата		

- предоставление данных для корректировки информации об угрозах и рисках компании на основании инцидентов информационной безопасности, зарегистрированных в процессе мониторинга;

— предоставление информации для аналитики информационной безопасности объекта, планирования комплексной защиты и принятия иных управленческих решений, основываясь на анализе данных о состоянии объекта защиты, установленных событиях и инцидентах.

Формирование системы мониторинга инцидентов информационной безопасности происходит на основании уже имеющихся в компании компонентов информационной безопасности. В общем случае, такими исходными данными выступают:

— Нормативно-правовая база компании в области информационной безопасности;

- Логическая структура и схема сети компании;

— Перечень бизнес-активов компании, угроз, рисков;

— Перечень и схема внедрения используемых средств защиты информации.

Внедрение системы мониторинга инцидентов информационной безопасности происходит в соответствие с лучшими практиками и предполагает наличие следующих составляющих:

— Организационная часть;

— Программно-техническая часть.

Для наиболее эффективной разработки процесса мониторинга инцидентов информационной безопасности рекомендуется в качестве рекомендаций и руководства пользоваться требованиями международных и российских стандартов. К документам, описывающим процесс мониторинга инцидентов информационной безопасности, можно отнести:

1. Международный и национальный стандарты ISO/IEC 27001:2013 и ГОСТ Р ИСО/МЭК 27001-2006 устанавливают требования к системе управления

информационной безопасностью для её создания, развития и поддержания, а также отдельно к процессу управления инцидентами.

2. Национальный стандарт ГОСТ Р ИСО/МЭК 18044-2007 описывает инфраструктуру управления инцидентами информационной безопасности в рамках циклической модели PDCA, дает подробные спецификации для стадий планирования, эксплуатации, анализа и улучшения процесса и рассматривает вопросы обеспечения нормативно-распорядительной документацией и ресурсами по необходимым процедурам.

3. CMU/SEI-2004-TR-015 описывает методологию планирования, внедрения, оценки и улучшения процессов управления инцидентами информационной безопасности. При этом основной упор делается на организацию работы группы или подразделения, обеспечивающего сервис и поддержку предотвращения, обработки и реагирования на инциденты информационной безопасности.

4. Нормативный документ США NIST SP 800-61 представляет собой сборник «лучших практик» по построению процессов управления инцидентами ИБ и реагирования на них.

1.3 Анализ регламентирующих документов

Первоначальным этапом создания системы мониторинга инцидентов ИБ является разработка необходимых нормативных документов и внесение поправок и дополнений в уже имеющиеся документы компании в области информационной безопасности.

Основным документом, описывающим и регулирующим обеспечение информационной безопасности в компании, является политика безопасности. Политика безопасности — совокупность правил, процедур или руководящих принципов в области безопасности для определенной организации. Обычно под политикой информационной безопасности понимается высокоуровневый

Подпись и дата	
Инв. № дубл.	
Взам. инв. №	
Подпись и дата	
Инв. № подл.	

					ФАЭС.10.05.02.056	Лист 14
Изм.	Лист	№ докум.	Подпись	Дата		

документ, предназначенный для обеспечения управления ИБ в соответствии с требованиями бизнеса, партнеров, клиентов, законодательной базы.

Однако кроме высокоуровневой политики, целесообразно выделить низкоуровневых политик (частных политик), которые, как правило, должны показывать требования в определенной области или сегменте. В случае разработки системы мониторинга инцидентов ИБ предполагается внесение поправок в высокоуровневую политику безопасности компании и разработка низкоуровневой политики проведения мониторинга инцидентов информационной безопасности. Как правило, данная политика должна включать в себя следующие разделы:

1. Общие (вводные) положения;
  2. Область действия политики;
  3. Цель разработки политики;
  4. Ссылки на стандарты, другие источники, на основании которых разработана политика;
  5. Реализация политики мониторинга инцидентов ИБ:
    - Критерии идентификации и оценки инцидентов ИБ;
    - Роли и ответственность;
    - Процедуры мониторинга ИБ, проводимые ответственным подразделением с использованием программно-технических средств;
    - Процедуры мониторинга ИБ, проводимые ответственным подразделением на основе организационных мер;
  6. Контроль за соблюдением требований политики управления инцидентами ИБ;
  7. Ответственность за несоблюдение требований политики управления инцидентами ИБ;
  8. Заключительные положения
- Упомянутые выше документы ориентированы на специалистов ИБ, руководителей подразделений. Для пользователей необходимо разработать

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата	ФАЭС.10.05.02.056	Лист					
							Изм.	Лист	№ докум.	Подпись	Дата

документ - инструкцию, в котором доступным языком будут сформулированы требования, которые должны выполнять сотрудники. Данный документ должен содержать следующее:

1. Общую информацию о том, что такое инцидент информационной безопасности;
2. Алгоритм – подробную информацию о том, кому и в каком виде сотрудник должен сообщить о возникновении инцидента, перечень действий, которые сотруднику следует выполнить самостоятельно (или же предупредить о том, что выполнять какие-либо действия самостоятельно запрещено);
3. Координаты ответственных лиц.

#### 1.4 Исследование центра обеспечения безопасности

Предприятия, занимающиеся производством, могут иногда держать в тайне процесс производства, такая информация является коммерческой тайной.

Например, сведения о структуре производства, производственных мощностях, типе и размещении оборудования, запасах материалов, комплектующих и готовой продукции могут относиться к коммерческой тайне. Также к коммерческой тайне можно отнести цели компании на её дальнейшее развитие, планы о расширении, сведения о используемых технологиях.

Есть несколько видов коммерческой тайны, которые имеют разный уровень секретности и соответственно, чем выше уровень, тем более серьезные убытки понесет компания при их разглашении.

У компаний имеется и открытая информация, разглашение таких сведений не несет угрозы для коммерческой деятельности компании.

В компании также присутствуют персональные данные о клиентах и работниках. Обработка и хранение персональных данных должна осуществляться с соблюдением принципов и правил, предусмотренных федеральным законом о персональных данных. Необходимо получить согласие на обработку

Инв. № подл.	Подпись и дата				Лист 16
	Инв. № дубл.				
	Взам. инв. №				
	Подпись и дата				
Изм.	Лист	№ докум.	Подпись	Дата	ФАЭС.10.05.02.056



персональных данных, в том числе и на передачу третьим лицам, если присутствует такая необходимость.

Подход к защите базы данных состоит из последовательных этапов:

- определение адекватной модели угроз;
- оценка рисков;
- разработка системы защиты на ее основе с использованием методов, предусмотренных для соответствующего класса информационных систем (ИС);
- проверка готовности систем защиты информации (СЗИ) с оформлением соответствующей документации (описание системы, правила работы, регламенты и т.д.), в том числе заключения о возможности эксплуатации данной СЗИ;
- установка и ввод в эксплуатацию СЗИ;
- учет применяемых СЗИ, технической документации к ним, а также носителей ПД;
- учет лиц, допущенных к работе с персональными данными в ИС;
- разработка полного описания системы защиты персональных данных;
- контроль использования СЗИ. [4]

Самые распространенные персональные данные, которые используются на сайтах это ФИО, телефон и email. Такая информация используется для авторизации пользователя на сайте. В некоторых ситуациях используются еще данные о месте проживания.

Для хранения этих данных используются СУБД. К самым распространенным СУБД относятся Oracle, MySQL, Microsoft SQL Server, Microsoft Access

Мониторинг инцидентов информационной безопасности – автоматизированный процесс, который, как правило, реализуется посредством специальных программно-аппаратных средств.

Но в некоторых случаях более эффективным и быстрым является реагирование на инциденты персоналом. В правильно организованной системе компетентные лица знают, что следует делать в случае обнаружения инцидентов. Важной частью в управлении системой мониторинга инцидентов

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата	<p>Самые распространенные персональные данные, которые используются на сайтах это ФИО, телефон и email. Такая информация используется для авторизации пользователя на сайте. В некоторых ситуациях используются еще данные о месте проживания.</p> <p>Для хранения этих данных используются СУБД. К самым распространенным СУБД относятся Oracle, MySQL, Microsoft SQL Server, Microsoft Access</p> <p>Мониторинг инцидентов информационной безопасности – автоматизированный процесс, который, как правило, реализуется посредством специальных программно-аппаратных средств.</p> <p>Но в некоторых случаях более эффективным и быстрым является реагирование на инциденты персоналом. В правильно организованной системе компетентные лица знают, что следует делать в случае обнаружения инцидентов. Важной частью в управлении системой мониторинга инцидентов</p>
Изм.	Лист	№ докум.	Подпись	Дата	<p>ФАЭС.10.05.02.056</p>
					<p>Лист</p> <p>17</p>

информационной безопасности является организация работы со штатным персоналом компании. Как уже говорилось в п. 1.3., для пользователей следует разработать инструкцию, регулиующую порядок реагирования на инциденты.

Для наиболее эффективного усвоения сотрудниками необходимых требований реагирования на инциденты ИБ целесообразно проведение инструктажей. Такие инструктажи должны быть плановыми, также возможно проведение внеплановых инструктажей при внесении каких-либо изменений в требования политики.

Организационный центр оперативного мониторинга и реагирования на инциденты кибербезопасности (SOC) представляет собой группу экспертов по защите информации, отвечающую за постоянный контроль и анализ состояния безопасности организации, используя комбинацию технологических решений и действуя в рамках четко выстроенных процессов. SOC обычно укомплектованы аналитиками и инженерами в области безопасности, а также сервис-менеджерами, которые обеспечивают оперативное взаимодействие с клиентом.

Кроме того, для быстрого устранения последствий инцидентов подключается группа реагирования. SOC призван отслеживать активность в сетях, на серверах и рабочих станциях, в базах данных, приложениях, веб-сайтах и других системах, обнаруживая аномальные и злонамеренные действия, которые могут указывать на инцидент безопасности или компрометацию данных.

Для сравнения рассмотрим три наиболее известных в России коммерческих SOC представленных в таблице 1.1:

- Solar JSOC
- BI.ZONE SOC
- IZ:SOC

Таблица 1.1– Сравнение коммерческих Центров обеспечения безопасности

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата	<div style="text-align: right; font-size: 1.2em; font-weight: bold;">ФАЭС.10.05.02.056</div>	Лист					
							Изм.	Лист	№ докум.	Подпись	Дата

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата

Критерий сравнения	Solar JSOC	BI.ZONE SOC	IZ:SOC
Способы подключения площадок клиента	Сервер коллекторов поставщика SOC разворачивается на площадке клиента или SOC интегрируется с существующими LM/SIEM-системами заказчика	Сервер коллекторов поставщика SOC разворачивается на площадке клиента или SOC интегрируется с существующими LM/SIEM-системами заказчика	Сервер коллекторов поставщика SOC разворачивается на площадке клиента или SOC интегрируется с существующими LM/SIEM-системами заказчика
Возможность разворачивания коллекторов в виртуальной среде	Любая среда виртуализации	Любая среда виртуализации, обеспечивающая работоспособность Red Hat Enterprise Linux	Любая среда виртуализации, обеспечивающая работоспособность ОС *.nix

Продолжение таблицы 1.1

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата

Типы поддерживаемых источников	Более 40 (DLP, AD, OS, IDS, AV, AntiDDoS, WAF, FW, Proxy, AntiSpam, VM, EDR, DB, Mail, VPN, Web, CRM, TDS, DNS, DHCP, СЗИ от НСД, HoneyPot, Sandbox, Hypervisor, операционные системы, бизнес-приложения)	Около 30 типов	Около 30 типов
Общее количество поддерживаемых источников (вендоров)	401	400	344
Подключение нестандартных источников	72 часа	До 5 рабочих дней	От 2 дней

Продолжение таблицы 1.1

[illegible]

Инв. № подл.	Подпись и дата	
	Инв. № дубл.	
	Взам. инв. №	
	Подпись и дата	
	Инв. № подл.	

Метод сбора событий	Безагентский	Агентский, безагентский, смешанный	Агентский, безагентский, смешанный
количество типов стандартных правил корреляции (use cases)	Более 200 унифицированных сценариев	8 типов, 250 правил	30 типов, более 300 правил
Количество типов стандартных правил корреляции (use cases)	Более 200 унифицированных сценариев	8 типов, 250 правил	30 типов, более 300 правил
Разработка правил корреляции для клиента	72 часа	1-3 рабочих дня	От 1 рабочего дня
Корреляция событий по историческим данным	Да	Да	Да
Возможность задать информацию об активах и уровень их критичности	Да	Да	Да

(assets)			
----------	--	--	--

Продолжение таблицы 1.1

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата	<div>ФАЭС.10.05.02.056</div>				Лист
									23
Изм.	Лист	№ докум.	Подпись	Дата					

Предоставление клиенту оборудования для разворачивания коллекторов	Платно	Платно	Платно
Возможность выбора сценариев мониторинга	Несколько наборов корреляционных правил: AV health, Internet Access and Application Control, Threat Hunting, User Management, Credential Theft, Network Security, Critical system profiling, возможность подключения индивидуальных сценариев, бизнес-систем и АСУ ТП	Сценарии по техникам и тактикам атак MITRE ATT&CK; по категориям источников событий; по решаемым функциональным задачам (контроль привилегированных пользователей, мониторинг сетевого периметра, выявление нарушения политик ИБ и т.п.)	Есть пакеты типовых сценариев и шаблоны сценариев для адаптации

Инва. № подл.	Подпись и дата	Взам. инв. №	Инва. № дубл.	Подпись и дата
Изм.	Лист	№ докум.	Подпись	Дата



Продолжение таблицы 1.1

Инв. № подл.	Подпись и дата				Взам. инв. №	Инв. № дубл.	Подпись и дата	
Изм.	Лист	№ докум.	Подпись	Дата	ФАЭС.10.05.02.056			Лист
								25

	Подпись и дата	
	Инв. № дубл.	
	Взам. инв. №	
	Подпись и дата	
Инв. № подл.		

Передача клиенту правил корреляции, разработанных по его требованиям	Да (в рамках отдельной услуги)	Да	Да (только если услуга оказывается при помощи SIEM заказчика)
Хранение и обработка «сырых» событий на стороне клиента без их передачи в облако провайдера (внутри периметра компании)	Да	Да	Да
Минимальные требования к инфраструктуре клиента: наличие оборудования и ПО	Наличие хотя бы 1 источника событий	Наличие ресурсов для развертывания сервера коллекторов либо наличие у заказчика уже развернутого LM/SIEM, с которого можно перенаправить события в сторону поставщика	Наличие хотя бы 1 источника событий
Минимальная ширина канала	5 Мбит/с	5 Мбит/с	0,72 Мбит/с

Изм.	Лист	№ докум.	Подпись	Дата

ФАЭС.10.05.02.056

Лист

26

## 1.7 Вывод

В первом разделе были рассмотрены основные подходы в организации мониторинга инцидентов ИБ, также был проведен анализ регламентирующих документов. Рассмотрена необходимость в составе компании центра управления инцидентами.

Инов. № подл.	Подпись и дата	Взам. инв. №	Инов. № дубл.	Подпись и дата
Изм.	Лист	№ докум.	Подпись	Дата
ФАЭС.10.05.02.056				Лист
				27

## 2 Исследование и анализ программно-аппаратных систем мониторинга инцидентов ИБ

### 2.1 Постановка задачи

В данной главе основной задачей является разобрать понятие SIEM-системы. Также необходимо разобрать основные принципы работы SIEM-систем.

### 2.2 Исследование и применение SIEM-систем

Программно-техническая часть системы мониторинга инцидентов информационной безопасности реализуется на основе продуктов по мониторингу событий безопасности класса SIEM (Security Information and Event Management).

Реализация SIEM – системы основана на объединении функционала двух других подсистем мониторинга и управления информационной безопасностью: SIM (Security Information Management), выполняющей сбор, хранение, анализ записей журнала и формирование отчетности, и SEM (Security Event Management), основанной на проведении мониторинга событий безопасности в реальном времени, выявлении инцидентов безопасности и реагирование на них. Таким образом, SIEM – это программно-аппаратное или программное средство, предназначенное для ведения комплексного контроля процессов функционирования системного и прикладного программного обеспечения, применяемого в данной системе средств вычислительной техники, в режиме реального времени.

Важно понимать, что система SIEM не способна самостоятельно предотвращать инциденты, как и не имеет встроенных защитных функций. Ее основные цели: анализ информации, собираемой из различных источников и последующее выявление отклонений от норм по заданным критериям.

Для достижения данных целей перед системой SIEM ставятся

Подпись и дата	
Инв. № дубл.	
Взам. инв. №	
Подпись и дата	
Инв. № подл.	
Изм.	Лист
№ докум.	Подпись
Дата	
ФАЭС.10.05.02.056	
Лист	
28	

- Обеспечение возможности анализа событий и расследования инцидентов;
- Обработка и корреляция событий по заданным правилам и политикам;
- Хранение журналов событий от различных источников и их консолидация;
- Оповещение и предоставление инструментов для управления и необходимой работы с инцидентами.

Нормализация означает приведение форматов записей журналов, собранных из различных источников, к единому внутреннему формату, который затем будет использоваться для их хранения и последующей обработки.

Классификация позволяет для атрибутов событий безопасности определить их принадлежность к определенным классам.

Корреляция выявляет взаимосвязи между разнородными событиями, что позволяет обнаруживать атаки на инфраструктуры, а также нарушения критериев и политики безопасности.

Генерация отчетов и предупреждений означает формирование, передачу, отображение и (или) печать результатов функционирования.

Принятие решений определяет выработку мер по реконфигурированию средств защиты с целью предотвращения атак или восстановления безопасности

инфраструктуры.

Визуализация информации предполагает представление в графическом виде данных, характеризующих результаты анализа событий безопасности и состояние защищаемой инфраструктуры и ее элементов. Нормализация означает приведение форматов записей журналов, собранных из различных источников, к единому внутреннему формату, который затем будет использоваться для их хранения и последующей обработки.

2.3 Анализ основных принципов работы и характеристик SIEM-системы

SIEM-системы разных производителей имеют различные подходы в реализации, предоставляемых сервисах и т.д. Однако, общая идея всех SIEM – обработать большой объем первичных данных, не поддающийся анализу человеком, и выдать небольшой набор потенциальных инцидентов.

В общем случае функционирование SIEM-системы обеспечивают следующие компоненты:

- Агенты, осуществляют сбор журналов событий и их передачу на сервер;
- Серверы-коллекторы, отвечают за сбор событий от множества различных источников;
- сервер-коррелятор, обеспечивает сбор информации от коллекторов и агентов и обработку по правилам и алгоритмам корреляции, заданным в системе;
- Сервер хранилища и баз данных, необходим для хранения журналов событий и их обработки.

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата						
Изм.	Лист	№ докум.	Подпись	Дата	ФАЭС.10.05.02.056					Лист
										30

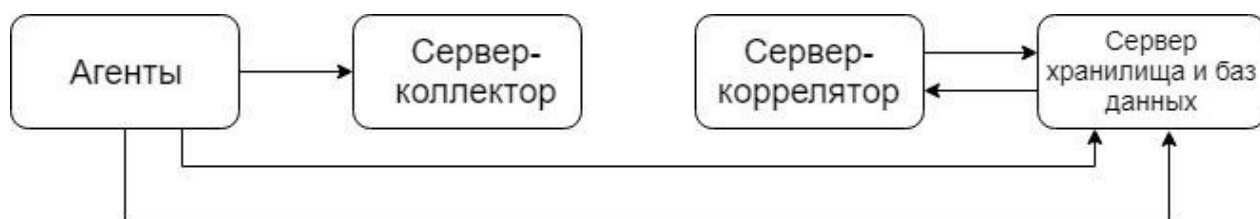


Рисунок 2.1 - Структурная схема SIEM-системы

Принцип работы SIEM заключается в сборе информации из различных источников посредством агентов и серверов-коллекторов. Информация заносится в специализированное хранилище (базу данных). Агент - составляющая программы, расширение или плагин, предоставленный SIEM, который выполняет функции переноса и преобразования записей системного журнала от источника в коллектор siem. Ключевые особенности таких агентов: префильтрация записей системного журнала, основываясь на их степени опасности, и структурирование входящих данных для дальнейшей работы. Агенты передают записи по защищенному каналу.

Серверы-коллекторы – это посредники между приложениями SIEM и агентами сети. Коллекторы способны к корреляции, но обычно они занимаются процессом структурирования записей системного журнала для приложений SIEM. Коллекторы могут быть обособлены, либо входить в состав приложения. Такой сбор данных позволяет осуществлять целостную оценку событий безопасности, способствует невозможности неконтролируемой конфигурации средств анализа событий. Негативным пунктом такого построения системы является возрастание нагрузки на сеть.

После сбора информации SIEM -система осуществляет анализ событий ИБ для обнаружения инцидента. Сервер-коррелятор находит связанные события и строит цепочки корреляции. Определенные особенности построенных цепочек корреляции могут служить индикатором того, что система под угрозой. По результатам анализа SIEM-система показывает выявленные инциденты ИБ.

Инв. № подл.	Подпись и дата				Лист 31
	Инв. № дубл.				
	Взам. инв. №				
	Подпись и дата				
Изм.	Лист	№ докум.	Подпись	Дата	ФАЭС.10.05.02.056

Агенты передают записи по защищенному каналу.					
<p>Серверы-коллекторы – это посредники между приложениями SIEM и агентами сети. Коллекторы способны к корреляции, но обычно они занимаются процессом структурирования записей системного журнала для приложений SIEM. Коллекторы могут быть обособлены, либо входить в состав приложения. Такой сбор данных позволяет осуществлять целостную оценку событий безопасности, способствует невозможности неконтролируемой конфигурации средств анализа событий. Негативным пунктом такого построения системы является возрастание нагрузки на сеть.</p> <p>После сбора информации SIEM -система осуществляет анализ событий ИБ для обнаружения инцидента. Сервер-коррелятор находит связанные события и строит цепочки корреляции. Определенные особенности построенных цепочек корреляции могут служить индикатором того, что система под угрозой. По результатам анализа SIEM-система показывает выявленные инциденты ИБ.</p>					

За счет своей логики SIEM-система является универсальным и уникальным инструментом. Однако для того, чтобы добиться эффективного функционирования данной системы, необходимо произвести выбор источников, которые будут подавать на вход системы данные для последующей обработки. Предположение «чем больше источников событий – тем меньше вероятность пропустить важное событие и не идентифицировать значимый инцидент» не является верным. При очень больших потоках событий возрастает вероятность ошибок, так как обработка большего количества событий приводит к усложнению задачи написания комплексных корреляционных правил и процесса фильтрации этих самых ошибок.

Лучшие практики рекомендуют "обрезать" объем событий посредством определения важности и конкретных модулей-источников. Критериями отбора таких источников являются следующие факторы:

— Критичность информационной системы и информации в ней обрабатываемой и хранимой;

— достоверность и информативность источника событий;

— покрытие каналов передачи информации.

решаемые задачи области ИТ и ИБ, например, обеспечение непрерывности, расследование инцидентов, соблюдение политик, предотвращение утечек информации и т. П.

Основными источниками информации для современных систем класса SIEM выступают:

— Системы контроля доступа и аутентификации – для мониторинга контроля доступа к информационным системам и использования привилегий;

— Журналы событий серверов и рабочих станций – для контроля доступа, обеспечения непрерывности, соблюдения политик информационной безопасности;

— Активное сетевое оборудование – для контроля изменений и доступа, счетчики сетевого трафика;

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата	<p>ФАЭС.10.05.02.056</p>	Лист
Изм.	Лист	№ докум.	Подпись	Дата	32	



— Средства обнаружения и предотвращения вторжений (ids/ips) – для отслеживания событий о сетевых атаках, изменении конфигураций и доступа к устройствам;

— Межсетевые экраны – для предоставления сведений об атаках, вредоносном ПО и т.д.

— Средства антивирусной защиты для контроля работоспособности программного обеспечения, баз данных, изменений конфигураций и политик, регистрации вредоносных программ;

— Средства анализа защищенности — для получения информации об уязвимостях программного обеспечения и сетевых устройств;

— GRC-системы – для выявления и учета рисков и наиболее критичных угроз, приоритезации инцидента;

Прочие системы защиты и контроля политик ИБ, например, DLP;

— Системы инвентаризации и управления активами — для выявления новых устройств и программного обеспечения, в том числе установленных несанкционированно;

— Системы учета трафика.

Оценить преимущества SIEM-решения поможет анализ по основным характеристикам.

1. Источники и обработка событий:

Чем больше источников событий поддерживает система, тем эффективнее защита. При этом важно, чтобы SIEM-система обеспечивала индивидуальный подход к нормализации каждого события из различных источников.

Работу с программой облегчает разбивка событий по категориям. Синтаксический анализ информационных потоков (парсинг) подобных решений реализуется с помощью обозначения наиболее критичных полей. Обновляются парсеры, как правило, одновременно с внедрением дополнений или изменений системы.

Автонахождение, а также периодическое обновление источников эксперты относят к преимуществам. Однако единого мнения по вопросу обновления SIEM-

Подпись и дата	
Инв. № дубл.	
Взам. инв. №	
Подпись и дата	
Инв. № подл.	
Изм.	Лист
№ докум.	Подпись
Дата	

ФАЭС.10.05.02.056

Лист  
33

решения не существует. Отсутствие автообновления анализаторов вендоры иногда объясняют защитой от изменений логики анализа и предлагают проводить изменения SIEM под контролем собственных специалистов. Такой подход увеличивает стоимость владения системой.

В итоге: стоит выбирать решение, которое взаимодействует с максимальным количеством разнородных систем, которые используются в компании. Многоуровневая платформа обработки инцидентов ускорит работу с источниками и легко адаптируется к программному обеспечению. Невысокие требования к аппаратно-программным средствам при этом будут дополнительным преимуществом. Отечественные разработчики реализуют в SIEM поддержку источников событий российского происхождения, которых нет у иностранных конкурентов, что также станет плюсом для заказчиков из России.

## 2. Сбор инцидентов:

Эффективная SIEM – это платформа с функциями нормализации, объединения и фильтрации инцидентов. Преимуществом будет обработка и хранение raw-событий. Скорость процессов при этом на общую картину не влияет. Маскирование сведений, мониторинг сетевого трафика – функции вспомогательные, но не бесполезные.

Проверить корректность работы нормализации, фильтрации и агрегации возможно на этапе тестирования SIEM в «боевом» режиме. Поэтому больше доверия вызывают производители, которые предоставляют бесплатный тест-драйв полнофункциональной версии продукта.

## 3. Корреляция:

Оптимальное SIEM-решение сопоставляет события в режиме реального времени, умеет проводить поведенческий анализ и сравнение исторических данных. Гибкие настройки системы корреляции, обогащение инцидентов в коннекторе или в консоли управления, дополнительная функция в виде ручной проверки, возможность одновременной работы со всеми механизмами – отличительные особенности удачной SIEM.

## 4 Визуализация:

Инв. № подл.	Подпись и дата				Лист 34
	Инв. № дубл.				
	Взам. инв. №				
	Подпись и дата				
Изм.	Лист	№ докум.	Подпись	Дата	ФАЭС.10.05.02.056

Комфортную работу ИБ-специалисту обеспечит русифицированный интерфейс. Это не принципиальный критерий выбора, но при прочих равных условиях – выгодно отличие.

Удобство работы с SIEM зависит прежде всего от наличия встроенных условий корреляции событий, графических панелей и шаблонов отчетов. Чем больше встроенных корреляционных ресурсов, тем меньше квалифицированной, а значит – платной помощи от сторонних специалистов потребуется при обслуживании платформы. Например, при разработке «СёрчИнформ SIEM» специалисты проанализировали типовые задачи клиентов из разных отраслей в России и СНГ.

## 6 Удобство применения:

Важный маркер удобства работы с SIEM – возможность централизованно координировать компоненты платформы из единой консоли, а также автоматически обновлять предустановленные политики и шаблоны отчетности. Все это облегчит труд специалиста по информационной безопасности. Еще один плюс в пользу решения – оперативность и качество технической поддержки. По этому параметру в большинстве случаев выигрывают отечественные производители, главным образом, из-за невысокой стоимости.

Оценка SIEM по основным характеристикам обеспечивает выбор решения на предварительном этапе. Параметры «успешности» у разных заказчиков



- цены на предоставляемые услуги;
- планы развития компании, маркетинговая стратегия;
- информация по проведенным транзакциям.

Информация, составляющая коммерческую тайну, располагается на серверах хранения данных в ЦОД.

Актуальные угрозы нарушения конфиденциальности, целостности, доступности персональных данных клиентов и коммерческой тайны представлены в приложении а.

## Доступ клиентов к веб-ресурсам компании

Веб-ресурсы компании составляет набор серверов, на которых располагаются общедоступные сервисы, а именно сайт компании, «личный кабинет» клиента и другие обслуживающие сервисы.

Угрозы, направленные на нарушение возможности доступа клиентов к веб-ресурсам компании представлены в приложении б.

Функционирование систем, обеспечивающих предоставление услуг связи абонентам

К системам, обеспечивающим предоставление услуг связи абонентам  
компаний, относятся:

- центр коммутации мобильной связи (MSC);
- оборудование голосового ядра;
- оборудование пакетного ядра;
- абонентские интернет-шлюзы;
- оборудование сигнальной сети;
- СМС-центры.

Угрозы, направленные на нарушение функционирования систем, обеспечивающих предоставления услуг связи абонентам компании, представлены в приложении В.

В рассматриваемой компании организована комплексная защита информации. Используемые средства защиты информации представлены в таблице 3.1.

Таблица 3.1 - средства защиты информации

Категория СЗИ	Функции	Наименование продукта	Место установки	Наличие сертификата ФСТЭК
Антивирусное программное обеспечение	Защита от вредоносного ПО серверов в ЦОД и рабочих мест пользователей в главном офисе компании и филиалах	Kaspersky Endpoint Security для Windows	Сервер ПО в ЦОД и клиентские программы на рабочих местах сотрудников	№ 4068 от 22.01.2019г.
Межсетевой экран нового поколения (Next-Generation Firewall) (NGFW)	Сегментирование сети, разграничение доступа между подсетями; Реализация функций системы обнаружения вторжений;	FortiGate 7040E	Программно-аппаратный комплекс, устанавливается на границах сети ЦОД,	№ 3720

Инв. № подл.	Подпись и дата
Взам. инв. №	Инв. № дубл.
Подпись и дата	
Инв. № подл.	

Изм.	Лист	№ докум.	Подпись	Дата
------	------	----------	---------	------

ФАЭС.10.05.02.056

Лист

38

Продолжение таблицы 3.1

Межсетевой экран для веб-приложений (Web Application Firewall) (WAF)	Контроль и фильтрация информационных потоков по протоколу передачи гипертекста, проходящих к веб-серверу и от веб-сервера	PT Application Firewall	Программно-аппаратный комплекс, устанавливается на границе DMZ-сегмента сети	№3455 от 27.10.2015 г.
IDM-система	Управление идентификационным и данными и правами доступа пользователей в информационных системах организации	Indeed Access Manager	Сервер ПО устанавливается в ЦОД	-
DLP-система	Предотвращение утечки защищаемой информации, контроль действий сотрудников	InfoWatch Traffic Monitor	Сервер ПО устанавливается в ЦОД, агентские программы устанавливаются на рабочих местах сотрудников	-
Средство защиты виртуализации и	Контроль инфраструктуры, действий администраторов и фильтрацию сетевого трафика	vGate R2	Сервер ПО устанавливается в ЦОД	№ 2308 от 28.03.2011г.

Инов. № подл.	Подпись и дата	Взам. инв. №	Инов. № дубл.	Подпись и дата

Изм.	Лист	№ докум.	Подпись	Дата

ФАЭС.10.05.02.056

Лист

39

	на уровне гипервизора			
--	--------------------------	--	--	--

Продолжение таблицы 3.1

Система контроля защищенности и соответствия стандартам	Оценка защищенности ИС и АРМ, оценка ИС на соответствие стандартам, контроль изменений состава ПО ИС и АРМ	MaxPatrol	Сервер ПО устанавливается в ЦОД	№ 2922 от 08.07.2013 г.
Эмулятора среды функционирования программного обеспечения (песочница)	Проверка файлов с помощью изолированной среды для безопасного исполнения компьютерных программ	Fortinet FortiSand-box	Сервер ПО устанавливается в ЦОД	-
Шлюз защиты электронной почты	Блокировка спама, фильтрация вредоносных ссылок и файлов, фишинговых писем	Fortimail	Сервер ПО устанавливается в ЦОД	-

Рассмотрим подробнее некоторые средства защиты информации.

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата

Изм.	Лист	№ докум.	Подпись	Дата

ФАЭС.10.05.02.056

Лист

40



Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата



информационной безопасности, дополняя или заменяя пароли. Поддерживаются различные способы аутентификации, за счет этого Indeed АМ адаптируется к требуемым сценариям доступа и в каждом конкретном случае предлагает пользователям оптимальную технологию аутентификации.

Помимо различных технологий аутентификации, Indeed АМ использует широкий спектр технологий интеграции, которые позволяют подключить целевые приложения к системе аутентификации. Такие технологии включают реализацию подхода Single Sign-On (web и enterprise sso), стандартизированные протоколы аутентификации и агентские модули. Indeed Access Manager позволяет организовать контролируемый доступ к информационным ресурсам как из внутренней сети компании, так и к системам, доступным из внешней сети, таким как почта, VPN, VDI и web-порталы. Такой подход позволяет построить централизованную систему предоставления доступа, которая охватывает все используемые целевые системы, минимизирует количество обращений пользователей в службу help desk, сокращает расходы на сопровождение инфраструктуры и повышает эффективность работы пользователей.

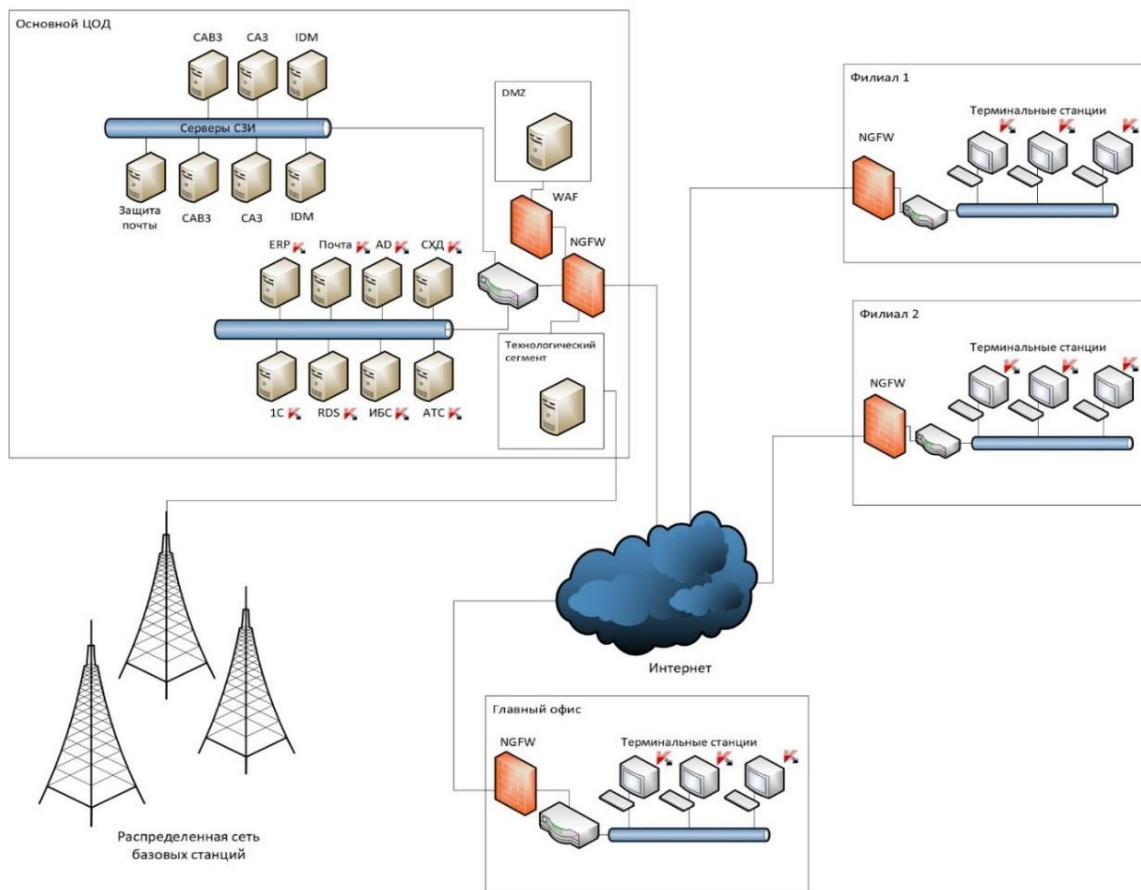
### 5. InfoWatch Traffic Monitor

InfoWatch Traffic Monitor надежно работает под большими нагрузками на сотнях тысяч рабочих мест не только в режиме мониторинга, но и блокировки. Чтобы минимизировать проблему ложных срабатываний, традиционную для всех DLP, InfoWatch Traffic Monitor сделал ставку на развитие технологий анализа контента и за 15+ лет продуктовой жизни стал технологическим лидером среди аналогов.

Система «ловит» сложные текстовые и графические объекты даже в случае, если нарушитель сумел значительно видоизменить их и ухитрился замаскировать свои действия. Благодаря многомерному анализу содержания, InfoWatch Traffic Monitor понимает, о какой информации идет речь. Это облегчает сотруднику службы информационной безопасности неблагодарную работу с ложноположительными срабатываниями.

Схема расположения средств защиты представлена на рисунке 2.2

Инв. № подл.	Подпись и дата				Лист 43
	Инв. № дубл.				
	Взам. инв. №				
	Подпись и дата				
Изм.	Лист	№ докум.	Подпись	Дата	ФАЭС.10.05.02.056




 - средство антивирусной защиты  
Kaspersky Endpoint Security

Рисунок 2.2 - Схема расположения средств защиты информации

## 2.5 Вывод

В главе было разобрано понятие SIEM-системы, а также были рассмотрены основные принципы работы SIEM-системы.

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата

Организация системы мониторинга инцидентов является трудоемким и финансово затратным процессом. В практической части данной работы рассмотрено внедрение программно-аппаратной части системы мониторинга инцидентов информационной безопасности. Данный процесс, включает в себя следующие этапы:

- ### 3.2 Анализ и выбор SIEM-системы

В настоящее время на российском рынке представлено большое количество как западных, так и отечественных siem-решений. Лидерами в области SIEM, по данным агентства gartner, являются ibm qradar, hewlett packard arc sight, splunk siem, mcafee siem, logrhythm siem, отечественные же решения преимущественно применяются только на территории РФ.

Современная SIEM-система должна удовлетворять следующим требованиям:

— SIEM-система должна предоставлять возможность расследовать инцидент. Администратор в ежедневных задачах проводит анализ инцидентов, обращается к данным, которые предвещали событие. Анализ инцидента позволяет более точно принять меры по предотвращению;

— SIEM-система должна не просто получать информацию, но быть «умной» и обогащать события дополнительной информацией, которая сможет расширить аналитику событий ИБ;

— SIEM-система должна предоставлять необходимую и запрашиваемую отчетность. Отчетность в SIEM позволяет визуально увидеть состояние информационной безопасности организации, оценить изменения и предоставить данные для высшего руководства организации как эффективность работы службы ИБ.

При принятии решения об интеграции siem-системы в рассматриваемой компании, ввиду развития импортозамещения в России, в том числе в области информационной безопасности, рассмотрены две наиболее популярных отечественные siem-системы: maxpatrol siem компании positive technologies и rusiem от компании "русием". Рассмотрим возможности выбранных siem-систем подробнее.

#### 1. Positive technologies maxpatrol siem

Maxpatrol siem — продукт российской компании positive technologies. Продукт поставляется в программном и программно-аппаратном исполнении.

С момента запуска продукта в 2015 году реализовано более 50 проектов по внедрению системы в государственных и коммерческих организациях.

Особенностью maxpatrol siem является актив-ориентированный подход, который обеспечивает устойчивость работы системы к изменениям в информационно-технологической инфраструктуре компании. Правила корреляции применяются к динамической группе активов (компьютеров, серверов и др.), которая формируется по выбранным признакам и состав которой может изменяться с развитием сети.

Информация постоянно пополняется новыми данными об ИТ-инфраструктуре за счет новых событий, результатов сканирований, сетевого трафика и агентов на конечных точках, создавая полную IT-модель предприятия. Эта возможность позволяет оценивать возникающие инциденты с привязкой к

Инв. № подл.	Подпись и дата				Лист 46
	Инв. № дубл.				
	Взам. инв. №				
	Подпись и дата				
Изм.	Лист	№ докум.	Подпись	Дата	ФАЭС.10.05.02.056

конкретным узлам сети и снизить число ложных срабатываний за счет сопоставления событий с текущими параметрами хостов.

В MaxPatrol SIEM реализован механизм передачи данных для экспертизы в исследовательский центр positive research, основанный на базе знаний positive technologies knowledge base (pt kb). В результате применения pt kb удастся снизить требования к экспертизе пользователей siem-системы, которые теперь не должны самостоятельно разбираться в признаках компрометации, разрабатывать правила корреляции и нормализации логов.

Преимущества maxpatrol siem:

— MaxPatrol SIEM предлагает полноценный функционал систем управления активами (Asset Management). Это позволяет создавать и автоматически обновлять группы активов по организационным, территориальным, функциональным и любым другим признакам;

— MaxPatrol SIEM автоматически строит топологию сети и постоянно обновляет ее данными от источников и по результатам сканирований.

— MaxPatrol SIEM приоритезирует инциденты в соответствии с важностью актива, и как следствие, позволяет реагировать только на действительно важные инциденты и снизить нагрузку на операторов системы;

— MaxPatrol SIEM предлагает открытый стандартизированный API, который позволяет осуществлять загрузку или выгрузку информации на любой момент работы системы. Это позволяет быстро решить ряд практических задач: выполнить интеграцию с SMS-шлюзом, корпоративным порталом, самописными приложениями и т. д.

— модульная архитектура позволяет построить любую конфигурацию системы, которая отвечает требованиям заказчика и не содержит избыточной функциональности, что дает существенную экономию средств при внедрении;

— специалисты Positive Technologies обеспечивают подключение источников без дополнительных затрат со стороны заказчиков. MaxPatrol SIEM обновляет правила нормализации через модуль PT KB, благодаря чему логи корректно интерпретируются после обновления источников;

Инв. № подл.	Подпись и дата				Лист 47
	Инв. № дубл.				
	Взам. инв. №				
	Подпись и дата				
Изм.	Лист	№ докум.	Подпись	Дата	ФАЭС.10.05.02.056

— решения Positive Technologies целиком спроектированы в России, с учетом специфики решаемых задач и требований регуляторов. В основе продукта лежит уникальная база знаний, накопленная за годы проведения масштабных тестов на проникновение, расследования сложных.

Maxpatrol SIEM входит в реестр российского по №1143, имеет сертификат минобороны рф № 3044 и сертификат фстэк россии № 3734, подтверждающий выполнение требований руководящего документа «защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия не декларированных возможностей» (гостехкомиссия россии, 1999) по 4 уровню контроля и технических условий.

## 2. RuSIEM

RuSIEM — российская разработка отечественной компании русием, резидента сколково. Разработка ведется с 2014 года. Решение позволяет организовать централизованный и распределенный сбор событий с систем любого класса (включая систему контроля и управления доступом), автоматическое обнаружение инцидентов ит, иб и бизнес-процессов по правилам корреляции и с применением механизмов искусственного интеллекта.

Развертывание решения возможно как в виртуальной среде на гипервизорах, так и на физической платформе. Решение состоит из нескольких модулей и включает в себя:

- RuSIEM — коммерческое решение класса SIEM;
- RvSIEM free — полнофункциональное свободно распространяемое готовое решение класса LM (log management);
- RuSIEM Analytics — модуль аналитики, работающий в режиме реального времени;
- RuSIEM Network Sensor — сетевой сенсор для анализа трафика.

RuSIEM имеет широкий набор визуализаций данных: дашборды, карта взаимосвязей, выборка по событиям, аналитика, отчеты, инциденты.

Инв. № подл.	Подпись и дата				Лист	
	Инв. № дубл.					
	Взам. инв. №					
	Подпись и дата					
<p>класса (включая систему контроля и управления доступом), автоматическое обнаружение инцидентов ит, иб и бизнес-процессов по правилам корреляции и с применением механизмов искусственного интеллекта.</p> <p>Развертывание решения возможно как в виртуальной среде на гипервизорах, так и на физической платформе. Решение состоит из нескольких модулей и включает в себя:</p> <ul style="list-style-type: none"><li>— RuSIEM — коммерческое решение класса SIEM;</li><li>— RvSIEM free — полнофункциональное свободно распространяемое готовое решение класса LM (log management);</li><li>— RuSIEM Analytics — модуль аналитики, работающий в режиме реального времени;</li><li>— RuSIEM Network Sensor — сетевой сенсор для анализа трафика.</li></ul> <p>RuSIEM имеет широкий набор визуализаций данных: дашборды, карта взаимосвязей, выборка по событиям, аналитика, отчеты, инциденты.</p>						
Изм.	Лист	№ докум.	Подпись	Дата	ФАЭС.10.05.02.056	48





- Управление событиями и данными;
- Управление инцидентами, уязвимостями, активами;
- Визуализация и аналитика;
- Методы кастомизации и разработки;
- Отказоустойчивость и резервирование;
- Техническая поддержка и обновления;
- Защищенность системы.

Сравнение выбранных SIEM-систем будет рассмотрено в таблице 3.1.

Таблица 3.1 - сравнение SIEM-систем

Критерий сравнения	RuSIEM	MaxPatrol SIEM
Общая информация		
Цена	от 500 тыс. руб.	от 3 млн. руб.
Обучение	Обучение бесплатное	Обучение проводится в офисе компании Positive Technologies, существуют специализированные вебинары
Язык интерфейса	Русский	Русский, Английский
Системная архитектура		
Операционная система в основе решения	Ubuntu x64	Windows, Debian
СУБД	Elasticsearch, RuS-IEM DB, postgresql, Click-House, neo4j	Elasticsearch
Распределенное развертывание компонентов	Да	Да

Подпись и дата	
Инв. № дубл.	
Взам. инв. №	
Подпись и дата	
Инв. № подл.	

Изм.	Лист	№ докум.	Подпись	Дата
------	------	----------	---------	------

ФАЭС.10.05.02.056

Лист

50

Продолжение таблицы 3.2

Возможность установки на сервер виртуализации ; Наличие сформированн ых образов для платформ виртуализации	Да VMWare, Hyper- V, KVM, QEMU	Да VMWare
Возможность хранения данных на внешних носителях (NAS/SAN )	Да	Да
Средняя степень сжатия при передаче сырых событий	Нет	До 7х
Ограничения по количеству обрабатываемы х событий в секунду	До 90к EPS событиями 300В на одну ноду, без лимита в распределенной инсталляции	15k EPS 30k EPS

Инв. № подл.	Подпись и дата
Взам. инв. №	Инв. № дубл.
Подпись и дата	
Инв. № подл.	

Изм.	Лист	№ докум.	Подпись	Дата
------	------	----------	---------	------

ФАЭС.10.05.02.056

Лист

51

Тип консоли администратора	Веб-консоль	Веб-консоль
----------------------------	-------------	-------------

Продолжение таблицы 3.2

Средняя степень сжатия при хранении нормализованных событий	До 0.7х оптимально без существенной потери производительности средствами Elastic Search	x5
Возможность развития системы за счет добавления дополнительных компонентов (параллельное масштабирование)	Да	Да

Подключение источников событий

Количество поддерживаемых источников событий	63 уникальных модели, 300+ разновидностей и версий	200+
Автообнаружение источников событий	Да	Да

Управление событиями и данными

Подпись и дата	Инва. № дубл.	Взам. инв. №	Подпись и дата	Инва. № подл.

Изм.	Лист	№ докум.	Подпись	Дата

ФАЭС.10.05.02.056

Агрегация событий по типу	Нет	Да
Нормализация событий	Да	Да

Продолжение таблицы 3.2

Метод сбора событий с источников	Агентский и безагентский	Агентский и безагентский
Основные поддерживаемые форматы сбора событий	Syslog, WMI, FTP, checkpoint lea, cisco sdee, file, ms sql, mysql, oracle, 1c, windows event log, hashlog	Syslog, Log File Protocol, SNMP, ODBC, WinRPC, OPSEC, FTP, smb, vSphere API, WMI
Возможность сохранения исходных событий (Log Management)	Да (встроенная функциональность)	Да. Не только на основе того, откуда пришел лог (пример с syslog), но и на основе данных в самих событиях
Управление инцидентами, уязвимостями, активами		
Карточка инцидента	372 настраиваемых полей	18 полей
Пути эскалации инцидента	Эскалация вручную с возможностью изменения критичности, темы и описания	Автоматическая маршрутизация инцидента при наличии условий (сработавшего правила, критичности инцидента, критичности активов, свойств активов)

Подпись и дата	
Инв. № дубл.	
Взам. инв. №	
Подпись и дата	
Инв. № подл.	

Изм.	Лист	№ докум.	Подпись	Дата
------	------	----------	---------	------

ФАЭС.10.05.02.056

Лист

53

Оповещение об инциденте (почта, мессенджеры, SMS, интеграции)	SMTP	SMTP, скрипты
---	------	---------------

Продолжение таблицы 3.2

Принятие решений в рамках процесса обработки инцидентов	Ручное	Ручное
Настройка собственной модели определения критичности	Да	CVSS уязвимости плюс критичность актива в формате CVSS 2.0
Сортировка уязвимостей по различным критериям — в т. ч. критичности	Да	Нет
Возможность выделения ложных срабатываний	В ручном режиме	В ручном режиме
Визуализация и аналитика		
Создание/изменение кастомизируемых панелей	Да	Да

Инв. № подл.	Подпись и дата
Взам. инв. №	Инв. № дубл.
Подпись и дата	

Изм.	Лист	№ докум.	Подпись	Дата
------	------	----------	---------	------

ФАЭС.10.05.02.056

Лист

54

Интерактивная работа с панелями (drill-down)	Да	Да
Возможность формирования отчетов в виде документов, форматы экспорта отчетов в виде документов	PDF, XLS, CSV	PDF, XLSX, MHT, DOCX, CSV

Продолжение таблицы 3.2

Формирование и рассылка отчетов по расписанию/по критерию	Формирование отчетов по активам, событиям, инцидентам, по расписанию	Формирование отчетов по активам, событиям, инцидентам, по расписанию
Объекты системы – методы кастомизации и разработки		
Возможности управления ИТ-активами	Только ручное удаление актива и изменение шаблона	Возможность автоматического поиска и создания
Изменение панели визуализации	Встроенный конструктор, фильтрация, drill-down	Встроенный конструктор, фильтрация, drill-down
Критерий сравнения	RuSIEM	MaxPatrol SIEM
Встроенный конструктор отчетов (показатели и графики)	Встроенный конструктор, фильтрация, сложные отчеты через аналитику, подсчет среднего,	Встроенного конструктора нет, фильтрация через генерацию отчета

Инва. № подл.	Подпись и дата
Взам. инв. №	Инва. № дубл.
Подпись и дата	
Инва. № подл.	

Изм.	Лист	№ докум.	Подпись	Дата
------	------	----------	---------	------

ФАЭС.10.05.02.056

Лист

55

	суммы, накопленной. Кастомизируется пользователем	
Варианты оповещения	Консоль, SMTP, API	Консоль, API
Управление правилами корреляции	Графический конструктор	Язык поисковых запросов
Возможность изменения и добавления категорий нормализации	Изменение парсеров в конфигурационных файлах	Встроенные категории, возможность создания собственных

Продолжение таблицы 3.2

Отказоустойчивость и резервирование		
Возможности по резервированию ядра системы	Пассивный, disaster recovery	Активный-пассивный
Возможности по резервированию компонентов сбора событий	Пассивный, disaster recovery	Активный-пассивный
Возможность сохранения событий локально на сборщике, если отсутствует связь с ядром	Да, с ротацией более старых в зависимости от свободного места на диске. MQ	Да

Подпись и дата	Продолжение таблицы 3.2				
	Отказоустойчивость и резервирование				
Инв. № докл.	Возможности по резервированию ядра системы	Пассивный, disaster recovery	Активный-пассивный		
	Возможности по резервированию компонентов сбора событий	Пассивный, disaster recovery	Активный-пассивный		
Взам. инв. №	Возможность сохранения событий локально на сборщике, если отсутствует связь с ядром	Да, с ротацией более старых в зависимости от свободного места на диске. MQ	Да		
Подпись и дата	ФАЭС.10.05.02.056				
Инв. № подл.	Изм.	Лист	№ докум.	Подпись	Дата







управление пользователями системы, включая создание учетных записей, назначение прав, блокирование и активацию учетных записей;  
журналирование действий пользователей.

4. PT MaxPatrol SIEM Server (MP SIEM Server) – компонент, который выполняет основные функции по обработке событий безопасности: агрегацию, фильтрацию, нормализацию и корреляцию событий; автоматическое создание инцидентов; привязку событий к активам.

5. PT MaxPatrol Agent (MP Agent) – компонент, осуществляющий сканирование активов системы и сбор событий.

Аппаратные требования к серверу компонентов MP Core, PT KB, PT MC, MP SIEM Server и MP Agent приведены в таблице 3.

Таблица 3.3 - аппаратные требования к серверу

Компонент сервера	Минимальные требования
Память (ОЗУ)	128 ГБ
Сетевой адаптер	4 порта со скоростью 1 Гбит/с каждый

Продолжение таблицы 3.3

Жесткие диски и свободное дисковое пространство	Файловая система жестких дисков — NTFS. Для работы ОС и установки компонентов PT MaxPatrol SIEM — RAID 1 (10 000 об./мин.), не менее 100 ГБ. Для БД компонентов PT MaxPatrol SIEM — RAID 10 (7200 об./мин.), не менее 1,2 ТБ. Для хранилища событий MP SIEM Server — RAID 10 (7200 об./мин., не менее 6 дисков), не менее 1,2 ТБ
---	--

Поддерживаемые операционные системы для mp core, pt mc, pt kb, mp siem server и mp agent:

- Microsoft Windows Server 2008 R2 SP1;
- Microsoft Windows Server 2012;

Инв. № подл.	Подпись и дата				Лист 59
	Инв. № дубл.				
	Взам. инв. №				
	Подпись и дата				
Изм.	Лист	№ докум.	Подпись	Дата	ФАЭС.10.05.02.056

— Microsoft Windows Server 2012 R2.

В соответствии со схемой сети компании, информации об используемых средствах защиты информации разработана схема развертывания pt maxpatrol siem в рамках исследуемой организации.

Рассмотрим ключевые аспекты, характерные для спроектированной схемы:

Установка компонентов mp core, pt mc, pt kb, mp siem server происходит на единый основной сервер, располагающийся в цод.

— Серверы компонента MP Agent располагаются в 6 разнесенных сегментах сети: демилитаризированной зоне, технологическом сегменте, центре обработки данных, главном офисе компании и филиалах.

— Управление компонентами основного сервера происходит с помощью Web-консоли управления.

— Сбор данных происходит со всех серверов средств защиты информации, представленных в пункте 3.3.

— Агенты MaxPatrol SIEM, размещенные в главном офисе и филиалах, производят сканирование узлов и сбор логов с журналов АРМ сотрудников, сетевого оборудования и межсетевых экранов.

— Агенты MaxPatrol SIEM, размещенные в ЦОД, производят сканирование узлов и сбор логов журналов серверов и баз данных информационно- биллинговой системы, офисных серверов, серверов средств защиты информации, сетевого оборудования, межсетевых экранов.

— Агенты MaxPatrol SIEM, DMZ-сегменте и технологическом сегменте, собирают информацию со специализированных серверов и оборудования.

Схема развертывания SIEM представлена на рисунке 3.3.

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата						
Изм.	Лист	№ докум.	Подпись	Дата	ФАЭС.10.05.02.056					Лист
										60

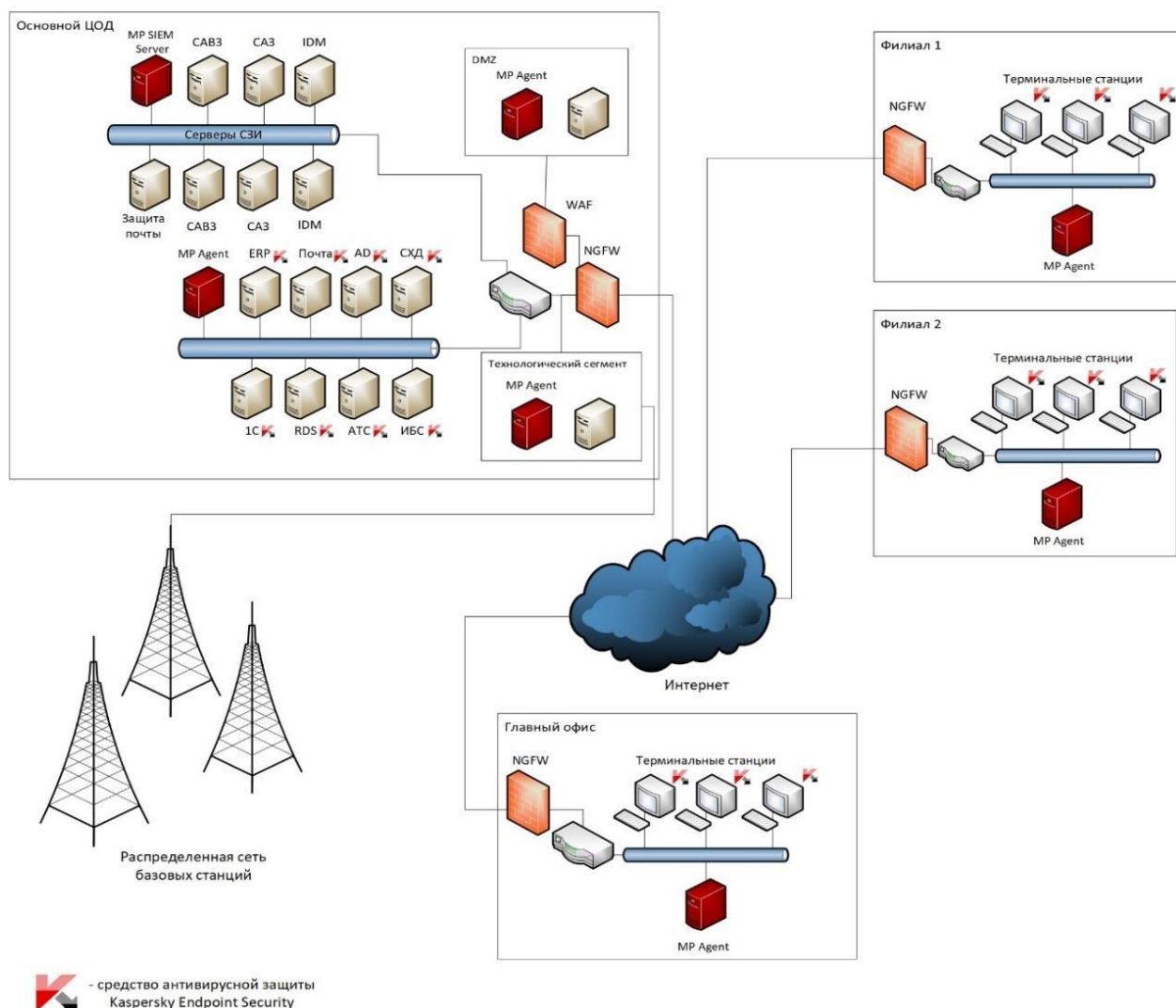


Рисунок 3.3 - Схема развертывания PT MaxPatrol SIEM.

### 3.6 Вывод

В данной главе была составлена информационно-технологическая инфраструктура рассматриваемой телекоммуникационной компании, проанализирован перечень актуальных угроз для компании. Далее был указан полный комплекс средств защиты информации.

Проведено сравнение двух наиболее популярных отечественных SIEM-решений. В результате сравнения по многим критериям, была выбрана система

MaxPatrol SIEM, как наиболее полностью удовлетворяющая потребностям телекоммуникационной компании в обеспечении информационной безопасности. В последней части третьей главы представлены этапы развертывания системы MaxPatrol SIEM.

Инв. № подл.	Подпись и дата				Инв. № дубл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата	
Изм.	Лист	№ докум.	Подпись	Дата	ФАЭС.10.05.02.056					Лист
										62

## Заключение

В результате выполнения дипломной работы была достигнута поставленная цель путем решения следующих задач:

- провести анализ компании;
- разработать модель нарушителя и проанализировать виды угрозы;
- спроектировать сайт и проверить его безопасность доступными средствами;
- анализ безопасности жизнедеятельности;
- технико-экономическое обоснование проекта.

При анализе компании были определены виды используемой информации и на основании каких законов эта информация должна храниться и обрабатываться. Разработка модели нарушителя и анализ видов угроз использовались при проектировании защищенного web-сайта. Было проведено сканирование сайта и выявленные уязвимости были закрыты.

Подпись и дата	Инв. № дубл.	Взам. инв. №	Подпись и дата	Инв. № подл.						Лист
										63
Изм.	Лист	№ докум.	Подпись	Дата	ФАЭС.10.05.02.056					

## 4 Безопасность жизнедеятельности

## 4.1 Постановка задачи

В данном разделе необходимо рассмотреть следующие вопросы:

- характеристика трудовой деятельности специалиста ИБ;
- влияние условий труда на здоровье пользователей ПК;
- профилактика зрительного утомления;
- экологические проблемы утилизации оборудования.

#### 4.2 Характеристика трудовой деятельности разработчиков сайта

Бесперебойное функционирование SIEM-системы является профстандартом 06.026: Администрирование информационно-коммуникационных (инфокоммуникационных) систем.

Основная цель вида профессиональной деятельности: Обеспечение требуемого качественного бесперебойного режима работы инфокоммуникационной системы.

Группа занятий:

- Специалисты в области техники, не входящие в другие группы (окз 2149);
- системные администраторы (окз 2522);
- инженеры по телекоммуникациям (окз 2153);
- специалисты-техники по компьютерным сетям и системам (окз 3513);
- специалисты по компьютерным сетям (окз 2153).

Таблица 4.2 Выполнение работ по выявлению и устранению инцидентов в информационно-коммуникационных системах



Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата

Трудовые действия	Выявление сбоев и отказов сетевых устройств и операционных систем
	Определение сбоев и отказов сетевых устройств и операционных систем
	Устранение последствий сбоев и отказов сетевых устройств и операционных систем
	Регистрация сообщений об ошибках в сетевых устройствах и операционных системах
	Обнаружение критических инцидентов при работе прикладного программного обеспечения
	Определение причин возникновения критических инцидентов при работе прикладного программного обеспечения
	Выполнение действий по устранению критических инцидентов при работе прикладного программного обеспечения в рамках должностных обязанностей
	Идентификация инцидентов при работе прикладного программного обеспечения
Необходимые умения	Идентифицировать инциденты, возникающие при установке программного обеспечения, и принимать решение об изменении процедуры установки
	Оценивать степень критичности инцидентов при работе прикладного программного обеспечения
	Устранять возникающие инциденты

Изм.	Лист	№ докум.	Подпись	Дата	ФАЭС.10.05.02.056	Лист 65

Продолжение таблицы 4.2

Необходимые умения	Локализовать отказ и инициировать корректирующие действия
	Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий
	Производить мониторинг администрируемой информационно-коммуникационной системы
	Конфигурировать операционные системы сетевых устройств
	Пользоваться контрольно-измерительными приборами и аппаратурой
	Документировать учетную информацию об использовании сетевых ресурсов согласно утвержденному графику
Необходимые знания	Лицензионные требования по настройке и эксплуатации устанавливаемого программного обеспечения
	Основы архитектуры, устройства и функционирования вычислительных систем
	Принципы организации, состав и схемы работы операционных систем
	Стандарты информационного взаимодействия систем
	Регламенты проведения профилактических работ на администрируемой информационно-коммуникационной системе
	Инструкции по установке администрируемых сетевых устройств

Инв. № подл.	Подпись и дата
Взам. инв. №	Инв. № дубл.
Подпись и дата	

Изм.	Лист	№ докум.	Подпись	Дата
------	------	----------	---------	------

ФАЭС.10.05.02.056

Продолжение таблицы 4.2

Необходимые знания	Инструкции по эксплуатации администрируемых сетевых устройств
	Инструкции по установке администрируемого программного обеспечения
	Инструкции по эксплуатации администрируемого программного обеспечения
	Требования охраны труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой информационно-коммуникационной системы

4.3 Влияние условий труда на здоровье пользователей ПК

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата	<p>4.3 Влияние условий труда на здоровье пользователей ПК</p>	<p>ФАЭС.10.05.02.056</p>	Лист
Изм.	Лист	№ докум.	Подпись	Дата			67

Условия труда, рабочее место и трудовой процесс в силу ст. 25 Федерального закона от 30.03.1999 № 52-ФЗ «О санитарно-эпидемиологическом благополучии населения» не должны оказывать вредное воздействие на работников. Требования к обеспечению безопасных для них условий труда устанавливаются санитарными правилами и иными нормативными правовыми актами Российской Федерации.

Юридические лица и индивидуальные предприниматели при этом обязаны осуществлять санитарно-противоэпидемические (профилактические) мероприятия по обеспечению безопасных для сотрудников условий труда и выполнению требований санитарных правил и иных нормативных правовых актов РФ, в частности к производственным процессам и технологическому оборудованию, организации рабочих мест в целях предупреждения травм, профессиональных заболеваний и заболеваний, связанных с условиями труда.

Условиями труда согласно ст. 209 ТК РФ является совокупность факторов производственной среды и трудового процесса, оказывающих влияние на работоспособность и здоровье работника. Вредным же производственным фактором в силу упомянутой ст. 209 ТК РФ признается фактор, воздействие которого на работника может привести к его заболеванию.

Постановлением Главного государственного санитарного врача РФ от 01.03.2021 утверждены Санитарно-эпидемиологические правила и нормативы СанПиН 1.2.3685-21 «Гигиенические нормативы и требования к обеспечению безопасности и (или) безвредности для человека факторов среды обитания» и СП 2.2.3670-20 "Санитарно-эпидемиологические требования к условиям труда».

Требования Санитарных правил в соответствии с их п. 1.3 направлены на предотвращение неблагоприятного воздействия на здоровье человека вредных факторов производственной среды и трудового процесса при работе с ПЭВМ.

При эксплуатации компьютера на работника могут оказывать влияние следующие опасные и вредные производственные факторы (п. 1.2 Типовой инструкции по охране труда при работе на персональном компьютере ТОИ Р-45-084-01, утв. Приказом Минсвязи России от 02.07.2001 № 162):

Инв. № подл.	Подпись и дата				Лист	
	Инв. № дубл.					
	Взам. инв. №					
	Подпись и дата					
Изм.	Лист	№ докум.	Подпись	Дата	ФАЭС.10.05.02.056	68

- повышенный уровень электромагнитных излучений;
- повышенный уровень статического электричества;
- пониженная ионизация воздуха;
- статические физические перегрузки;
- перенапряжение зрительных анализаторов.

При длительной работе за компьютером у работника могут возникать боли в позвоночнике, венозная недостаточность, потеря (или ухудшение) зрения из-за перенапряжения глаз, хронический стресс из-за необходимости постоянного принятия решений, от которых зависит эффективность работы.

Правильная же организация рабочего места (помещение, освещенность, микроклимат) может существенно сократить воздействие на здоровье работников вредных факторов и свести к минимуму вероятность возникновения заболевания, связанного с условиями труда.

#### 4.4 Профилактика зрительного утомления

При возникновении у работающих с ПЭВМ зрительного дискомфорта и других неблагоприятных субъективных ощущений, несмотря на соблюдение санитарно-гигиенических и эргономических требований, рекомендуется применять индивидуальный подход с ограничением времени работы с ПЭВМ.

В случаях, когда характер работы требует постоянного взаимодействия с ВДТ (набор текстов или ввод данных и т. п.) с напряжением внимания и сосредоточенности, при исключении возможности периодического переключения на другие виды трудовой деятельности, не связанные с ПЭВМ, рекомендуется организация перерывов на 10 — 15 мин через каждые 45 — 60 мин работы.

Продолжительность непрерывной работы с ВДТ без регламентированного перерыва не должна превышать 1 ч. Снижение зрительного переутомления достигается реализацией следующих рекомендаций:

Инв. № подл.	Подпись и дата				Лист 69
	Инв. № дубл.				
	Взам. инв. №				
	Подпись и дата				
Изм.	Лист	№ докум.	Подпись	Дата	ФАЭС.10.05.02.056

1) устранить пульсации освещенности рабочего места, постоянную смену полей зрения, резкие световые и цветовые контрасты, сильную освещенность, слепящие поверхности;

2) при работе с дисплеями необходимо регламентировать яркость фоновое свечения экрана, яркость и контрастность изображения на экране, цвет свечения экрана и высвечивания информации, частоту мельканий изображений, ширину линий. По своему усмотрению операторы должны иметь возможность изменять наклон корпуса, высоту пульта с клавиатурой, высоту экрана, расстояние от экрана до глаз, наклон экрана;

3) с целью предотвращения развития перенапряжения органов зрения необходимо соблюдать правильный режим труда и отдыха, включающий распорядок и продолжительность рабочего дня, введение регламентированных перерывов в работе, сеансов релаксации, выполнение упражнений для глаз соблюдение рекомендаций по организации активного отдыха;

4) проведение окулистами отбора лиц на работу, требующую напряжения органов зрения.

Комплексы упражнений для глаз.

Упражнения выполняются сидя или стоя, отвернувшись от экрана при ритмичном дыхании, с максимальной амплитудой движения глаз. Способ снятия напряжения с глаз предложенный в СанПиНе: [25]

1. Закрывать глаза, сильно напрягая глазные мышцы, на счет 1-4, затем раскрыть глаза, расслабив мышцы глаз, посмотреть вдаль на счет 1—6. Повторить 4-5 раз.

2. Посмотреть на переносицу и задержать взор на счет 1—4. До усталости глаза не доводить. Затем открыть глаза, посмотреть вдаль на счет 1-6. Повторить 4-5 раз.

3. Не поворачивая головы, посмотреть направо и зафиксировать взгляд на счет 1-4, затем посмотреть вдаль прямо на счет 1-6. Аналогичным образом проводятся упражнения, но с фиксацией взгляда влево, вверх и вниз. Повторить 3-4 раза.

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата	<p>ФАЭС.10.05.02.056</p>	Лист
Изм.	Лист	№ докум.	Подпись	Дата	70	

4. Перенести взгляд быстро по диагонали: направо вверх – налево вниз, потом прямо вдаль на счет 1-6; затем налево вверх направо вниз и посмотреть вдаль на счет 1-6. Повторить 4-5 раз.

#### 4.5 Экологические проблемы утилизации оборудования

Устаревшие персональные компьютеры или их элементы должны быть правильно утилизированы в целях предотвращения вредного воздействия отходов производства и потребления на здоровье человека и окружающую среду, а также вовлечения таких отходов в хозяйственный оборот в качестве дополнительных источников сырья. За несоблюдение законодательства России по утилизации офисной техники на организацию могут быть наложены штрафные санкции.

Выбрасывание компьютерной техники ведет к загрязнению окружающей среды. Персональный компьютер включает в свой состав как органические составляющие (пластик различных видов, материалы на основе поливинилхлорида, фенолформальдегида), так и почти полный набор металлов, в том числе и драгоценных. В связи с этим организации требуется документально контролировать оборот средств компьютерной техники от поступления до выбытия.

Согласно Приказу ГТК РФ от 19.11.2002 N 1224 «О порядке учета и хранения изделий и материалов, изготовленных с применением драгоценных металлов и драгоценных камней», организация вправе:

- самостоятельно обрабатывать (перерабатывать) собранный лом, содержащий драгоценные металлы;
- реализовывать лом, содержащий драгоценные металлы;
- передавать на давальческой основе аффинажным организациям или организациям, осуществляющим деятельность по заготовке лома и отходов, первичной обработке и переработке, для дальнейшего производства и аффинажа.

Процесс утилизации компьютерной техники включает следующие пункты:

Инв. № подл.	Подпись и дата				Лист 71
	Инв. № дубл.				
	Взам. инв. №				
	Подпись и дата				
Изм.	Лист	№ докум.	Подпись	Дата	ФАЭС.10.05.02.056

- создание внутренней комиссии в организации, которая решит, что нужно списать;
- составление экспертного заключения и подтверждение невозможности дальше пользоваться компьютерным оборудованием;
- осуществление списания компьютерной техники, которое будет отражено в бухгалтерском учете;
- утилизация мусора на лицензированном предприятии и получение документального подтверждения о проведенных действиях (акт выполненной работы, приема-передачи). Утилизация персональных компьютеров имеет определенные сложности в реализации, но это необходимый этап в поддержании экологической ситуации.

#### 4.6 Вывод

В данном разделе были рассмотрены вопросы характеристики трудовой деятельности специалиста ИБ, влияние условий труда на здоровье пользователей ПК, профилактика зрительного утомления, экологические проблемы утилизации оборудования.

#### 5 Техничко-экономическое обоснование работы

##### 5.1 Постановка задачи

Целью выпускной квалификационной работы являлась Исследование и организация процесса мониторинга событий информационной безопасности.

SIEM-система является программным продуктом, который, согласно ст. 1259 ГК РФ, относится к объектам авторских прав, таким образом, является интеллектуальной собственностью.

В данном разделе будут рассмотрены следующие вопросы:

- расчет трудоемкости и длительности работ;
- расчет себестоимости и цены программного продукта.

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата	ФАЭС.10.05.02.056	Лист
Изм.	Лист	№ докум.	Подпись	Дата	72	





Результаты расчета средней оценки затрат времени на разработку программного продукта приведены в таблице 5.1.

Таблица 5.1 – Время, затраченное на разработку программного продукта

Этапы разработки программного продукта	Наименее возможная величина затрат ( $a_i$ ), дни			Наиболее вероятная величина затрат ( $m_i$ ), дни			Наиболее возможная величина затрат ( $b_i$ ), дни		
	$T_{авт}$	$T_{рук}$	$\bar{T}$	$T_{авт}$	$T_{рук}$	$\bar{T}$	$T_{авт}$	$T_{рук}$	$\bar{T}$
1. Построение структурной схемы информационно технической инфраструктуры компании и анализ сегментов сети	4	3	3,6	6	5	5,6	7	6	6,6
2. Составление перечня и анализ актуальных угроз компании	5	4	4,6	6	5	5,6	7	6	6,6
3. Сбор и анализ информации об имеющихся средствах защиты информации в компании	3	2	2,4	4	2	2,8	6	4	4,8
4. Анализ рынка SIEM-решений и выбор подходящей системы	2	1	1,4	3	2	2,4	5	4	4,4
5. Проектирование и развертывание SIEM-системы	15	12	13,2	18	16	16,8	21	20	20,4

На основе средних оценок рассчитываются математическое ожидание и отклонение по каждому этапу разработки программного продукта. Формула расчета математического ожидания для  $i$ -го этапа:

Инов. № подл.	Подпись и дата
Взам. инв. №	Инов. № дубл.
Подпись и дата	
Инов. № подл.	

Изм.	Лист	№ докум.	Подпись	Дата
------	------	----------	---------	------

ФАЭС.10.05.02.056

Лист

74

$$MO_i = \frac{a_i + 4m_i + b_i}{6}, \quad (5.2)$$

где  $MO_i$  – математическое ожидание для  $i$ -го этапа;

$a_i, m_i, b_i$  – средние значения.

Стандартное отклонение для каждого этапа разработки программного продукта определяется по формуле:

$$G_i = \frac{b_i - a_i}{6}, \quad (5.3)$$

где  $G_i$  – стандартное отклонение по  $i$ -му этапу.

Зная математическое ожидание по каждому этапу, рассчитываем общую величину математического ожидания в целом по программному продукту:

$$MO = \sum MO_i, \quad (5.4)$$

где  $MO$  – общая величина математического ожидания.

Стандартное отклонение G в целом по программному продукту рассчитывается по следующей формуле:

$$G = \sqrt{\sum G_i^2}, \quad (5.5)$$

где  $G$  – стандартное отклонение;

$G_i$  – стандартное отклонение по i-му этапу.

На основе расчетов математического ожидания (5.4) и стандартного отклонения (5.5) рассчитываем коэффициент вариации – коэффициент согласованности мнения экспертов. Коэффициент вариации рассчитывается по формуле:

$$v_i = \frac{G_i}{MO_i}, \quad (5.6)$$

Подпись и дата	<p>Стандартное отклонение <math>G</math> в целом по программному продукту рассчитывается по следующей формуле:</p> $G = \sqrt{\sum G_i^2}, \tag{5.5}$ <p>где <math>G</math> –стандартное отклонение;</p> <p><math>G_i</math> – стандартное отклонение по i-му этапу.</p> <p>На основе расчетов математического ожидания (5.4) и стандартного отклонения (5.5) рассчитываем коэффициент вариации – коэффициент согласованности мнения экспертов. Коэффициент вариации рассчитывается по формуле:</p> $v_i = \frac{G_i}{MO_i}, \tag{5.6}$					
Инв. № докл.	<div>ФАЭС.10.05.02.056</div>					Лист
Взам. инв. №						75
Подпись и дата						
Инв. № подл.						
Изм.						Лис

где  $v_i$  – коэффициент вариации по i-му этапу.

Все произведенные расчеты сведены в таблицу 5.2.

Таблица 5.3 – Затраты на разработку программного продукта

Этапы разработки программного продукта	Средняя величина затрат по этапам, дни			Матем. ожидание (МО <sub>i</sub> , дни)	Станд. отклонение (G <sub>i</sub> , дни)	Коэффициент вариации (v <sub>i</sub> )
	Наименее возможная величина затрат (a <sub>i</sub> , дни)	Наиболее вероятная величина затрат (m <sub>i</sub> , дни)	Наиболее возможная величина затрат (b <sub>i</sub> , дни)			
1. Построение структурной схемы информационно-технической инфраструктуры компании и анализ сегментов сети	3,6	5,6	6,6	5,43	0,50	0,092
2. Составление перечня и анализ актуальных угроз компании	4,6	5,6	6,6	5,6	0,33	0,059
3 Сбор и анализ информации об имеющихся средствах защиты информации в компании.	2,4	2,8	4,8	3,07	0,40	0,130
4. Анализ рынка SIEM-решений и выбор подходящей системы	1,4	2,4	4,4	2,57	0,50	0,195
5. Проектирование и развертывание SIEM-системы	13,2	16,8	20,4	16,80	1,20	0,071
Итого	21,6	33,2	42,8	33,47	1,47	0,044

Инв. № подл.	Подпись и дата
Взам. инв. №	Инв. № дубл.
Подпись и дата	
Инв. № подл.	

Изм.	Лист	№ докум.	Подпись	Дата
------	------	----------	---------	------

ФАЭС.10.05.02.056

Лист

76

В итоге коэффициент вариации равен 0,044 и не превосходит 0,33. Поэтому мнения экспертов считаются согласованными.

### 5.3 Расчет себестоимости и цены программного продукта

Себестоимость программного продукта – это все виды затрат, понесенные при разработке продукта. Чтобы определить себестоимость разработки применяется метод экспертных оценок.

Себестоимость программного продукта определяется по формуле (5.7):

$$C = \frac{3}{m} \cdot k \cdot k_{TEP} \cdot k_{IP} \cdot (t_1 + t_2) \cdot (1 + k_H) + 8 \cdot t_3 \cdot C_M + 8 \cdot t_4 \cdot C_{II}, \quad (5.7)$$

где 3 – среднемесячная заработная плата рhr-разработчика, 3 = 30000;

$k_{TEP}$  – территориальный коэффициент,  $k_{TEP} = 1,2$  (для НСО);

$k_{IP}$  – коэффициент премии,  $k_{IP} = 1$ ;

$k$  – коэффициент, учитывающий страховые взносы (фонды пенсионного, социального и медицинского страхования),  $k = 1,3$ ;

$m$  – количество рабочих дней в месяце,  $m = 22$ ;

$k_H$  – коэффициент, учитывающий накладные расходы (отопление, освещение, уборка и т. д.),  $k_H = 0,4$ ;

$t_1$  – время, затраченное разработчиком на разработку требований к программе, т.е. подготовительное время, которое необходимо потратить, чтобы приступить к написанию программы и отладки программы, чел./дни;

$t_2$  – сборка устройства, составление алгоритма в программе, время, затраченное на написание и отладку программы, чел./дни;

$t_3$  – время, затраченное на разработку программы с использованием машинного времени, чел./дни;

$t_4$  – время работы в сети интернет, дни;

$C_{II}$  – стоимость 1 часа работы в сети интернет, руб. (оценивается через абонентскую плату);

$C_M$  – стоимость одного часа машинного времени.

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата	<div style="text-align: center; font-size: 1.2em; font-weight: bold;">ФАЭС.10.05.02.056</div>	Лист 77
Изм.	Лис	№ докум.	Подпись	Дата		

$$C_M = \frac{3_{эл} + 3_a + 3_{компл} + 3_{пр}}{T_{обш}}. \quad (5.8)$$
$$T_{обм} = 22 * 12 * 8 = 2112 \text{ (часов)}$$
$$\mathcal{Z}_{\mathfrak{A}l} = T_{obu} * C_{\mathfrak{A}l} * P, \quad (5.9)$$

По (5.9) затраты на электроэнергию за год работы составляют:

$$3_{37} = 2112 * 2,68 * 0,500 = 2830,1 \text{ (pyб.)}$$

$$3_q = C * \Pi_p, \quad (5.10)$$

$\Pi_p$  – процент отчисления на амортизацию,  $\Pi_p = 40\%$ .

$$3_a = 72000 * 0,4 = 28800 \text{ (руб.)}$$
$$Z_{\text{компл}} = 3000 \text{ (руб.)}$$

					ФАЭС.10.05.02.056	Лист
						78
Изм.	Лист	№ докум.	Подпись	Дата		

$$З_{np} = \frac{0,05 * (З_{эл} + З_a + З_{компл})}{0,95}. \quad (5.11)$$

По (5.11) прочие расходы равны:

$$З_{np} = \frac{0,05 * (2830,1 + 28800 + 3000)}{0,95} = 1822,63 \text{ (руб.)}$$

По формуле 5.8 стоимость одного часа машинного времени равна:

$$C_m = \frac{2830,1 + 28800 + 3000 + 1822,63}{2112} = 17,26 \text{ (руб.)}$$

Тариф на услугу интернет составляет 990 руб. в месяц, следовательно, стоимость 1 дня работы в сети интернет равен:

$$C_{и} = \frac{990}{30} = 33 \text{ (руб.)}$$

Заключительным этапом расчета является распределение ранее рассчитанной трудоемкости (таблица 5.3) по 4 направлениям:

–  $t_1$  включает первые три этапа:

$$t_1 = 5,43 + 5,6 + 3,07 = 14,1 \text{ (дней)}$$

–  $t_2$  включает оставшиеся этапы:

$$t_2 = 16,80 + 2,57 = 19,37 \text{ (дней)}$$

–  $t_3$  включает время работы ПК для разработки программы:

$$t_3 = 55 \text{ (дней)}$$

–  $t_4$  включает время использования интернета для разработки программы:

$$t_4 = 50 \text{ (дней)}$$

Наконец, итоговая себестоимость программного продукта составляет:

$$C = \frac{30000}{22} \cdot 1,3 \cdot 1,2 \cdot 1 \cdot (14,1 + 19,37) \cdot (1 + 0,4) + 8 \cdot 55 \cdot 17,26 + 8 \cdot 50 \cdot 33 = 120474,02 \text{ (руб.)}$$

В случае, если программный продукт будет доработан и реализован на рынке, следует рассчитать цену по следующей формуле:

$$Ц = C * \left(1 + \frac{P}{100}\right), \quad (5.12)$$

где  $C$  – себестоимость разработки программы, руб;

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата					Лист 79
Изм.	Лист	№ докум.	Подпись	Дата	ФАЭС.10.05.02.056				

$P$  – рентабельность, руб.

Определим цену программного продукта, при условии, что значение рентабельности равно 20%:

$$Ц = 154097,5 \cdot \left(1 + \frac{20}{100}\right) = 144568,8 \text{ (руб.)}$$

Цена с учетом налога на добавленную стоимость находится по формуле:

$$Ц_{НДС} = Ц * K_{НДС}, \quad (5.13)$$

где  $Ц$  – цена программного продукта;

$K_{НДС}$  – коэффициент, учитывающий ставку налога на добавленную стоимость (НДС),  $K_{НДС} = 1,20$ . [24]

Цена с учетом налога на добавленную стоимость составит:

$$Ц_{НДС} = 144568,8 * 1,20 = 173482,6 \text{ (руб.)}$$

#### 5.4 Выводы по разделу

В данном разделе была определены и рассчитаны трудоемкость и длительность работ, а также рассчитаны себестоимость и цена программного продукта.

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата	ФАЭС.10.05.02.056					Лист
										80
Изм.	Лист	№ докум.	Подпись	Дата						



## Заключение

В результате выполнения дипломной работы была достигнута поставленная цель путем решения следующих задач:

- рассмотреть основные подходы в организации мониторинга инцидентов ИБ ;
- провести анализ программно-технической части мониторинга инцидентов ИБ;
- выполнить внедрение системы мониторинга ИБ для телекоммуникационной компании;
- анализ безопасности жизнедеятельности;
- технико-экономическое обоснование проекта.

В данной работе рассмотрены основные принципы организации процесса мониторинга инцидентов информационной безопасности и проработан процесс реализации и внедрения программно-технической части мониторинга инцидентов в систему информационной безопасности телекоммуникационной компании.

В процессе изучения теоретического материала, нормативно-правовой документации по вопросам исследуемой области проведено подразделение процесса внедрения системы мониторинга инцидентов информационной безопасности на две составляющие: организационную и программно-техническую, рассмотрены средства реализации каждой из этих частей.

Практическая часть работы включает в себя аналитическую работу по внедрению программно-технического средства мониторинга инцидентов информационной безопасности – SIEM-системы в инфраструктуру телекоммуникационной компании, а именно изучение информационно-технологической инфраструктуры компании, выбор SIEM-решения на основе сравнительного анализа двух российских SIEM по разработанным критериям, проектирование примерной схемы развертывания системы мониторинга в рамках конкретной телекоммуникационной компании.

Изм.	Лист	№ докум.	Подпись	Дата	Изм. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата	<p>реализации. При внедрении программно-технической части мониторинга инцидентов в систему информационной безопасности телекоммуникационной компании.</p> <p>В процессе изучения теоретического материала, нормативно-правовой документации по вопросам исследуемой области проведено подразделение процесса внедрения системы мониторинга инцидентов информационной безопасности на две составляющие: организационную и программно-техническую, рассмотрены средства реализации каждой из этих частей.</p> <p>Практическая часть работы включает в себя аналитическую работу по внедрению программно-технического средства мониторинга инцидентов информационной безопасности – siem-системы в инфраструктуру телекоммуникационной компании, а именно изучение информационно-технологической инфраструктуры компании, выбор SIEM-решения на основе сравнительного анализа двух российских SIEM по разработанным критериям, проектирование примерной схемы развертывания системы мониторинга в рамках конкретной телекоммуникационной компании.</p>	Лист

## Список литературы

2 ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. – Введ. 01.02.2008. М.: Госстандарт России. 2008. - 31 с.

3 ГОСТ Р ИСО/МЭК ТО 18044-2007. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. – Введ. 01.07.2008. М.: Стандартинформ, 2008. – 62 с.

4 ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. – Введ. 01.10.2009. М.: Стандартинформ, 2009. – 16 с.

5 Cisco Systems. Построение центра мониторинга и управления безопасностью Cisco. Архитектура, процессы и результаты.

6 Обзор предпосылок для создания SOC [Электронный ресурс] – 2017.

7 Сравнение услуг коммерческих SOC (Security Operations Center).

Часть 1 [Электронный ресурс] – 2019. – Режим доступа: <https://www.anti-malware.ru/compare/SOC-Security-Operations-Center>

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата
<p>информационной безопасности в организации. Основные термины и определения. – Введ. 01.10.2009. М.: Стандартиформ, 2009. – 16 с.</p> <p>5 Cisco Systems. Построение центра мониторинга и управления безопасностью Cisco. Архитектура, процессы и результаты.</p> <p>6 Обзор предпосылок для создания SOC [Электронный ресурс] – 2017.</p> <p>7 Сравнение услуг коммерческих SOC (Security Operations Center).          Часть 1 [Электронный ресурс] – 2019. – Режим доступа: <a href="https://www.anti-malware.ru/compare/SOC-Security-Operations-Center">https://www.anti-malware.ru/compare/SOC-Security-Operations-Center</a></p>				
Изм.	Лист	№ докум.	Подпись	Дата
ФАЭС.10.05.02.056				Лист
				82

Приложение А Актуальные угрозы для персональных данных клиентов и коммерческой тайны исследуемой компании

- Общая информация;
- Угроза воздействия на программы с высокими привилегиями;
- Угроза восстановления аутентификационной информации;
- Угроза выхода процесса за пределы виртуальной машины;
- Угроза доступа к защищаемым файлам с использованием обходного пути;
- Угроза деструктивного изменения конфигурации/среды окружения программ;
- Угроза загрузки нештатной операционной системы;
- Угроза заражения DNS-кеша;
- Угроза изменения компонентов системы;
- Угроза изменения системных и глобальных переменных;
- Угроза искажения вводимой и выводимой на периферийные устройства информации;
- Угроза использования альтернативных путей доступа к ресурсам (только для ПДн);
- Угроза использования информации идентификации/аутентификации, заданной по умолчанию;
- Угроза использования механизмов авторизации для повышения привилегий;
- Угроза использования слабостей кодирования входных данных;
- Угроза исследования механизмов работы программы;
- Угроза нарушения изоляции пользовательских данных внутри виртуальной машины;
- Угроза нарушения технологии обработки информации путём несанкционированного внесения изменений в образы виртуальных машин;

Инв. № подл.	Подпись и дата					Лист
	Инв. № дубл.					
	Взам. инв. №					
	Подпись и дата					
<div>— Угроза искажения вводимой и выводимой на периферийные устройства информации;</div> <div>— Угроза использования альтернативных путей доступа к ресурсам (только для ПДн);</div> <div>— Угроза использования информации идентификации/аутентификации, заданной по умолчанию;</div> <div>— Угроза использования механизмов авторизации для повышения привилегий;</div> <div>— Угроза использования слабостей кодирования входных данных;</div> <div>— Угроза исследования механизмов работы программы;</div> <div>— Угроза нарушения изоляции пользовательских данных внутри виртуальной машины;</div> <div>— Угроза нарушения технологии обработки информации путём несанкционированного внесения изменений в образы виртуальных машин;</div>						
					ФАЭС.10.05.02.056	83
Изм.	Лист	№ докум.	Подпись	Дата		

- Угроза невозможности миграции образов виртуальных машин из-за несовместимости аппаратного и программного обеспечения;
- Угроза неконтролируемого роста числа виртуальных машин;
- Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов;
- Угроза некорректного задания структуры данных транзакции;
- Угроза некорректного использования функционала программного и аппаратного обеспечения;
- Угроза неправомерного ознакомления с защищаемой информацией;
- Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением;
- Угроза неправомерных действий в каналах связи;
- Угроза несанкционированного восстановления удалённой защищаемой информации;
- Угроза несанкционированного доступа к аутентификационной информации;
- Угроза несанкционированного доступа к виртуальным каналам передачи;
- Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети;
- Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение;
- Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети;
- Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин;
- Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети;

Инв. № подл.	Подпись и дата				Инв. № довл.	Подпись и дата				Взам. инв. №	Подпись и дата				Инв. № подл.	Подпись и дата				Изм.	Лист	№ докум.	Подпись	Дата	Лист			
<div style="text-align: right; font-size: 1.2em; font-weight: bold;">ФАЭС.10.05.02.056</div>																												84

- Угроза несанкционированного доступа к системе по беспроводным каналам;
- Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети;
- Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации;
- Угроза несанкционированного изменения аутентификационной информации;
- Угроза несанкционированного копирования защищаемой информации;
- Угроза несанкционированного редактирования реестра;
- Угроза несанкционированного удаления защищаемой информации;
- Угроза несанкционированного управления буфером;
- Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб;
- Угроза обнаружения хостов;
- Угроза обхода некорректно настроенных механизмов аутентификации;
- Угроза опосредованного управления группой программ через совместно используемые данные;
- Угроза ошибки обновления гипервизора;
- Угроза перебора всех настроек и параметров приложения;
- Угроза передачи данных по скрытым каналам;
- Угроза перезагрузки аппаратных программно-аппаратных средств вычислительной техники;
- Угроза переполнения целочисленных переменных (только для ПДн);
- Угроза перехвата данных, передаваемых по вычислительной сети;
- Угроза перехвата привилегированного потока;
- Угроза перехвата привилегированного процесса;
- Угроза перехвата управления гипервизором;

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата	
Изм.	Лист	№ докум.	Подпись	Дата	ФАЭС.10.05.02.056
					85



- Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет;
- Угроза использования уязвимых версий программного обеспечения;
- Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика;
- Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы;
- Угроза скрытной регистрации вредоносной программой учетных записей администраторов;
- Угроза несанкционированного доступа к параметрам настройки оборудования за счет использования «мастер-кодов» (инженерных паролей);
- Угроза нарушения работы информационной системы, вызванного обновлением используемого в ней программного обеспечения;
- Угроза использования непроверенных пользовательских данных при формировании конфигурационного файла, используемого программным обеспечением администрирования информационных систем;
- Угроза перехвата управления информационной системой.

Приложение Б Актуальные угрозы, направление на нарушение возможности доступа клиентов к веб-ресурсам компании

- Угроза воздействия на программы с высокими привилегиями;
- Угроза деструктивного изменения конфигурации/среды окружения программ;
- Угроза длительного удержания вычислительных ресурсов пользователями;
- Угроза доступа к локальным файлам сервера при помощи;
- Угроза избыточного выделения оперативной памяти;
- Угроза использования альтернативных путей доступа к ресурсам;
- Угроза использования информации идентификации/аутентификации, заданной по умолчанию;
- Угроза использования механизмов авторизации для повышения привилегий;
- Угроза использования слабостей кодирования входных данных;
- Угроза исследования механизмов работы программы;
- Угроза исследования приложения через отчёты об ошибках;
- Угроза межсайтового скриптинга;
- Угроза межсайтовой подделки запроса;
- Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением;
- Угроза несанкционированного удаления защищаемой информации;
- Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб;
- Угроза обнаружения хостов;
- Угроза перезагрузки аппаратных программно-аппаратных средств вычислительной техники;
- Угроза преодоления физической защиты;
- Угроза приведения системы в состояние «отказ в обслуживании»;

Инв. № подл.	Подпись и дата				Лист	
	Инв. № дубл.					
	Взам. инв. №					
	Подпись и дата					
Изм.	Лист	№ докум.	Подпись	Дата	ФАЭС.10.05.02.056	88

—	Угроза использования слабостей кодирования входных данных;
—	Угроза исследования механизмов работы программы;
—	Угроза исследования приложения через отчёты об ошибках;
—	Угроза межсайтового скриптинга;
—	Угроза межсайтовой подделки запроса;
—	Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением;
—	Угроза несанкционированного удаления защищаемой информации;
—	Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб;
—	Угроза обнаружения хостов;
—	Угроза перезагрузки аппаратных программно-аппаратных средств вычислительной техники;
—	Угроза преодоления физической защиты;
—	Угроза приведения системы в состояние «отказ в обслуживании»;



- Угроза физического вывода из строя средств хранения, обработки и (или) ввода/вывода/передачи информации;
- Угроза включения в проект не достоверно испытанных компонентов;
- Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы;
- Угроза скрытной регистрации вредоносной программой учетных записей администраторов;
- Угроза нарушения работы информационной системы, вызванного обновлением используемого в ней программного обеспечения;
- Угроза использования непроверенных пользовательских данных при формировании конфигурационного файла, используемого программным обеспечением администрирования информационных систем;
- Угроза перехвата управления информационной системой.

Инв. № подл.	Подпись и дата				Инв. № дубл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата	
Изм.	Лист	№ докум.	Подпись	Дата	ФАЭС.10.05.02.056					Лист
										89

Приложение В Актуальные угрозы, направление на нарушение функционирования систем, обеспечивающих предоставления услуг связи абонентам компании

- Угроза воздействия на программы с высокими привилегиям;
- Угроза спользования информации идентификации/аутентификации, заданной по умолчанию;
- Угроза использования механизмов авторизации для повышения привилегий;
- Угроза использования слабостей кодирования входных данных;
- Угроза исследования механизмов работы программы;
- Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением;
- Угроза несанкционированного доступа к системе по беспроводным каналам;
- Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб;
- Угроза обнаружения хостов;
- Угроза перезагрузки аппаратных программно-аппаратных средств вычислительной техники;
- Угроза преодоления физической защиты;
- Угроза приведения системы в состояние «отказ в обслуживании»;
- Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации;
- Угроза включения в проект не достоверно испытанных компонентов;
- Угроза использования уязвимых версий программного обеспечения;
- Угроза скрытной регистрации вредоносной программой учетных записей администраторов;
- Угроза нарушения работы информационной системы, вызванного обновлением используемого в ней программного обеспечения;

Инв. № подл.	Подпись и дата				Лист	
	Инв. № дубл.					
	Взам. инв. №					
	Подпись и дата					
Изм.	Лист	№ докум.	Подпись	Дата	ФАЭС.10.05.02.056	90

—	Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб;
—	Угроза обнаружения хостов;
—	Угроза перезагрузки аппаратных программно-аппаратных средств вычислительной техники;
—	Угроза преодоления физической защиты;
—	Угроза приведения системы в состояние «отказ в обслуживании»;
—	Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации;
—	Угроза включения в проект не достоверно испытанных компонентов;
—	Угроза использования уязвимых версий программного обеспечения;
—	Угроза скрытной регистрации вредоносной программой учетных записей администраторов;
—	Угроза нарушения работы информационной системы, вызванного обновлением используемого в ней программного обеспечения;

- Угроза использования непроверенных пользовательских данных при формировании конфигурационного файла, используемого программным обеспечением администрирования информационных систем;
- Угроза перехвата управления информационной системой.

Инв. № подл.	Подпись и дата				Инв. № дубл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата	
Изм.	Лист	№ докум.	Подпись	Дата	ФАЭС.10.05.02.056					Лист
										91