МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»

Институт математики, физики и информационных технологий
(наименование института полностью)

Кафедра Прикладная математика и информатика
(наименование)

09.04.03 Прикладная информатика
(код и наименование направления подготовки)

Информационные системы и технологии корпоративного управления
(направленность (профиль))

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ)

на тему «Исследование технологии построения информационной системы внутреннего аудита информационной безопасности в транспортной компании»

Студент В.С. Демочкин _____
(И.О. Фамилия) (личная подпись)

Научный
руководитель к.т.н., доцент, А.Б. Кузьмичев
(ученая степень, звание, И.О. Фамилия)

Тольятти 2021

Оглавление

Введение 4

Глава 1 Анализ внутреннего аудита информационной безопасности ТОО «KARCHER» 7

1.1 Анализ задач и структуры ТОО «KARCHER» 7

1.2 Анализ и технологии проведения внутреннего аудита информационной безопасности ТОО «KARCHER» 14

1.3 Анализ угроз информационной безопасности ТОО «KARCHER», требующие решения 20

Глава 2 Пути решения выявленных угроз информационной безопасности 26

2.1 Анализ путей решения выявлен угроз информационной безопасности в функционировании ТОО «KARCHER» 26

2.2 Возможности системы SIEM для аудита информационной безопасности организации 32

2.3 Интеграция внутреннего аудита информационной безопасности в систему программного обеспечения компании 42

Глава 3 Реализация разработанной технологии внутреннего аудита информационной безопасности компании ТОО «KARCHER» 45

3.1 Характеристика общей структуры системы аудита информационной безопасности 45

3.2 Алгоритмы работы модулей корреляции и прогнозирования 46

3.3 Корреляция общей структуры системы аудита информационной безопасности 50

Глава 4 Тестирование разработанной технологии внутреннего аудита информационной безопасности компании ТОО «KARCHER» и анализ результатов тестирования 58

4.1 Этапы работы SIEM системы 58

4.2 Имитационное моделирование обнаружения атак 60

4.3 Имитационное моделирование построения вектора уже обнаруженных атак 63

4.4 Оценка эффективности SIEM-системы 65

Заключение 67

Список используемых источников 69
Приложение А Статистика роста целевых атак 73
Приложение Б Блок-схема алгоритма работы программы 74

Введение

Информационная безопасность компании, общественной организации или производственного предприятия – это комплекс мероприятий, направленных на предотвращение несанкционированного доступа к внутренней IT-инфраструктуре, незаконного завладения конфиденциальной информацией и внесения изменений в базы данных.

Учитывая важность информации в современном мире, защите от утечек конфиденциальной информации в адрес конкурентов необходимо уделять повышенное внимание. Возможный ущерб может быть намного большим, чем стоимость всех материальных активов предприятия.

Внутренний аудит можно рассматривать как регламентированную внутренними документами компании деятельность по контролированию системы управления и различных аспектов функционирования компании, исполняемую представителями особого контрольного органа в рамках помощи органам управления предприятию.

Главная цель внутреннего аудита заключается в предоставлении массы объективной и своевременной информации о управленческой деятельности организации для совета директоров (либо общего собрания) с целью достижения ряда общекорпоративных целей и соблюдения стандартов по ведению бизнеса.

Актуальность темы «Исследование методов проведения внутреннего аудита информационной безопасности транспортной компании» обуславливает тот факт, что с каждым годом угрозы взлома информационных систем и компрометации данных становятся все более и более актуальными, более того вектор угроз смещается от простых методов к серьезным, продуманным и нетривиальным атакам. По итогам третьего квартала 2019 года экспертами Positive Technologies был отмечен рост числа целенаправленных атак по сравнению с 2018 годом [АОК-1-01з] (см. приложение А).

Такие атаки называются APT-атаками(Advanced persistent threat) и направленны они на конкретную организацию или отрасль промышленности

или бизнеса. По данным ФинЦЕРТ, за 2018 год было зафиксировано 687 атак на организации кредитно-финансовой отрасли. Из них 177 являлись целевыми.

Только от группировок Cobalt и Silence за 2018 год ущерб составил 58 млн. рублей. Одна такая атака может проводиться на протяжении нескольких месяцев, что существенно затрудняет ее обнаружение, так как администратор безопасности может и не заметить связи между несколькими событиями на отрезке в несколько недель, а специализированные системы обнаружения вторжений зачастую работают только с одним сегментом информационной системы, будь то сеть или управление контролем доступа. Такие СОВ не видят полной картины.

Для решения подобной задачи может потребоваться более комплексное программное обеспечение, способное не просто замечать признаки попыток нарушения конфиденциальности, целостности и доступности информационной системы и данных в ней, но и находить взаимосвязи между такими событиями.

Для всего этого подойдет система мониторинга и управления событиями информационной безопасности, такая система способна находить корреляции между различными событиями ИБ. В проекте, решается задача по разработке SIEM-системы, с добавлением к ней возможности сопоставления обнаруженных событий информационной безопасности признакам APT-атак.

Задача разработки собственной реализации системы мониторинга ставится, вследствие невозможности использовать представленные на рынке варианты SIEM-систем «из коробки». Для каждой такой системы необходима полноценная настройка, учитывающая специфику предприятия, необходимо создание дополнительных правил для обнаружения инцидентов информационной безопасности, месяцы накопления статистики и корректировка уже созданных правил обнаружения. Все это требует дополнительных расходов и привлечения группы специалистов.

Основное направление в проекте сделано на разработку SIEM-системы, опирающуюся на категорирование признаков APT-атак. Это позволит обнаружить целевую атаку на предприятие при минимальной настройке, что существенно сокращает время развертывания и финансовые издержки. В

первом разделе будет проанализирована общая информация о предприятии, необходимая для развертывания системы мониторинга безопасности.

Целью данной работы является исследование методов проведения внутреннего аудита информационной безопасности транспортной компании на примере.

Задачи:

- проанализировать цель, методы и технологии проведения внутреннего аудита информационной безопасности ТОО «KARCHER»;

- выявить проблемы и угрозы информационной безопасности ТОО «KARCHER», требующие решения;

- выбрать методологию решения поставленных проблем: методы аудита информационной безопасности организации , интеграцию внутреннего аудита информационной безопасности в систему программного обеспечения компании;

- разработать технологию внутреннего аудита информационной безопасности компании ТОО «KARCHER»;

- протестировать разработанную технологию внутреннего аудита информационной безопасности компании ТОО «KARCHER» и анализ результатов тестирования.

Объектом исследования в работе выступает транспортная компания ТОО «KARCHER».

Предметом исследования в работе является механизм проведения внутреннего аудита информационной безопасности.

Методы исследования. При проведении исследования настоящей темы использовались методы анализа и синтеза, логический, сравнительный, системно-структурный, метод описания и изложения.

Практическая значимость результатов исследования состоит в разработке направлений совершенствования системы внутреннего аудита информационной безопасности компании.

Структура работы представлена введением, тремя главами, заключением и списком используемых источников.

Глава 1 Анализ внутреннего аудита информационной безопасности ТОО «KARCHER»

1.1 Анализ задач и структуры ТОО «KARCHER»

ТОО «KARCHER» является официальным дистрибьютором таких популярных брендов как Astell&Kern, Audio-Technica, Colorfly, Coloud, Comply, Cowon, Fostex, Gametrix, HiFiMan, Koss, Marshall, Molami, Ritmix, Ultrasone, Urbanears, Westone [40].

Успешно развиваясь с начала 1993 года, ТОО «KARCHER» заслужила доверие и признание многочисленных клиентов, которые по достоинству оценили качество обслуживания и внимание к изменяющимся потребностям рынка.

Юридический адрес: г. Москва, ул. Сущевский Валл, 23.

ТОО «KARCHER» в первую очередь стремится способствовать росту и развитию своих партнеров, отдавая себе отчет, что прогресс партнера - это прогресс собственного бизнеса.

С помощью развитой сети сервисных центров компания обслуживает свою продукцию не только в любой точке Российской федерации, но и в странах СНГ.

ТОО «KARCHER»- является коммерческой организацией, основными направлениями деятельности которой являются:

- оптовая торговля непродовольственными потребительскими товарами;
- прочая оптовая торговля;
- розничная торговля в неспециализированных магазинах;
- хранение и складирование;
- организация перевозок грузов;
- деятельность автомобильного грузового транспорта.

Таким образом, объект исследования - ТОО «KARCHER»- является динамично развивающейся компанией по оказанию услуг доставки международных грузов.

Основная деятельность отдела транспортной логистики в компании ТОО «KARCHER» консолидация и доставка сборных грузов из Китая до двери получателя в России, город Москва, через порт Владивосток.

На сегодняшний день данная услуга пользуется большим спросом ввиду широкого распространения китайской продукции на российском и мировых рынках.

Доставка грузов в Китай и из него осуществляется в полном комплексе соответствующих услуг. В данный комплекс услуг входит, в частности, обеспечение товара необходимыми документами, а также таможенное оформление грузов.

Рассмотрим организацию международных перевозок грузов компании ТОО «KARCHER», при доставке грузов из Китая (см. рисунок 1.1).

Рассмотрим каждый этап более подробно.

- определение потребности в закупаемой продукции. Для этого отдел закупок рассчитывает остатки на складе, количество необходимой продукции, сроки поставки и характеристики товара.

Далее передают эту информацию отделу транспортной логистики для связи с поставщиком и оформления заявок на заказ.

- формирование и отправка заявок поставщикам. Так как перевозка международная, заявка составляется на английском языке. В заявке необходимо указать:

- идентификационный номер заказа;

- дата отправления заказа;

- краткую характеристику товара;

- количество товара;

- артикул заказываемых товаров.

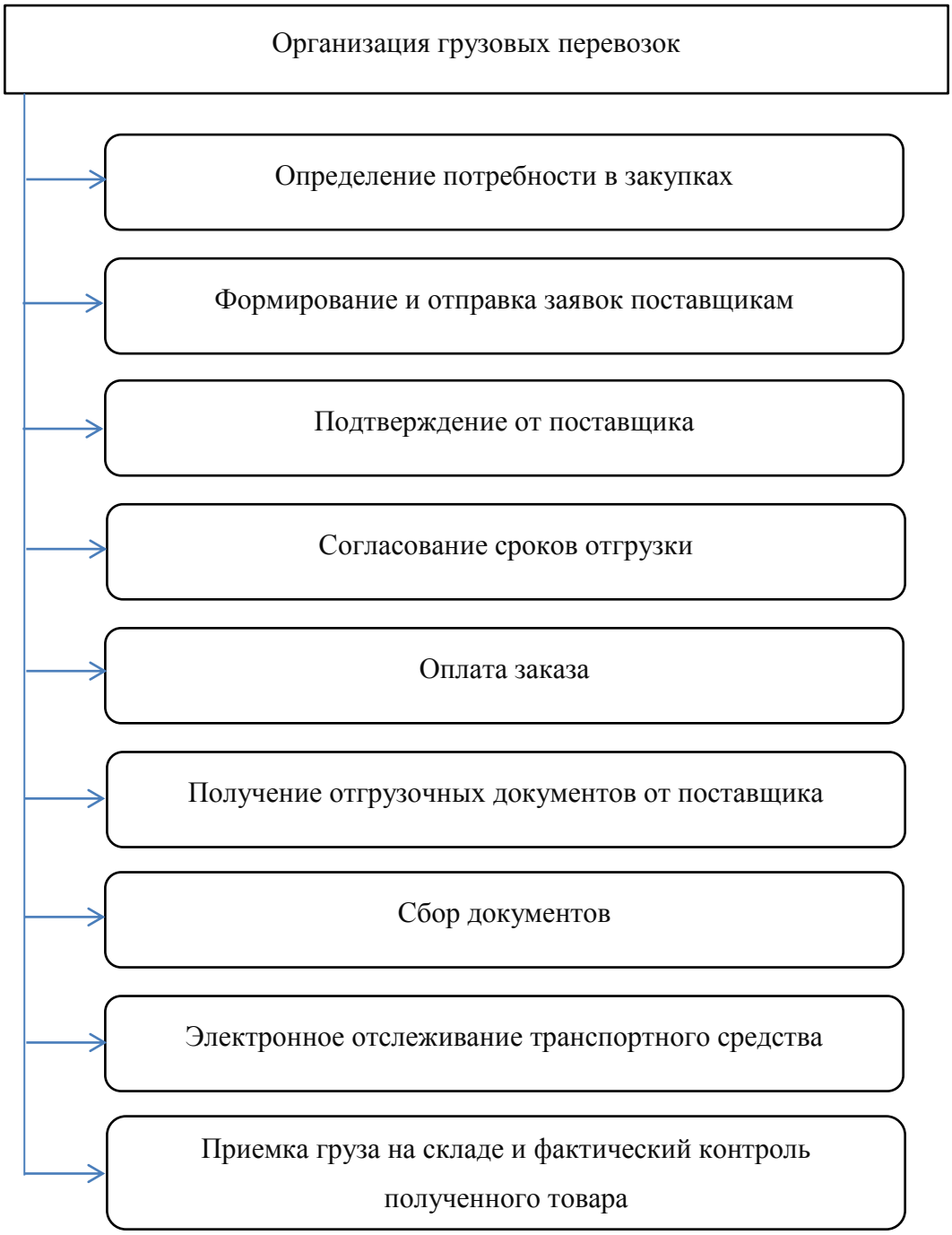


Рисунок 1.1 – Алгоритм организации грузовых перевозок ТОО «KARCHER»

- подтверждение от поставщика. На данном этапе сотрудникам отдела логистики необходимо удостовериться, что поставщик получил заявку, то есть поставщик должен отправить инвойс, в котором будет указываться:

- идентификационный номер инвойса;

- дата отправки инвойса;

- идентификаторы заказываемых товаров (артикулы);

- количество товара;

- цена за 1 единицу товара;

- примерные сроки отгрузки;

- условия оплаты согласно договору с указанием реквизитов счета;

- идентификатор расчетной валюты.

Вся информация, указанная в инвойсе проверяется сотрудниками отдела снабжения во избежание ошибок. Если же найдены какие-либо ошибки или неточности, то персонал связывается с поставщиком (чаще всего это происходит по электронной почте).

- согласование сроков отгрузки. В случае если на данном этапе все устраивает как поставщика, так и покупателя и на складе присутствует необходимое количество товара, происходит процесс подготовки груза к отправлению (сбор грузовых единиц, маркировка, упаковка) и обсуждение сроков отгрузки, дата и время прибытия транспортного средства для перевозки груза. Оформляется в виде заявки.

- оплата заказа. Оплата поставщику производиться только по безналичному расчету. Оплата по безналичному расчету оформляется исходящим платежным поручением и банковской выпиской.

- получение отгрузочных документов от поставщика. Отгрузочные документы являются документами, подтверждающими факт отгрузки, перевозки, страхования груза.

- сбор документов, необходимых для перевозки груза и прохождения таможни.

На перевозку морем и автотранспортом требуются следующие документы:

- внешнеторговый контракт с отправителем, подтверждающий наличие внешнеэкономической деятельности между компанией-отправителем и компанией-получателем;

- коммерческий инвойс, упаковочный лист.

- экспортная декларация производителя Линейный коносамент.

- накладная CMR. Документ, регламентирующий договорные отношения, которые возникают в процессе международных перевозок грузов автомобильным транспортом

- TIR CARNET (или книжка МДП) документ таможенного транзита, дающий право перевозить грузы через границы государств в опломбированных таможней кузовах автомобилей [12].

- сертификат РОСТЕСТ, если товар подлежит сертификации, если нет – требуется отказное письмо.

- электронное отслеживание транспортного средства. На данном этапе производится контроль времени прибытия транспортного средства, через электронную программу, где проложен маршрут следования груза и на каком этапе он перевозится.

- приемка груза на складе и фактический контроль полученного товара. Данная процедура осуществляется в несколько этапов. Во-первых, заказывается пропуск на машину с грузом, где указывается марка и номер транспортного средства. Во-вторых, сотрудник отдела транспортной логистики осуществляет внешний контроль контейнера, то есть контроль сохранности контейнера, проверка снятия пломб, внешнее состояние принятого товара, фотоконтроль.

В-третьих, получение и заполнение транспортно-грузовых документов.

За долгий срок сотрудничества с китайскими компаниями, компания ТОО «KARCHER» приобрела огромный опыт в построении логистических схем, подбирая наиболее оптимальный способ доставки груза из Китая, учитывая характер и особенности груза.

Среда для разработки информационной системы предприятия представляют собой как сервера с исходными кодами и «прошивками» программно-технических продуктов, так и персональные данные сотрудников организации.

Программными продуктами, содержащими информацию и применяемыми в предпринимательской деятельности ТОО «KARCHER» являются:

- 1С: Предприятие (версия 7.7);
- 1С: Предприятие (версия 8.2);
- 1С: Камин расчет заработной платы (версия 3.0);
- Oracle Database 11g
- Visual SVN server.

Современный уровень развития транспортной логистики требует постоянного улучшения и внедрения новых информационных систем. В настоящее время использование IT-технологий в транспортной логистике основывается на применении базовых решений.

Технологии бесконтактного определения уникальности товара (груза) при использовании штрих-кодов или электронных носителей сопровождения груза, что позволяет быстро и надежно получать необходимые данные. В результате производится быстрый и надежный контроль отгрузки и получения товара, кодируется отправитель, получатель, курьер, идентифицируется номер партии груза, серийные номера и информация о доставке.

В качестве отдельной подсистемы информационной логистики используется система управления складом (Warehouse Management System – WMS), которая объединяет все автоматизированные комплексы и системы, которые направлены на контролирование складских помещений. Она является неотъемлемой частью складской логистики и позволяет реализовать: визуализацию (наглядное отображение сегментов и зон склада) посредством применения мультимедийных приложений; голосовые команды оператора (voice order) при выполнении поиска нужного объекта хранения и его места на

складе за счёт голосового или цифрового запроса; радиоидентификацию (RFYD) по технологии передачи информации с помощью радиоволн и специальных считывающих устройств распознавания и отображения информации по каждой единице или партии хранения.

Для решения задачи комплексной оптимизации технологических, логистических и организационных процессов предприятие применяет универсальный подход. В качестве основы такого подхода выступает использовать имитационное моделирование в комплексе с эвристикой и численными методами.

В современных условиях в работе транспортнологистических терминалов используется информационное приложение Electronic data interchange (EDI), которое представляет самый современный и эффективный подход к решению проблем, возникающих в информационной логистике. Оно позволяет обмениваться логистической, коммерческой и финансовой информацией между деловыми партнёрами транспортно-логистического бизнеса в виде стандартных структурированных электронных сообщений. Достоинством использования EDI является то, что необходимые данные от одной компании извлекаются, форматируются, проверяются, пересылаются через платформу Edisoft, и во время пересылки вводится дополнительная информация, а весь информационный пакет переводится в стандартный формат, сохраняя её содержание. Принимающая сторона тут же получает сообщение в удобном и понятном виде.

Таким образом, в качестве объекта исследования в работе выступает компания ТОО «KARCHER». Информационную систему компании включают, в основном, данные о перевозимых грузах, схемах перевозок, перевозимом товаре. Учет всей входной информации осуществляется с помощью ряда компонентов – программ.

1.2 Анализ и технологии проведения внутреннего аудита информационной безопасности ТОО «KARCHER»

Основной целью проведения внутреннего аудита информационной безопасности ТОО «KARCHER» является определение перечня возможных угроз предприятия. Для этого разрабатывается частная модель угроз.

Цель внутреннего аудита содержится в содействии органам управления организации в осуществлении действий в системе управления. Наиболее принципиальной целью внутренних аудиторов на предприятии является обеспечивание удовлетворения потребностей органов управления в части предоставления контрольной информации по различным интересующим их вопросам.

Главным фактором, за счет которого исполняется эффективность применения систем внутреннего аудита в целях обеспечения качественного управления предприятием, считается оперативный (текущий) характер осуществляемого контроля.

За счет принятия значимых управленческих решений по предоставленным данным службой внутреннего аудита компании дается возможность вносить исправления, касающиеся отрицательных отклонений в деятельности фирмы в момент осуществления финансово-хозяйственной деятельности, а не только устанавливать обнаруженные негативные факты по данным финансовой отчетности. Настоящая модель была разработана на основании следующих документов (см. таблицу 1.1.).

Таблица 1.1 – Документы для разработки модели угроз [30]

Документ	Характеристика
Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, Утверждена заместителем директора ФСТЭК России 14 февраля 2008 г	Применяется для оценки угроз сохранности и использования информационных данных сотрудников или клиентов компании.

Продолжение таблицы 1.1

Документ	Характеристика
Методика определения угроз безопасности информации в информационных системах.	Включает общий алгоритм определения угроз и степени их воздействия на информационную систему.
Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, Утверждена заместителем директора ФСТЭК России 15 февраля 2008 г.	Применяется для оценки угроз сохранности и использования информационных данных сотрудников или клиентов компании.

Целью оценки возможностей нарушителей по реализации угроз безопасности информации является формирование предположения о типах, видах нарушителей, которые могут реализовать угрозы безопасности информации в информационной системе с заданными структурно-функциональными характеристиками и особенностями функционирования, а также потенциале этих нарушителей и возможных способах реализации угроз безопасности информации.

С учетом наличия прав доступа и возможностей по доступу к информации и (или) к компонентам информационной системы нарушители подразделяются на два типа:

- внешние нарушители (тип I) – лица, не имеющие права доступа к информационной системе, ее отдельным компонентам и реализующие угрозы безопасности информации из-за границ информационной системы;

- внутренние нарушители (тип II) – лица, имеющие право постоянного или разового доступа к информационной системе, ее отдельным компонентам [30].

Виды нарушителей и их возможные цели реализации угроз безопасности информации представлены в таблице 1.2.

Таблица 1.2 - Виды, типы и потенциал нарушителей [21]

Виды нарушителей	Типы нарушителей	Возможные цели реализации угроз безопасности информации	Потенциал нарушителей
Преступные группы	Внешний	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды.	Низкий
Внешние субъекты	Внешний	Идеологические или политические мотивы. Причинение имущественного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации. Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды.	Низкий
Конкурирующие организации	Внешний	Получение конкурентных преимуществ. Причинение имущественного ущерба путем обмана или злоупотребление доверием.	Средний
Разработчики, производители, поставщики программных, технических и программно-технических средств	Внешний	Внедрение дополнительных функциональных возможностей в программное обеспечение или программно-технические средства на этапе разработки. Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия.	Средний
Лица, привлекаемые для установки, наладки, монтажа пусконаладочных и иных видов работ	Внутренний	Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия.	Низкий
Лица, обеспечивающие функционирование информационной системы или обслуживающие инфраструктуру	Внутренний	Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия.	Низкий

Продолжение таблицы 1.2

Виды нарушителей	Типы нарушителей	Возможные цели реализации угроз безопасности информации	Потенциал нарушителей
Пользователи информационной системы	Внутренний	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Месть за ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия.	Низкий
Администраторы информационной системы и администраторы безопасности	Внутренний	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации. Месть за ранее совершенные действия. Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды.	Высокий
Бывшие работники	Внешний	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Месть за ранее совершенные действия.	Низкий

Угрозы безопасности информации могут быть реализованы нарушителями за счет [13]:

- несанкционированного доступа и (или) воздействия на объекты на аппаратном уровне (программы (микропрограммы), «прошитые» в аппаратных компонентах (чипсетах));

- несанкционированного доступа и (или) воздействия на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы);

- несанкционированного доступа и (или) воздействия на объекты на прикладном уровне (системы управления базами данных, браузеры, web-приложения, иные прикладные программы общего и специального назначения);

- несанкционированного доступа и (или) воздействия на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы);

- несанкционированного физического доступа и (или) воздействия на линии, (каналы) связи, технические средства, машинные носители информации;

- воздействия на пользователей, администраторов безопасности, администраторов информационной системы или обслуживающий персонал (социальная инженерия) [18].

Исходя из того, что в ИС обрабатываются также и персональные данные (ПДн), то следует определить также базовый уровень защищенности ИС, как ИСПДн.

Система внутреннего аудита информационной безопасности, в общем случае, состоят из 4 компонентов:

- компонент сбора информации, или же агрегатор, обеспечивает сбор информации из различных источников, таких как программное и аппаратное обеспечение, средства защиты информации, файлы логов;

- компонент обработки информации, участвующий в обработке событий, собранных агрегатором, и корреляции по различным критериям, на основании которых принимается решение о наличии инцидента ин-формационной безопасности;

- компонент хранения данных, который участвует в хранении данных в едином, понятном, как для остальных компонентов, так и для администратора;

- компонент управления системой мониторинга событий ин-формационной безопасности, который нужен для более гибкой настройки параметров.

Так как любая SIEM-система, это, прежде всего, средство защиты информации, то перед тем, как сформировать требования к ней, следует разобраться в том, из чего состоит атака на информационную систему, и на какие этапы она подразделяется, а также в чем состоят меры защиты от такой атаки. Такой разбор атаки и мер защиты позволит определить на каком из этапов защиты должна работать SIEM, следовательно, требования, предъявляемые к реализации системы мониторинга и управления событиями информационной безопасности, будут более осмысленными и актуальными.

Под уровнем исходной защищенности информационной системы персональных данных (ИСПДн) понимается обобщенный показатель,

зависящий от технических и эксплуатационных характеристик ИСПДн. Характеристики ИСПДн приведены в таблице 1.3

Таблица 1.3 - Базовый уровень защищенности ИСПДн [32]

Параметр	Значение	Уровень защищенности
По территориальному размещению информационной системы персональных данных	Локальная информационная система персональных данных, развернутая в пределах одного здания.	Высокий
По наличию соединения с сетями общего пользования	Информационная система персональных данных физически отделенная от сети общего пользования.	Высокий
По разграничению доступа к персональным данным	Информационная система персональных данных, к которой имеют доступ определенный перечень лиц работников организации, являющейся владельцем информационной системы персональных данных, либо субъектом персональных данных	Средний
По наличию соединения с персональными данными других информационной системы персональных данных	Информационная система персональных данных, в которой используется одна база персональных данных, принадлежащая организации - владельцу информационной системы персональных данных.	Высокий
По уровню обезличивания персональных данных	Информационная система персональных данных, в которой предоставляемые пользователю данные являются обезличенными.	Высокий
По объему персональных данных, которые предоставляются сторонним пользователям информационной системы персональных данных без предварительной обработки	Информационная система персональных данных не предоставляющая часть персональных данных.	Средний

Значению уровня защищенности «Высокий» соответствуют 4 характеристики. Значению уровня «Средний» - 3 характеристики, значению уровня «Низкий» - 0 характеристик. Таким образом, числовой коэффициент исходной защищенности ИСПДн Оператора соответствует значению 5 (средняя).

Таким образом, основной целью проведения внутреннего аудита информационной безопасности компании является определение перечня возможных угроз предприятия. Выделяют два типа нарушителей: внутренние и внешние. В качестве объекта защиты выступают: информационные данные сотрудников и клиентов компании; данные о технологиях перевозок; применяемых сервисов и методов складирования, что составляет коммерческую тайну.

1.3 Анализ угроз информационной безопасности ТОО «KARCHER», требующие решения

Актуальной считается угроза, которая может быть реализована в ИС и представляет опасность для конфиденциальной информации.

Актуальность угрозы определяется следующими параметрами:

- уровень исходной защищенности ИС (в нашем случае, ИСПДн тоже);
- частота (вероятность) реализации рассматриваемой угрозы.

Уровень исходной защищенности ИС и ИСПДн был представлен выше.

Под частотой (вероятностью) реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности КИ для данной ИС в складывающихся условиях обстановки. Вводятся четыре вербальных градации этого показателя:

- маловероятно – отсутствуют объективные предпосылки для осуществления угрозы (например, угроза хищения носителей информации

лицами, не имеющими легального доступа в помещение, где последние хранятся);

- низкая вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (например, использованы соответствующие средства защиты информации);

- средняя вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности конфиденциальной информации недостаточны;

- высокая вероятность - объективные предпосылки для реализации угрозы существуют, и меры по обеспечению безопасности конфиденциальной информации н не приняты.

При составлении перечня актуальных угроз безопасности ИС каждой градации вероятности возникновения угрозы ставится в соответствие числовой коэффициент, а именно:

- 0 для маловероятной угрозы;

- 2 для низкой вероятности угрозы;

- 5 для средней вероятности угрозы;

- 10 для высокой вероятности угрозы.

Полный перечень угроз, с полным перечнем угроз безопасности информации, показателями опасности этих угроз и вероятностью их реализации, а также подсчитанными коэффициентами реализуемости угроз представлены в таблице 1.4.

Следует отметить, что показатель опасности угрозы безопасности информации, так же как и перечень угроз утечки информации по техническим каналам и за счет несанкционированного доступа определяются на основании экспертной оценки.

Таблица 1.4 - Актуальность угроз безопасности информации

Угрозы утечки ин-формации по техническим каналам и за счет НСД	Уровень исходной защищенности (Y1)	Вероятность реализации угрозы (Y2)	Коэффициент реализуемости угрозы Y=(Y1+Y2)/20	Показатель опасности угрозы	Вывод об актуальности угрозы
Угроза повышения привилегий	5	2	0,35	высокая	актуальная
Угроза подмены программного обеспечения	5	2	0,35	средняя	актуальная
Угроза загрузки не-штатной операционной системы	5	5	0,5	средняя	актуальная
Угроза несанкциони-рованного создания учетной записи пользователя	5	2	0,35	средняя	актуальная
Угроза внедрения кода или данных	5	2	0,25	высокая	актуальная
Угроза преодоления физической защиты	5	2	0,35	низкая	неактуальная

При рассмотрении перечня актуальных угроз безопасности информации, представленных в таблице 1.4, можно заметить, что большая часть актуальных угроз в том или ином виде являются признаками APT-атаки.

Такими признаками являются:

- реализация угрозы повышения привилегий;
- реализация угрозы подмены программного обеспечения;

- реализация угрозы несанкционированного создания учетной записи пользователя;

- реализация угрозы внедрения кода или данных.

Следовательно, будет иметь смысл внедрение средства, способного своевременно обнаружить реализацию определенных угроз. Таким средством является SIEM-система, анализ требований к реализации которой будут рассмотрены.

Исходя из действий злоумышленника, атаку на информационную систему Electronic data interchange (EDI) можно разделить на 3 этапа:

- разведка:

- сканирование сетей и портов;

- обнаружение уязвимостей систем;

- сбор отпечатков систем;

- индексация web-страниц;

- атака:

- атаки типа «отказ в обслуживании»(dos/ddos);

- атаки типа «полный перебор»(bruteforce);

- повышение привилегий(privilege escalation);

- мошеннические атаки;

- спам;

- использование уязвимостей;

- социальная инженерия;

- закрепление в системе:

- сканирование внутренней сети;

- взлом соседних узлов;

- установка средств повторного внедрения.

Графически этапы атаки представлены на рисунке 1.2.

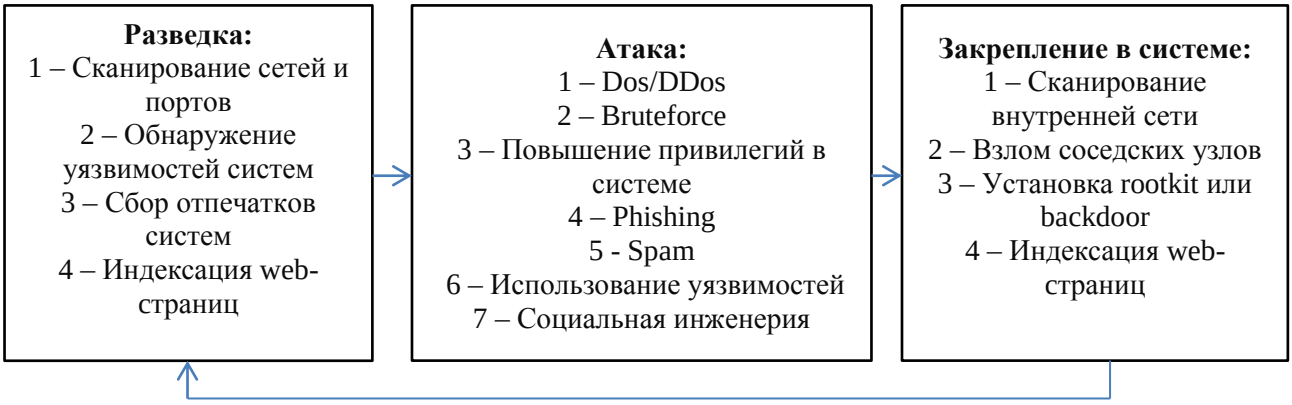


Рисунок 1.2 - Этапы проведения атаки на информационную систему

Важно понимать, что как атака ни информационную систему, так и защита от таких атак, это циклический процесс.

После закрепления в системе, злоумышленник вновь может провести разведку, саму атаку и закрепление в других узлах системы, пока не достигнет своей цели.

Такое подразделение атаки на этапы не является единственно верным. Существуют сервисы, вроде Mitre ATT | CK, которые предлагают свою цепочку действий злоумышленника, которая подразделяется на следующие этапы:

- начальный доступ;
- закрепление в системе;
- повышение привилегий;
- избегание средств защиты;
- получение доступа к учетным данным;
- изучение системы;
- дальнейшее продвижение;
- сбор данных;
- подготовка к выгрузке и выгрузка данных;
- влияние на ресурсы системы.

В отличие от этапов атаки злоумышленника, представленных на рисунке 1.2, этапы атаки злоумышленника, описанные Mitre, не являются циклически-

ми, то есть это вектор, который направлен от «начального доступа» к окончательному «влиянию на ресурсы системы». Каждое из «звеньев цепи» атаки на информационную систему согласно сервису Mitre ATT | CK будет более подробно рассмотрено в следующем подразделе.

В качестве механизма обнаружения угроз информационной безопасности в работе предлагается рассмотреть SIEM-систему, включающую следующие компоненты: компонент сбора информации, или же агрегатор; компонент обработки информации, участвующий в обработке событий, собранных агрегатором; компонент хранения данных; компонент управления системой мониторинга событий ин-формационной безопасности.

Таким образом, к выявленным в ходе исследования проблемам, угрожающим информационной безопасности ТОО «KARCHER», в работе отнесены следующие:

- реализация угрозы повышения привилегий;
- существование угрозы подмены программного обеспечения;
- вероятность угрозы несанкционированного создания учетной записи пользователя;
- реализация угрозы внедрения кода или данных.

Глава 2 Пути решения выявленных угроз информационной безопасности

2.1 Анализ путей решения выявлен угроз информационной безопасности в функционировании ТОО «KARCHER»

Конфиденциальная для бизнеса информация входит в сферу повышенного интереса конкурирующих компаний.

Для недобросовестных конкурентов, коррупционеров и других злоумышленников особый интерес представляет информация о составе менеджмента предприятий, их статусе и деятельности фирмы. Доступ к конфиденциальной информации и ее изменение могут нанести существенный урон финансовому положению компании. При этом, информационная утечка может быть даже частичной. В некоторых случаях даже обеспечение хищения 1/5 конфиденциальной информации может иметь критические последствия для финансовой безопасности. Причиной утечки информации, если отсутствует должное обеспечение информационной безопасности организации, могут быть различные случайности, вызванные неопытностью сотрудников.

Информационная безопасность ТОО «KARCHER» предполагает обеспечение защиты данных от хищений или изменений как случайного, так и умышленного характера. Система обеспечения информационной безопасности организации – эффективный инструмент защиты интересов собственников и пользователей информации. Следует отметить, что ущерб может быть нанесен не только несанкционированным доступом к информации. Он может быть получен в результате поломки коммуникационного или информационного оборудования. Особенно актуальна эффективная организация обеспечения безопасности информационных банковских систем и учреждений открытого типа (учебные, социальные и др.).

Для того чтобы наладить должное обеспечение защиты информации следует иметь четкое представление об основных понятиях, целях и роли информационной безопасности.

Оценка информационной безопасности (ИБ) ТОО «KARCHER» заключается в выработке оценочного суждения относительно адекватности используемых защитных мер и процессов управления ИБ или целесообразности (достаточности) затрат для обеспечения необходимого уровня ИБ на основе измерения и оценивания критических факторов объекта оценки.

Наиболее применяемой и хорошо разработанной является оценка соответствия ИБ объекта установленному эталону. Под оценкой соответствия ИБ объекта установленным требованиям понимается деятельность, связанная с прямым или косвенным определением выполнения или невыполнения соответствующих требований ИБ объекта. С помощью оценки соответствия ИБ оценивается правильность реализации защитных мер и правильность реализации процессов системы управления ИБ и идентифицируются недостатки реализации.

В результате проведения такой оценки ИБ формируется оценка степени соответствия ИБ эталону, в качестве которого могут быть приняты (в совокупности или отдельно):

– требования законодательства Российской Федерации в области ИБ;

– отраслевые требования по обеспечению ИБ;

– требования нормативных, методических и организационно-распорядительных документов по ИБ объекта;

– требования национальных и международных стандартов в области ИБ.

Однако если оценка соответствия правильности реализации защитных мер является информативной и основанной на значительном количестве нормативных, методических и организационно-распорядительных документов по ИБ объекта (политика ИБ объекта, план обработки риска, план реализации защитных мер и другое), то оценка соответствия правильности реализации

процессов управления ИБ является не столь информативной, поскольку не дает оценку возможности процессов, а дает лишь оценку уровня реализации процессов управления ИБ.

Таким образом, формирование и применение при проведении аудита ИБ ТОО «KARCHER» оценки соответствия для защитных мер и оценки возможности для процессов управления ИБ создаст наиболее адекватные информационные потребности для улучшения и совершенствования ИБ объекта.

Правильность реализации защитных мер определяется с помощью измерения атрибутов (свойств, характеристик) защитных мер. Измерение атрибутов осуществляется с помощью методов измерения, включающих следующие процедуры:

– сбор свидетельств оценки атрибутов с помощью опроса, наблюдения, документальной проверки;

– измерение (оценивание) атрибутов относительно определенной шкалы, зафиксированной или в анкетах (для совокупности атрибутов), или в метриках (для каждого атрибута).

С целью оценки соответствия атрибутов процессов обеспечения ИБ установленным критериям оценка строится на основе показателей функционирования защитных мер, которые применяются для измерения правильности реализации защитных мер объекта.

Для описания соответствия реальных атрибутов Y требуемым атрибутам Y^{TP} введем числовую функцию на множестве атрибутов защитных мер - функцию соответствия:

$$p = p\,(Y, Y^{TP}) \qquad (1)$$

Эту функцию можно использовать в качестве показателя W функционирования (правильности реализации) защитных мер объекта, то есть p=W:

$$W = p\,(Y, Y^{TP}) \qquad (2)$$

Показатель функционирования W защитной меры есть мера степени соответствия реальных атрибутов требуемым.

Для отдельной защитной меры измеряется Wji - частный показатель i-го атрибута (защитной меры) j-й области обеспечения ИБ. Для совокупности защитных мер единой области обеспечения ИБ (криптографическая защита, антивирусная защита и др.) вычисляется Wj - комплексный показатель j-й области обеспечения ИБ.

Характеристики и свойства защитных мер, которые несут атрибуты, не равнозначны с точки зрения значимости защитных мер для обеспечения ИБ. Поэтому необходимо определить способ объединения частных показателей при формировании комплексных показателей из частных.

Комплексные показатели при различной значимости частных показателей можно вычислять с помощью свертки:

$$W_j = \sum a_{ij} W_{ij} \qquad (3)$$

где a_{ij} - коэффициент значимости частного показателя i-ого атрибута (защитной меры) j-ой области обеспечения ИБ;

Wij – защитная мера отдельного атрибута.

Так получается оценка соответствия реализованных защитных мер установленным требованиям и оценка реализованных областей обеспечения ИБ относительно установленной шкалы уровней соответствия областей обеспечения ИБ.

Следующим этапом оценки ИБ объекта является оценка возможности процессов управления ИБ.

Оценка возможности процессов управления информационной безопасностью основывается на следующих принципах:

– процессы управления ИБ оцениваются по пяти уровням: от первого (минимального) до пятого (максимального), причем, каждый следующий уровень включает полностью реализацию предыдущих уровней;

– каждый уровень описывается определенным набором показателей и их значениями;

– оценка процессов управления ИБ осуществляется на основе свидетельств оценки возможности процессов.

Для оценки возможности процессов управления ИБ используются основные и комплексные показатели. Комплексные показатели Ki (i – номер комплексного показателя) возможности процессов управления ИБ отражают совокупность характеристик уровней возможности.

Основные показатели Kij (i – номер комплексного показателя, j – номер основного показателя в комплексном показателе) отражают отдельные характеристики уровней возможности процессов управления ИБ и входят в состав комплексных показателей.

Основные показатели оценки возможности процессов управления ИБ разрабатываются для каждого комплексного показателя. Например, для комплексного показателя К3 основные показатели могут быть следующими (см. таблицу 2.1).

Таблица 2.1 - Основные бинарные показатели для комплексного показателя К3

Уровень возможности процесса	Основной показатель процесса
К3.1	Зафиксирован ли документально процесс управления ИБ
К3.2	Существует ли на объекте ролевая политика в области ИБ
К3.3	Определены ли цели осуществления процесса управления ИБ
К3.4	Определены ли ответственности и полномочия по осуществлению процесса управления ИБ
К3.5	Идентифицированы ли ресурсы и информация, необходимая для осуществления процесса управления ИБ
К3.6	Определен ли перечень результатов (выходов) процесса управления ИБ
К3.7	Формализована ли существующая на объекте практика в области управления ИБ в виде процедур процесса управления ИБ
К3.8	Регламентирован ли на объекте подход к обучению и информированию о реализованном процессе управления ИБ
К3.9	Установлены ли на объекте требования по осуществлению контроля за реализацией процесса управления ИБ
К3.10	Осуществляется ли на объекте оценка процесса управления ИБ

Основные показатели определяются с помощью методов измерения, включающих следующие процедуры:

– сбор свидетельств оценки возможности процессов управления ИБ с помощью опроса, наблюдения, документальной проверки;

– измерение (оценивание) основных показателей относительно определенной шкалы, зафиксированной или в анкетах (для совокупности основных показателей), или в метриках (для каждого основного показателя).

Шкала может быть следующей (см. таблицу 2.2).

Таблица 2.2 – Шкала

Шкала	Интервал	Характеристика
Н – не выполнен	[0% - 15%]	Свидетельств выполнения основного показателя мало или они отсутствуют;
Ч – частично выполнен	[15% - 50%]	Имеются свидетельства частичного, некоторого выполнения основного показателя;
В – в основном выполнен	[50% - 85%]	Имеются свидетельства существенного выполнения основного показателя. В оцениваемой характеристике процесса возможны некоторые слабые места;
П – полностью выполнен	[85% - 100%]	Имеются свидетельства систематического и полного выполнения основного показателя.

Предложенная оценка ИБ объекта при проведении аудита ИБ позволяет сформировать оценку соответствия правильности реализации защитных мер, что важно для оценивания текущего уровня защищенности объекта, и оценку возможности процессов управления ИБ, что необходимо для прогнозирования развития уровня ИБ объекта.

2.2 Возможности системы SIEM для аудита информационной безопасности организации

Для проведения аудита информационной безопасности сетевой инфраструктуры ТОО «KARCHER» требуется осуществить сбор и анализ большого массива данных за определенный период времени. Кроме того, требуется периодически осуществлять повторение процедур сбора и анализа сетевых данных для более полного представления о возможных проблемах в сети.

Способ проведения аудита зависит от задач и уровня угрозы. Чем меньше компания и ниже продвинутость используемых технологий, тем меньше интерес злоумышленников и проще оценка. Важное условие перед началом аудита — составление технического задания на работающую систему информационной безопасности: и руководство компании и аудитор должны представлять, как будет работать идеальная в их понимании служба.

Существует несколько категорий угроз, способных привести к утечке, потере или ненадлежащему использованию информации в бизнесе.

Первый вид — целенаправленные действия злоумышленников, намеревающихся получить доступ к вашим данным и использовать их против вас или для получения выгоды. Способов много — от компьютерных атак и хищений до методов социальной инженерии и рейдерских захватов. Причем атаки не обязательно совершают сторонние злоумышленники. Такими действиями вполне могут заниматься сотрудники компании: для шантажа, продажи, захвата власти и т.д.

Второй источник — неосмотрительные действия, приводящие к уязвимостям в системе безопасности. Это может быть, например, использование сотрудниками зараженных программ или посещение инфицированных сайтов.

Третий вид угрозы — несоблюдение элементарных правил защиты: отсутствие антивирусов, беспорядочное хранение документов и

беспрепятственный доступ к ним всех подряд, отсутствие систем дублирования и т.д.

Сейчас большое распространение получили системы типа SIEM (Security information and event management), которые позволяют осуществлять процедуры аудита сетевой инфраструктуры в процессе ее эксплуатации непрерывно. Целью данного типа аудита является определение того, на сколько сетевая инфраструктура соответствует предъявляемым к ней требованиям информационной безопасности (ИБ). Таким образом определяется так же уровень защищённости информационных сетевых компонентов корпоративной информационной системы (КИС) предприятия.

Для достижения целей аудита (превентивного и детектирующего типа) информационной безопасности сетевой инфраструктуры АСУ ТП ТОО «KARCHER» требуется решить ряд задач:

- осуществить поиск уязвимостей сетевых систем различными методами;

- оценить риски с учетом результатов исследования активности в сетевой инфраструктуре организации (отслеживание легитимных и вредоносных запросов);

- оценить уровень защищенности с учетом всех данных и всех факторов, влияющих на состояние инфраструктуры;

- определить уровень соответствия стандартам ИБ и выработать ряд рекомендаций по повышению уровня защищенности.

Для решения поставленных задач требуется изучить состояние сети, определить особенности ее инфопотоков и, если позволяет специфика инфраструктуры, провести тестирования на проникновение, то есть реализовать активный аудит (pen-тест). Однако в сетях АСУТП на диспетчерском уровне pen-тест, как правило, не допускается, поскольку подобные действия могут снизить работоспособность системы, что негативно скажется на работоспособности предприятия в целом.

Поскольку при аудите ТОО «KARCHER» и последующем анализе его результатов следует учитывать влияние уже встроенных в инфраструктуру

средств информационной безопасности, нужно изучить, какие компоненты систем защиты активны на рассматриваемом уровне АСУ ТП. Защита может обеспечиваться следующим:

-системами распределения прав доступа;

-системами контроля трансляции данных через пользовательский интерфейс OPC-сервера, сервер базы данных и подсистемы сбора и хранения данных;

-антивирусными системами;

-системами обнаружения вторжений.

Разграничение доступа осуществляется средствами операционной системы. Также могут применяться специальные программные и программно-аппаратные средства для защиты операционной системы, позволяющие контролировать разрешения политик безопасности на критически важных компонентах сети. Следует учитывать, что при аудите цели злоумышленника не очевидны, и часто проявления деструктивных влияний на компоненты уровня могут оказываться непоказательными, поскольку не затрагивают целевые объекты атаки.

Однако большую сложность представляет контроль среды передачи данных на диспетчерском уровне АСУТП. Сейчас Ethernet используется как единая среда передачи данных для АСУТП, хотя на диспетчером уровне могут транслироваться данные подключенных ПЛК, которые используют протоколы Modbus/TCP, EtherNet/IP, PROFInet и др. При этом рекомендуется применять те устройства передачи данных, которые обеспечивают защиту от подмены IP-адресов узлов сети, а также защиту от утечки данных. Соответственно, требуется определить те методы и технологии, которые могут, учитывая специфичность сетевой инфраструктуры уровня системы, использоваться для реализации полноценного аудита. Необходимо понять, какие при аудите слабые и сильные стороны существуют у техник анализа данных с учетом технологических ограничений.

Одним из важнейших направлений контроля состояния АСУ ТП ТОО «KARCHER» является внедрение и «тонкое» (то есть учетом функциональных особенностей компонентов сети) использование систем обнаружения сетевых атак как в сетевой, так и в хвостовой реализации. Известные сетевые системы обнаружения и предотвращения вторжений могут использоваться как средства защиты и, одновременно, как средство сбора данных с последующей сигнализацией об аномальном состоянии системы или данных трафика.

Такие системы, размещенные на диспетчерском (среднем) уровне, используются для защиты нижних уровней АСУТП, на которых работа средств контроля трафика может привести к задержкам в трансляции данных, что критически скажется на работе ПЛК.

Принцип работы средств аудита и контроля защищенности строится на основе централизации процедур журналирования (системные журналы и журналы аудита безопасности) и выявлении критичных для системы событий с оповещением о них администраторов безопасности. При этом следует учитывать проблемы, которые могут возникнуть при эксплуатации данных систем. Главная проблема – это несовместимость технологий обработки данных и способов их трансляции. Технологические различия могут проявляться в использовании или неиспользовании OPC-сервера в системе, касаться различий операционных платформ. Проблемы несовместимости могут быть связаны с использованием протоколов, уникальных для технологической сборки уровня ПЛК. Несовместимость средств аудита и исследуемых систем может возникнуть по следующим причинам:

- влияние на поток данных, что ограничит функционал SCADA, работающей в реальном режиме времени, с последующим вызовом коллизий;

- возможен эффект исчерпания ресурсов при активном аудите сервисов и/или сетевых служб SCADA.

Таким образом, средства аудита и контроля трафика ТОО «KARCHER» следует встраивать на диспетчерский уровень, во-первых, учитывая технологическую специфику конкретно взятого диспетчерского уровня АСУ

ТП системы, во-вторых, учитывая разделение технологий передачи данных на два уровня: уровень стандартных протоколов, используемых в корпоративных информационных системах и уровень технических протоколов типа CANopen, HART, Modbus. Так же требуется соблюдать осторожность при перехвате данных для анализа в процессе аудита, поскольку это может вызвать критическую для системы нижнего уровня АСУТП задержку.

Для проведения аудита информационной безопасности ТОО «KARCHER» на диспетчерском уровне необходимо определить основной компонентный состав уровня, функциональные свойства его компонентов, а так же выявить средства информационной защиты, применение которых возможно с учетом технологической специфики уровня. Необходимо учитывать особенности организации АСУТП, а именно: подсистемы диспетчерского и полевого (нижнего) уровня должны быть связаны с корпоративной сетью и компонентами административного управления. Часть системы при эксплуатации полевого уровня, может работать в реальном режиме времени, который часто совмещается с виртуализированной обработкой данных на уровнях общего управления. Таким образом, исследуя инфраструктуру предприятия при аудите, требуется определить, к какому уровню относятся следующие компоненты:

- межсетевые экраны (мэ), расположенные на границах уровней.

- системы удаленного доступа позволяющие контролировать производственные процессы.

- модемы, предназначенные для связи между mtu-терминалами и периферийными устройствами.

- маршрутизирующие устройства, выполняющие функции соединения сетей lan с wan-сетями, mtu-терминалов и rtu-устройств.

Кроме того, следует проанализировать промышленную сеть ТОО «KARCHER», которая включает сенсоры, датчики и элементы оборудования с программируемым логическим контроллером (ПЛК). Учитывая эти факторы, можно выделить те технологии, при работе с которыми проблем совместимости

возникнуть не должно. В рамках решения задач аудита применимы системы обнаружения (СОВ) типа OSSEC. Эта система классифицируется как HIDS (система хостового типа), и имеет клиентско-серверную архитектуру. В ней в качестве клиентов применяются агенты, установленные на контролируемые узлы сети. Агенты передают данные на сервер для последующего анализа с использованием специально созданных для заданного уровня инфраструктуры АСУТП правил аудита. Также данная СОВ решает задачи контроля целостности среды, отслеживает до-ступ привилегированных пользователей. Эта технология позволяет не использовать интеллектуальные методы анализа данных, и объем анализируемой информации не ограничен только сетевыми данными.

Перед этапом внедрения СОВ нужно было определить принципы встраивания механизмов OSSEC HIDS и принципы формирования правил аудита с учетом топологии сети и технологических особенностей диспетчерского уровня. Эти принципы были сформулированы следующим образом:

- функционал OSSEC HIDS не должен влиять не работоспособность АСУТП. Это может быть достигнуто за счет избирательной установки агентов на специально отобранные узлы с учетом специфики сетевых сервисов диспетчерского уровня. При этом СОВ будет функционировать на уровне предупреждений в режиме Real-Time.

- необходимо обеспечить зеркалирование трафика через SPAN-порт (Switched Port Analyzer) в том случае, если есть вероятность возникновения коллизии в трансляции данных при работе OSSEC.

- порт 1514/ udp должен быть свободен, так как агенты подключаются к серверу через этот порт. Поскольку агент взаимодействует с сервером через UDP-порт 1514, OSSEC может работать на узле и как сервер и как агент. В этом случае он не будет влиять на трафик, но будет исключен из общей сети агентов, что снизит уровень централизации аудита.

Основываясь на указанных принципах, целесообразно формировать компонентную сборку механизмов СОВ следующим образом: узлы МРВ (монитор реального времени) и Web-сервисов будут включать в свой состав и серверы OSSEC, и агенты, поскольку при работе с данными компонентами опасность задержки в передаче сетевых пакетов будет критична для системы. Использование полноценной клиентско-серверной архитектуры СОВ, то есть когда сервер будет отделен от агентов сбора данных, возможно, если агенты будут интегрированы на отдельные узлы АРМ и серверы архивов, поскольку в этом случае допустима небольшая задержка при трансляции данных.

Правила должны учитывать специфику компонентной организации механизмов СОВ, а также требования трансляции служебных данных при работе в инфраструктуре диспетчерского уровня. При этом, у каждого правила OSSEC есть уникальный идентификатор (идентификаторы в диапазоне от 100000 до 109999 для собственных правил). Правила сгруппированы в соответствии с целью их применения. Так же у каждого правила есть уровень критичности (level) от 0 до 15. При значении 0 событие игнорируются, а 15 означает максимальный уровень критичности. Это позволяет задать приоритеты при анализе событий. Всего для рассмотрения процедур аудита было сформировано 11 типов правил:

- угроза внедрения вредоносного кода или данных.
- угроза перехвата данных, передаваемых по вычислительной сети.
- угроза подделки записей журнала регистрации событий.
- угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы.
- угроза воздействия на программы с высокими привилегиями.
- угроза сканирования веб-сервисов.
- угроза подбора пароля.
- угроза «кражи» учётной записи доступа к сетевым сервисам.
- угроза обнаружения хостов.

- угроза использования механизмов авторизации для повышения привилегий.

- угроза внедрения кода или данных.

Таким образом, каждое правило отнесено к определенному типу узлов диспетчерского уровня, учитывает архитектурные особенности построения серверно-агентной системы HIDS и имеет уровень критичности в соответствии с оценкой опасности угрозы. При этом надо отметить, что данные правила могут работать с протоколами технических систем уровня ПЛК, такими как ModBus.

Как дополнение к системам SIEM для объективной оценки рисков сетевой инфраструктуры можно использовать интеллектуальные методы и, соответственно, механизмы анализа. Реализация данных методов имеет свою специфику. Один из наиболее эффективных интеллектуальных методов связан с построением аналитических моделей, которые используются для анализа данных.

Применяя их, можно понять закономерности проявления нарушений и в дальнейшем прогнозировать появление потенциальных угроз. Данные модели можно непрерывно обучать. В целом, эта методика предназначена для нахождения комбинации математических уравнений, которые лучше всего предсказывают результат.

Перед обучением модели необходимо сформировать обучающую выборку. Ее можно получить, снимая данные в определенный период времени с подконтрольной сети перед началом процедур аудита, или же заимствовать данные из набора СОВ OSSEC в той части, где фиксируются атаки.

Однако и в первом и во втором случае данные необходимо привести к тому виду, который требуется для обработки в модели. Для этого в модуле анализа обязательно должны присутствовать:

- подмодуль обработки и анализа типа Pandas;

- инструментарий для прогнозного анализа данных типа Scikit-learn (он включает в себя библиотеки классификаторов, которые будут использоваться для анализа).

Анализатор захватывает весь сетевой трафик, но поскольку обучение касается протоколов модели OSI, то будут интерпретироваться только кадры Ethernet. В выбранной модели заранее задаются исключения на отбор пакетов технологического уровня, что позволит сохранить требуемую скорость передачи для технических данных.

После интерпретации кадра, пользователю демонстрируется информация заголовков кадра и происходит сравнение значения поля «EtherType» (Ethernet_protocol). Согласно стандарту IEEE 802.3 полю IPv4 соответствует значение 0x0800. При несоответствии поля заданным параметрам будет указано: «неопределённый сетевой протокол». Такой пакет не будет обрабатываться.

Следующий необходимый компонент - программа Argus, которая генерирует информацию о состоянии трафика. Она обрабатывает полученные пакеты и генерирует сводные данные о сетевом потоке. Argus может работать на отдельном граничном узле, фильтруя весь сетевой трафик. Кроме того, эта программа может работать как автономный модуль сбора и анализа сетевых данных.

Используя включенные в свой состав алгоритмы, Argus находит признаки для формирования шаблона. Каждый признак и его атрибуты, используемые для обучения модели и создания решения, нужно анализировать вручную, чтобы найти ошибки в наборах: требуется исключить неактуальные признаки, произвести масштабирование числовых атрибутов и преобразование категориальных атрибутов (для приведения всех данных к требуемому единому масштабу атрибутов используется два типа масштабирования: масштабирование по минимаксу или нормализация (min-max scaling / normalization) и стандартизация (standardization)). Таким образом можно сформиро-вать шаблоны отбора для конкретной сети диспетчерсго уровня,

который, очевидно, характеризуются большей технологической специфичностью и большим количеством ограничений, чем стандартная корпоративная сеть.

Однако выбранные интеллектуальные методы ограничены спецификой обучаемой модели и необходимостью приведения к требуемому виду данных, то есть данные должны быть одного порядка.

С другой стороны, подобный механизм позволяет посредством обучения и выработки приемлемой модели классификации учесть динамику изменений сетевых угроз с учетом их специфики, что в системе HIDS, основанной на статических правилах, сделать не возможно. При этом, учитывая специфику встраивания OSSEC в сеть диспетчерского уровня и принципы формирования правил, сложно с помощью хостовой системы обнаружения создать единый контур аудита, то есть когда управление и анализ отслеживаемых событий будут полностью централизованным. Однако подобные системы позволят учесть все виды событий в сети и, более того, позволяет частично контролировать трафик уровня контроллеров.

Таким образом, в ходе исследования в рамках данного раздела были проанализированы возможные варианты решения проблем информационной безопасности организации. В качестве решения в работе предложено рассмотреть систему типа SIEM, позволяющую осуществлять процедуры аудита сетевой инфраструктуры в процессе ее эксплуатации непрерывно. Так же в работе исследованы различные сложности, которые могут возникнуть на этапе внедрения системы SIEM в деятельности компании.

2.3 Интеграция внутреннего аудита информационной безопасности в систему программного обеспечения компании

Для организации безопасной разработки программного обеспечения ТОО «KARCHER» необходимо соответствовать следующим условиям:

- наличие службы информационной безопасности и максимальная близость к производству сотрудников данной службы.

- наличие подготовленных qa-инженеров.

- наличие подготовленных performance-инженеров.

- наличие устоявшихся и зарекомендовавших себя производственных процессов.

Ориентиром может быть международный стандарт ISO 17799 по управлению информационной безопасностью. Безусловно, для большинства предприятий внедрение всех его положений избыточно, но именно оттуда можно почерпнуть максимум знаний по этому вопросу. Также важно, чтобы исполнитель, проводящий аудит, в отчете отразил приоритетность и степень каждой из угроз, чтобы руководитель представлял, в каком порядке и с какой скоростью следует приниматься за их устранение.

Основными задачами комплексной интеграции практик аудита информационной безопасности программного обеспечения в жизненный цикл разработки является:

- выстраивание процесса интеграции аудита информационной безопасности по в стадии жизненного цикла проектов разработки по, а не постфактум, когда аудит проводится после реализации кодирования программного обеспечения.

- в создании условий масштабируемости аудита иб по, а именно:

- развитие внутренних ключевых компетенций команды разработки и экспертов по кибербезопасности.

- автоматизация процесса аудита иб по.

- в формировании приоритетов проведения аудита иб по компании:

- интеграции аудита иб по осуществляется для приложений и сервисов с высоким уровнем риска.

- фокус на базовые практики software security.

- аудит иб по осуществляется только для реалистичных угроз и уязвимостей конкретного сервиса или продукта.

Для построения аудита информационной безопасности программного обеспечения рекомендуется к использованию следующих стандартов по ИБ, в рамках которых формируются критерии безопасности аудита.

В случае осуществления компанией банковской деятельности используется СТО БР ИББС - Стандарт Банка России, направленный на установление единых требований по обеспечению информационной безопасности организаций банковской системы Российской Федерации и повышение эффективности мероприятий по обеспечению и поддержанию информационной безопасности организаций банковской системы Российской Федерации.

Все указанные стандарты безопасности должны прорабатываться под реальные проблемы, которые влияют на методику интеграции аудита информационной безопасности программного обеспечения в жизненный цикл разработки.

Таким образом, в целях проведения аудита информационной безопасности сетевой инфраструктуры осуществляется сбор и анализ большого массива данных за определенный период времени. Так же требуется периодически осуществлять повторение процедур сбора и анализа сетевых данных для более полного представления о возможных проблемах в сети. Способ проведения аудита зависит от задач и уровня угрозы. Чем меньше компания и ниже продвинутость используемых технологий, тем меньше интерес злоумышленников и проще оценка.

Наиболее распространенной системой внутреннего аудита выступает система типа SIEM (Security information and event management), которые

позволяют осуществлять процедуры аудита сетевой инфраструктуры в процессе ее эксплуатации непрерывно.

Целью данного типа аудита является определение того, на сколько сетевая инфраструктура соответствует предъявляемым к ней требованиям информационной безопасности (ИБ). Таким образом определяется так же уровень защищённости информационных сетевых компонентов корпоративной информационной системы (КИС) предприятия.

Формирование и применение при проведении аудита ИБ оценки соответствия для защитных мер и оценки возможности для процессов управления ИБ создаст наиболее адекватные информационные потребности для улучшения и совершенствования ИБ объекта.

Таким образом, Для проведения аудита информационной безопасности ТОО «KARCHER» на диспетчерском уровне необходимо определить основной компонентный состав уровня, функциональные свойства его компонентов, а так же выявить средства информационной защиты, применение которых возможно с учетом технологической специфики уровня. В соответствии с этим в качестве решения выявленных угроз информационной безопасности ТОО «KARCHER» в работе предлагается внедрение системы типа SIEM. Принцип работы средств аудита и контроля защищенности строится на основе централизации процедур журналирования и выявлении критичных для системы событий с оповещением о них администраторов безопасности.

Глава 3 Реализация разработанной технологии внутреннего аудита информационной безопасности компании ТОО «KARCHER»

3.1 Характеристика общей структуры системы аудита информационной безопасности

Костяк любой системы аудита информационной безопасности, это агрегатор информации и ее анализатор. Агрегатор собирает информацию из разных источников и упаковывает ее в необходимый для анализатора формат.

Анализатор по собранным данным формирует уведомление об инцидентах информационной безопасности и оповещает администратора информационной безопасности о наличии несанкционированных действий в системе.

Иными словами, для создания самой простой SIEM системы необходимо разработать модуль корреляции и модуль агрегации.

Разрабатываемая SIEM система помимо модулей агрегации и корреляции будет состоять также из модуля предсказаний дальнейшего поведения злоумышленника в системе на основании матрицы симптомов кибератак различных группировок, также при разработке настоящей SIEM системы будут учитываться все требования, сформированные в предыдущем разделе.

С архитектурной точки зрения, разрабатываемая система внутреннего аудита и управления событиями информационной безопасности представляет собой совокупность модулей, взаимодействующих между собой.

Сама система разрабатывается на языке программирования C++. Выбор данного языка программирования позволяет с одной стороны позволяет воспользоваться преимуществами объектно-ориентированного подхода при проектировании программ, с другой стороны, программы написанные на этом языке программирования выполняются значительно быстрее программ, написанных на других ЯП, поддерживающих объектно-ориентированную парадигму программирования.

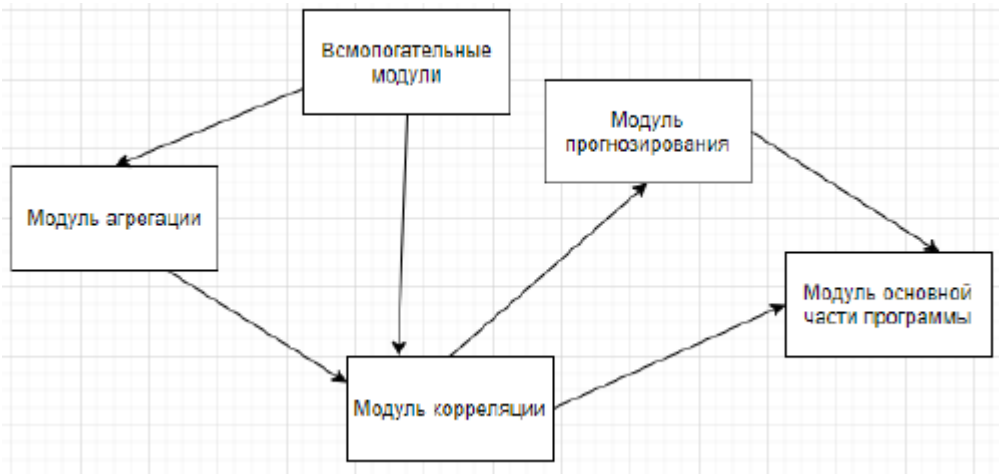


Рисунок 3.1 - Общая архитектура приложения

Если при проектировании самой программы применяется модульный подход к программированию, что позволяет довольно легко модернизировать SIEM-систему, просто заменяя один модуль другим при необходимости. То при проектировании самих модулей уже применяется объектно-ориентированный подход к программированию, это позволяет легко масштабировать каждый из модулей, добавляя новые сущности – классы, при необходимости.

Более подробная информация о ходе разработки каждого из модулей представлена ниже. Также ниже представлены алгоритмы работы модулей корреляции и прогнозирования.

3.2 Алгоритмы работы модулей корреляции и прогнозирования

Агрегация – это процесс объединения элементов в единую систему. Применительно к разрабатываемой SIEM, этот термин означает интеграцию информации с различных источников в единый формат, удобный для анализа модулем корреляции. В настоящем проекте в качестве единого формата выступает набор JSON-файлов, конструируемый из log-файлов от различных источников информации. Формат JSON был выбран не случайно, данный формат представления данных является одним из самых популярных, наряду с XML. Также JSON формат крайне удобен для программного представления

данных и легко читается человеком при просмотре исходного содержимого JSON файла.

Модуль агрегации состоит из совокупности классов унаследованных от одного общего класса. Этот общий класс является реализацией интерфейса всего модуля. UML-диаграмма модуля агрегации представлена на рисунке 3.2.

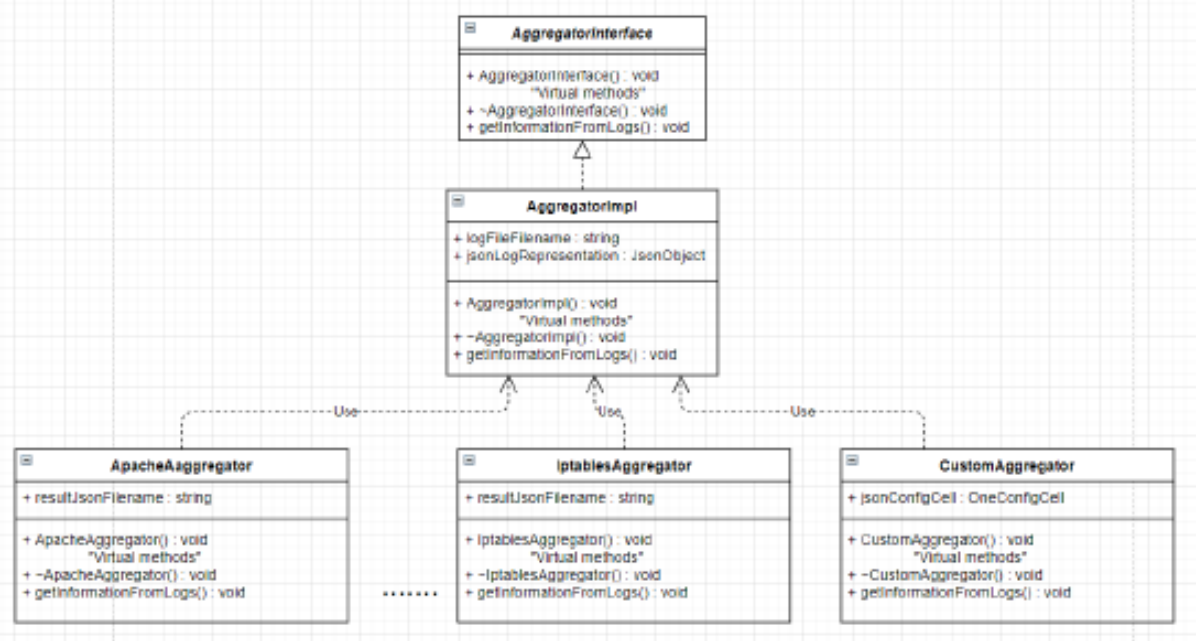


Рисунок 3.2 – UML-диаграмма классов модуля агрегации

Многоточием обозначается пропуск некоторого количества классов, в угоду наглядности. Классов унаследованных от основного класса реализации может быть неограниченное количество, это позволяет добавлять сколь угодное число источников агрегации информации для новых признаков. Также на диаграмме представлен класс пользовательских агрегаций. Спроектированный класс пользовательских агрегаций позволяет добавлять дополнительные источники для сбора информации, не создавая дополнительных классов в коде. Этот класс является пользовательским инструментов внедрения дополнительных правил агрегации. Например, если на предприятии будет установлен СКУД, который хранить информации о ходе своей работы в log-файлах, то в SIEM-систему можно будет добавить правило, по которому она будет собирать ин-формацию из log-файлов системы контроля и управления доступом.

Теперь более подробно рассмотрим источники информации для агрегирования, как уже было сказано выше, данными источниками выступают различные log-файлы. По умолчанию используются log-файлы, которые являются стандартными для операционных систем семейства unix и log-файлы самых распространенных программных продуктов систем этого семейства.

Вот полный перечень используемых SIEM системой файлов логов:

- /var/log/syslog(/var/log/messages) - содержит глобальный системный журнал, в котором пишутся сообщения с момента запуска системы, от ядра Linux, различных служб, обнаруженных устройствах, сетевых интерфейсов и много другого;

- /var/log/auth.log(/var/log/secure) — информация об авторизации пользователей, включая удачные и неудачные попытки входа в систему, а также задействованные механизмы аутентификации;

- /var/log/dmesg — драйвера устройств;

- /var/log/cron — Отчет службы crond об исполняемых командах и сообщения от самих команд;

- /var/log/faillog — Неудачные попытки входа в систему;

- var/log/kern.log — Журнал содержит сообщения от ядра и предупреждения, которые могут быть полезны при устранении ошибок пользовательских модулей встроенных в ядро;

- /var/log/lastlog — Последняя сессия пользователей;

- /var/log/httpd/(/var/log/apache2/) — Лог веб сервера Apache, журнал доступа находится в access_log, а ошибки — в error_log.

Как уже было сказано выше, в модуль агрегации встроена возможность добавления своих файлов логов для сбора информации из них. В отличие от стандартного расширения функционала, данная возможность предусматривает добавление дополнительных лог файлов без написания кода и является инструментов пользователя разработанной системы мониторинга и управления событиями информационной безопасности. Для этого предусмотрен специальный конфигурационный файл aggr.json, в котором при помощи

несложного синтаксиса можно указать log-файл для сбора информации, и саму информацию, которую нужно агрегировать при помощи регулярных выражений. В результате будет создан JSON-файл для модуля корреляции.

Примерный синтаксис конфигурационного файла представлен на рисунке 3.3.

```
{
    “one-config”:{
        “result-json”:”apache2.json”,
        “parent-node”:”requests”,
        “key-regexp”:” \d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}”,
        “type-node”:”object”,
        “inner-cell”:{
            “type-node”: “string”,
            “key-value”:”time”,
            “parameter-regexp”:” \d{4}:\d{2}:\d{2}:\d{2}”,
            “and-cell”:{
                “type-node”:”string”,
                “key-value”:”path”,
                “parameter-regexp”:” (?:\s)\/.*(?:\sH)”,
                “and-cell”:{
                    “type-node”:”string”,
                    “key-value”:”response code”,
                    “parameter-regexp”:” (?:\”\s)\d{3}(?:\s)”
                }
            }
        }
    }
```

Рисунок 3.3 - Примерный синтаксис конфигурационного файла

После рассмотрения устройства и принципов работы модуля агрегации следует привести общую схему спроектированного модуля, представленную на рисунке 3.4.

Рисунок 3.4 - Структурная схема модуля агрегации

Как можно заметить по схеме, представленной выше, модуль агрегации также использует модуль для работы с JSON файлами. JSON модуль также является разработанным вручную, о нем и о других модулях, напрямую не относящихся к SIEM речь пойдет в конце раздела.

3.3 Корреляция общей структуры системы аудита информационной безопасности

Корреляция – это один из основных терминов теории вероятности, показывающий меру зависимости между двумя и более случайными величинами.

Корреляция применительно к SIEM-системам, это сопоставление различных признаков некоторому симптому, который является событием информационной безопасности.

Существуют сигнатурные (rule based) и бессигнатурные методы корреляции. Сигнатурные — те, в которые человек должен добавить некие правила определения инцидентов. Бессигнатурные — черный ящик, который сам отличает хорошее от плохого.

На практике применяются следующие:

- Statistical — сложный бессигнатурный метод корреляции событий, основанный на измерении двух или более переменных и вычислении степе-ни статистической связи между ними;

- RBR Rule-based (pattern based) (HP ECS, IMPACT, RuleCore) — метод, в котором взаимосвязи между событиями определяются аналитиками в заранее заданных специфических правилах;

- CBR Codebook (case) based (SMARTS). Корреляция производится по подходящим векторам из предварительно заданной матрицы событий;

- MBR model based reasoning (слишком большой MTTR) — метод основан на абстракции объектов и наблюдения за ними в рамках модели;

- Bayesian (BDR) — это, надо полагать, всем известный метод, не требующий особых разъяснений. На практике — неэффективен.

- NMBR — Normalized model based reasoning. Схож с MBR, известен как baseline;

- Graph based. Корреляция заключается в поиске зависимостей между системными компонентами (network devices, hosts, services) и построении графа на их основе;

- Neural network based — идеологический метод. Нейронная сеть обучается для обнаружения аномалий в потоке событий.

В разрабатываемой SIEM-системе применяется Graph based подход. Особенностью разрабатываемого модуля корреляции является сопоставление событий информационной безопасности симптомам векторов атак APT-группировок. Таким образом, можно проследить конкретный тип атаки на информационную систему.

В общем случае работа модуля корреляции сводится к тому, чтобы собрать информацию с подготовленных JSON-файлов логов и принять решение о наличии зависимости между событиями информационной безопасности, если такая зависимость есть, то уведомить администратора информационной безопасности о наличии инцидента ИБ.

Структура модуля корреляции похожа на структуру модуля агрегации. Модуль корреляции также состоит из совокупности классов, унаследованных от общего класса, реализующего интерфейс корреляции. В данном модуле это также сделано для возможности масштабировать весь проект путем добавления корреляции по новым признакам или дополнением правил корреляции по уже существующим.

Ниже, на рисунке 3.5, представлена UML-диаграмма классов модуля корреляции.

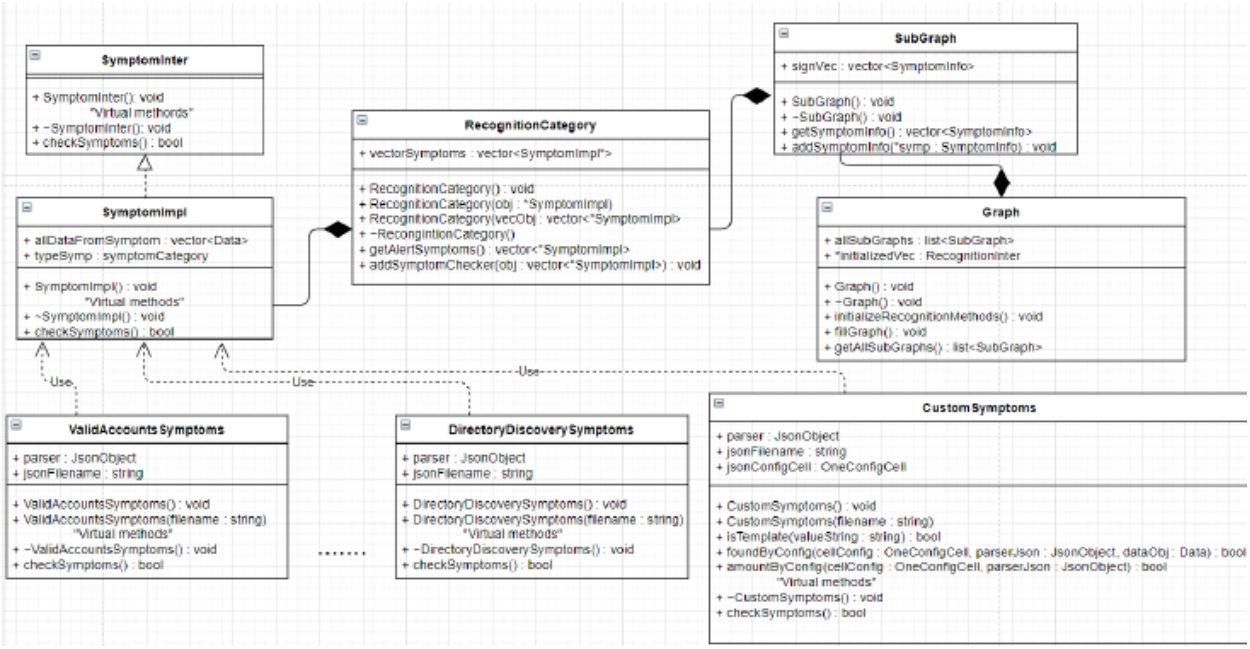


Рисунок 3.5 - UML-диаграмма классов модуля корреляции

На диаграмме видно, что над модулем корреляции спроектирован модуль-обертка, который принимает классы обнаруженных признаков и на их основе строит структуру данных, известную, как граф.

Более подробно работа модуля корреляции выглядит так:

- получение информации из json-файлов логов – на данном этапе происходит загрузка содержимого json-логов в оперативную память для дальнейшего использования в алгоритме поиска зависимостей;

- проверка наличия симптомов событий информационной безопасности в содержимом загруженных json-логов;

- при обнаружении события информационной безопасности, информация о найденном событии иб помещается в специальный контейнер, который представляет из себя вершину будущего графа найденных симптомов;

- после обнаружения всех симптомов, осуществляется поиск зависимостей между найденными симптомами на основании схожести найденной информации и приоритете отдельных записей о событии информационной безопасности;

- при обнаружении зависимостей между несколькими симптомами модуль корреляции формирует уведомление об обнаружении инцидента ИБ и сохраняет найденную информацию в файле результата работы.

Возможность добавления пользовательских условий корреляции позволяет внедрить в SIEM-систему поиск абсолютно любых симптомов и возможность их корреляции, как со стандартными симптомами целевых атак кибер-группировок, так и с другими пользовательскими симптомами.

Общая схема модуля корреляции представлена на рисунке 3.6.

По структурной схеме, представленной выше можно заметить, что для полноценной работы основной части модуля корреляции необходимо обращаться к модулю JSON, а также формировать граф событий ИБ. Сам граф и совокупность составляющих его подграфов, представляют собой отдельные классы, в которые инкапсулированы алгоритмы поиска взаимосвязей между обнаруженными событиями информационной безопасности.

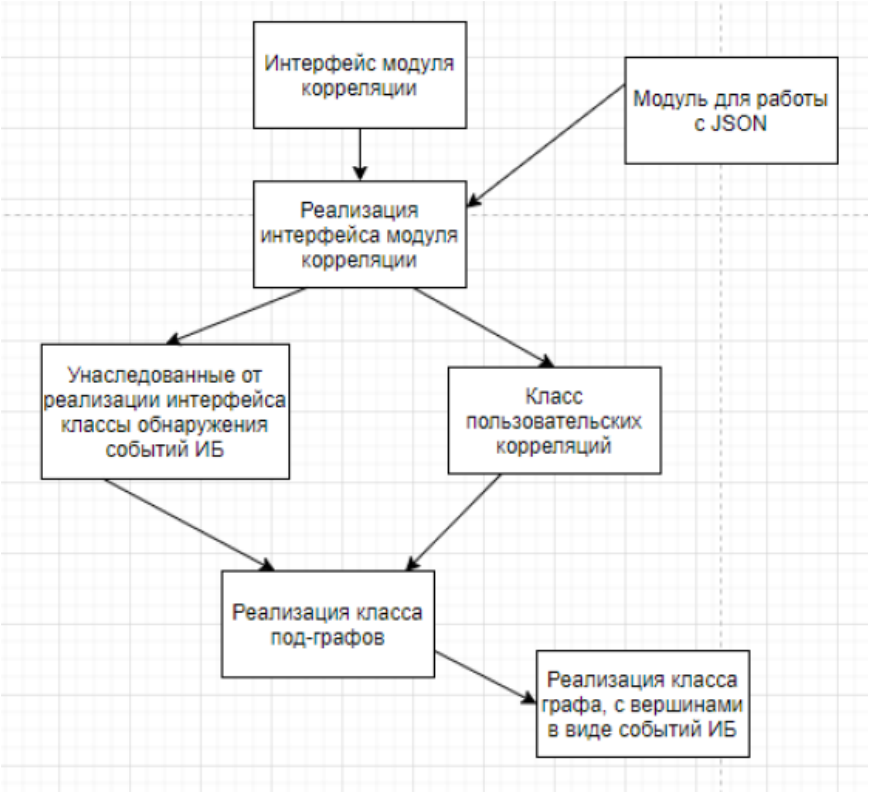


Рисунок 3.6 - Структурная схема модуля корреляции

Сам алгоритм поиска взаимосвязей между признаками реализовано в классе RecognitionCategory, представленном на UML-диаграмме.

Возможность предсказать дальнейшие действия злоумышленника, может помочь принять эффективные контрмеры для того, чтобы смягчить последствия атаки или полностью ее предотвратить. Для этого в разрабатываемую SIEM-систему был добавлен модуль прогнозирования.

Созданный модуль работает на основе собранной о симптомах информации и базы данных MITRE | ATT&CK. После того, как модуль корреляции завершит построение графа симптомов и сформирует уведомление о соответствующем инциденте информационной безопасности, модуль прогнозирования начнет проверку найденных признаков из вектора атаки, построенного на основе графа симптомов. Каждому найденному событию информационной безопасности присваивается категория симптома из базы данных MITRE, далее идет проверка на совпадение со всеми занесенными в

базу данных MITRE | ATT&CK векторами атак. После проверки формируется предупреждение о наиболее вероятном типе целевой атаки. Если найденные симптомы относятся к нескольким атакам, то формируется сообщение о каждой из них. Так как все симптомы каждой из атак уже исследованы и занесены в базу данных MITRE, то нетрудно выяснить дальнейшее развитие атаки по уже обнаруженным при-знакам.

Схематичное представление обнаруженных симптомов и прогнозирования дальнейшего развития целевой атаки APT1 представлено на рисунке 3.7.

Рисунок 3.7 - Схематичное представление атак APT1 и APT3

Как можно заметить по изображению выше, прогнозирование дальнейших действий не связано с какой-то одной атакой, оно, при прочих равных, относится и к другим целевым атакам, большинство признаков которых было обнаружено в ходе корреляции.

Структурно, модуль прогнозирования представляет собой один класс, который принимает на вход подграф обнаруженных симптомов и сверяет их с информацией из файла, в котором содержаться признаки APT-атак, и на выходе возвращает вектор, состоящий из типов атак и соответствующих им вариантов развития атаки. UML-диаграмма модуля прогнозирования представлена на рисунке 3.8.

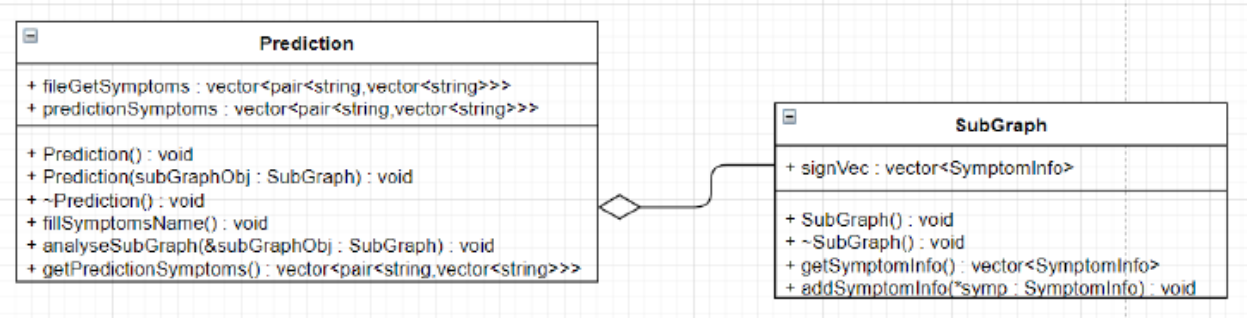


Рисунок 3.8 – UML-диаграмма классов модуля прогнозирования

Общая схема модуля прогнозирования представлена на рисунке 3.9.

Рисунок 3.9 - Структурная схема модуля корреляции

На схеме выше видно, что модуль прогнозирования, также как и остальные модули SIEM-системы включается в основной модуль программы, куда и возвращает результат своей работы.

Как можно было заметить по схемам, приведенным выше, в SIEM-систему помимо основных модулей также встроены и вспомогательные модули, выполняющие утилитарные для работы остальных модулей функции. Такими модулями являются JSON-модуль и модуль для работы с представлением времени.

Глава 4 Тестирование разработанной технологии внутреннего аудита информационной безопасности компании ТОО «KARCHER» и анализ результатов тестирования

4.1 Этапы работы SIEM системы

После описания работы всех модулей, следует рассмотреть их работу в комплексе, а также описать некоторые аспекты работы каждого из модулей отдельно.

Условно алгоритм работы всей SIEM системы можно разделить на следующие несколько этапов:

- обход и сбор информации со стандартных системных log-файлов, формирование результатов сбора информации в соответствующие json-файлы;
- обход и сбор информации с log-файлов, по прописанным в конфигурационном файле правил агрегации информации;
- поиск событий информационной безопасности в сформированных log-файлах;
- построение графа симптомов на основе найденных событий информационной безопасности;
- поиск взаимосвязи между симптомами;
- формирование уведомления о возможном инциденте информационной безопасности;
- прогнозирование дальнейших возможных действий злоумышленника и уведомление о типе атаки/атак.

Схема алгоритма представлена в Приложении Б.

В модуле корреляции разработанной SIEM-системы используется graph-based метод корреляции. На практике это означает, что во время работы модуля корреляции будет формироваться граф из обнаруженных событий информационной безопасности. В сформированном графе сами симптомы будут являться вершинами, а взаимосвязи между ними – ребрами.

Подход с графами удобен тем, что можно быстро, относительно полного перебора, найти взаимосвязь между двумя симптомами. Для этого используется такой алгоритм поиска в графах, как поиск в глубину.

Поиск в глубину — один из методов обхода графа. Стратегия поиска в глубину, как и следует из названия, состоит в том, чтобы идти «вглубь» графа, насколько это возможно. Алгоритм поиска описывается рекурсивно: перебираем все исходящие из рассматриваемой вершины ребра. Если ребро ведет в вершину, которая не была рассмотрена ранее, то запускаем алгоритм от этой нерассмотренной вершины, а после возвращаемся и продолжаем перебирать ребра. Возврат происходит в том случае, если в рассматриваемой вершине не осталось ребер, которые ведут в нерассмотренную вершину.

Скорость работы алгоритма поиска в глубину в среднем равна O(E + V), где E – количество вершин графа, а V – количество ребер между всеми вершинами.

Для сравнения полный перебор для нахождения взаимосвязи одной вершины с другой занял бы O(n * m), если представить совокупность вершин в виде матрицы со сторонами n и m. Для поиска взаимосвязи для каждой вершины, полный перебор уже будет занимать в среднем O(n^2 * (n*m)) = O(m * n^5), в то время как для выявления взаимосвязей между симптомами, применяя алгоритм поиска в глубину, в среднем будет потрачено O(n^3 + m * n^2).

После формирования уведомления о возможном инциденте, модуль корреляции формирует вектор взаимосвязанных симптомов и передает его модулю прогнозирования. Модуль прогнозирования, в свою очередь, получает данный вектор, извлекает из него симптомы и сопоставляет их с симптомами из матрицы признаков атак группировок APT. Сопоставляю симптомы, модуль прогнозирования пытается выяснить наиболее вероятный тип атаки. Расчет вероятности происходит достаточно тривиальным способом, а именно расчетом отношения числа обнаруженных симптомов к числу симптомов конкретной атаки. После вычисления наиболее вероятного типа атаки, из базы данных

признаков собираются оставшиеся, еще не обнаруженные симптомы и информация о них выводится в соответствующем уведомлении пользователю.

Подход к алгоритмизации, описанный в этом разделе позволяет SIEM-системе достаточно быстро исполнять свои функции. С одной стороны можно заключить, что поиск взаимосвязей при помощи простых алгоритмов на графах довольно простым, с другой, такой выбор упрощает разработку и является достаточно надежным. К примеру, можно было бы повысить степень обнаружение взаимосвязей между событиями ИБ при помощи нейронной сети, но такое решение будет намного сложнее в проектировании и внедрение и развертывание его в конкретную организацию потребует довольно большого времени, так как нейронную сеть необходимо обучать и адаптировать под конкретную организацию. Исходя из этого, можно заключить, что алгоритм поиска взаимосвязей на графах является оптимальным для поставленных в проекте задач.

4.2 Имитационное моделирование обнаружения атак

После стадии разработки необходимо проверить работоспособность спроектированной SIEM-системы, а именно возможности обнаружения целевой атаки, способности указать тип атаки и оценить возможные дальнейшие действия злоумышленника.

Для имитационного моделирования, была выбрана имитация атаки APT41.

APT41 – это спонсируемая Китаем группировка, занимающаяся шпионажем и атаками на отрасли в сфере здравоохранения, телекоммуникаций, технологий и видеоигр в 14 странах.

Для проверки обнаружения атаки APT41 и прогнозирования дальнейших действий, связанных с этой атакой необходимо подготовить соответствующие log-файлы, в которых помимо симптомов атаки также будут содержаться записи о действиях легитимных пользователей.

Для моделирования атаки будут использованы следующие симптомы, являющиеся частью атаки APT41:

- External Remote Services;
- Valid Accounts;
- Command-line Interface;
- Create Accounts;
- Clear Command History;
- Brute Force;
- File Deletion;
- System Network Configuration Discovery;
- Network Service Scanning;
- System Owner/User Discovery;
- System Network Connections Discovery;
- Data compressed.

Признаки симптома External Remote Services, Valid Accounts находятся в log-файле auth.log. Информацию о симптомах Command-line Interface, Create Accounts, File Deletion, Data Compressed, System Network Connections Discovery, System Owner/User Discovery, System Network Configuration Discovery можно найти в файлах .bash_history пользователей и файле .bash_history администратора. При отсутствии таковых файлов или установке того факта, что они были очищены, можно утверждать о наличии такого признака APT атаки, как Clear Command History. Информацию о признаке Brute Force можно найти, как в файле auth.log так и в файле secure.log.

Само моделирование атаки происходило в операционной системе Debian GNU/Linux 9 (stretch), с версией ядра 4.9.0-12.

После моделирования атаки и действий легитимных пользователей операционной системы, запустим разработанную SIEM-систему для анализа log-файлов и поиска в них признаков смоделированной атаки. Рисунки 4.1 – 4.3 иллюстрируют результаты анализа log-файлов SIEM-системой.

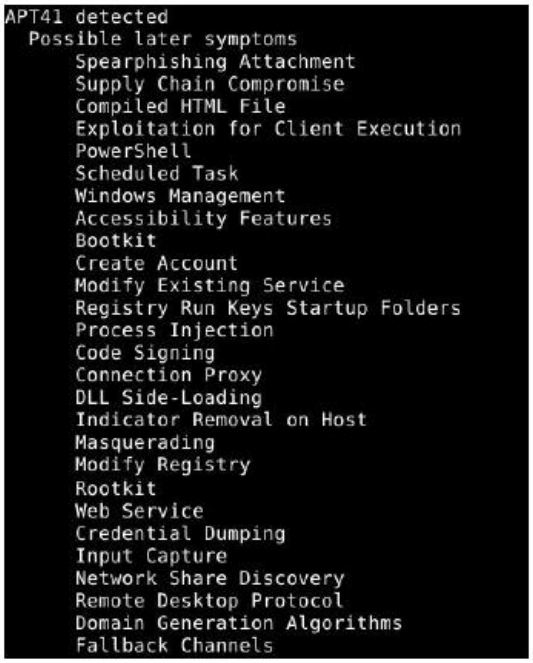


Рисунок 4.1 - Уведомление об обнаруженной атаке APT41 и прогнозирование дальнейших действий злоумышленника

Рисунок 4.2 - Уведомление об обнаруженной атаке APT32 и прогнозирование дальнейших действий злоумышленника

4.3 Имитационное моделирование построения вектора уже обнаруженных атак

Как можно заметить, результаты работы модуля прогнозирования иллюстрируют признаки APT41 и APT32, которые могут появиться при дальнейшем развитии текущей атаки.

Ниже представлены скриншоты результатов построения вектора уже обнаруженных признаков развития атаки.

```
One sub graph
  One symptom
      Time: 2020/5/20/0:43:0
      Category: files_and_directory_discovery
      Information: 291.235.112.122
  One symptom
      Time: 0/0/0/0:0:0
      Category: network_service_scanning
      Information: 291.235.112.122
      Information: 78.12.281.112
  One symptom
      Time: 2019/12/5/01:02:35
      Category: brute_force
      Information: 291.235.112.122
      Information: Denis
  One symptom
      Time: 2019/12/5/01:15:30
      Category: external_remote_service
      Information: 291.235.112.122
      Information: Denis
  One symptom
      Time: 2019/12/5/01:15:32
      Category: valid_accounts
      Information: 291.235.112.122
      Information: Denis
  One symptom
      Time: 2019/12/5/01:15:32
      Category: command_line_interface
      Information: Denis
      Information: bash
  One symptom
      Time: 0/0/0/0:0:0
      Category: system_owner_user_discovery
      Information: Denis
      Information: who
      Information: args:
  One symptom
      Time: 0/0/0/0:0:0
      Category: system_network_connections_discovery
      Information: Denis
      Information: lsof
      Information: args: -U | head -5
```

Рисунок 4.3 - Первая часть графа обнаруженных признаков атаки

Как можно заметить по рисункам выше, SIEM-система обнаружила все смоделированные автором симптомы, и построила на их основе вектор атаки.

Следует обратить внимание, что разработанная система мониторинга и управления событиями ИБ обнаруживает атаку при нахождении взаимосвязи между определенным количеством событий ИБ. Это количество зависит от приоритета для каждого из событий, например, если двух признаков выставлен высокий приоритет, то при нахождении взаимосвязи даже между ними, будет сформировано уведомление о целевой атаке.

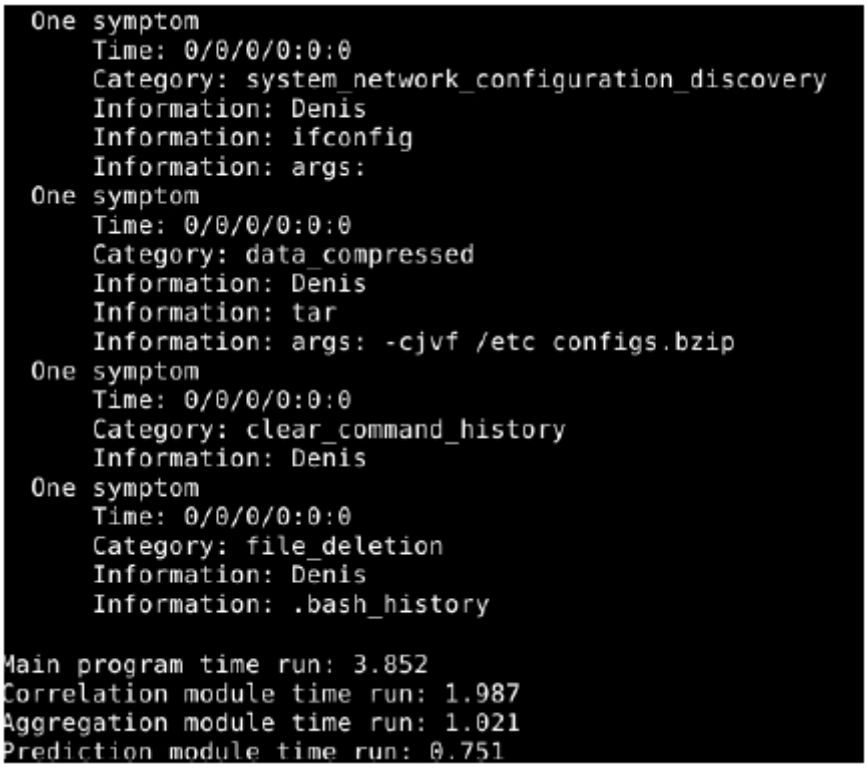


Рисунок 4.4 - Вторая часть графа обнаруженных признаков атаки

И наоборот, если у событий выставлен низший приоритет, то, потребуется найти взаимосвязь между множеством событий, чтобы сформировать уведомление о возможном инциденте информационной безопасности.

4.4 Оценка эффективности SIEM-системы

Перед подведением итогов всего проекта, следует оценить эффективность разработанной SIEM-системы, это позволит сделать более полные и построенные на фактах выводы.

Как уже был сказано выше, разработанная SIEM-система обнаружила все из смоделированных симптомов, успешно сформировал уведомление о наличие атаки APT41. Также было сформированы уведомление о дальнейшем развитии этой и других атак.

Программа отработала за 3.852 секунды.

Графически, время работы каждого из модулей представлено на рисунке 4.5.

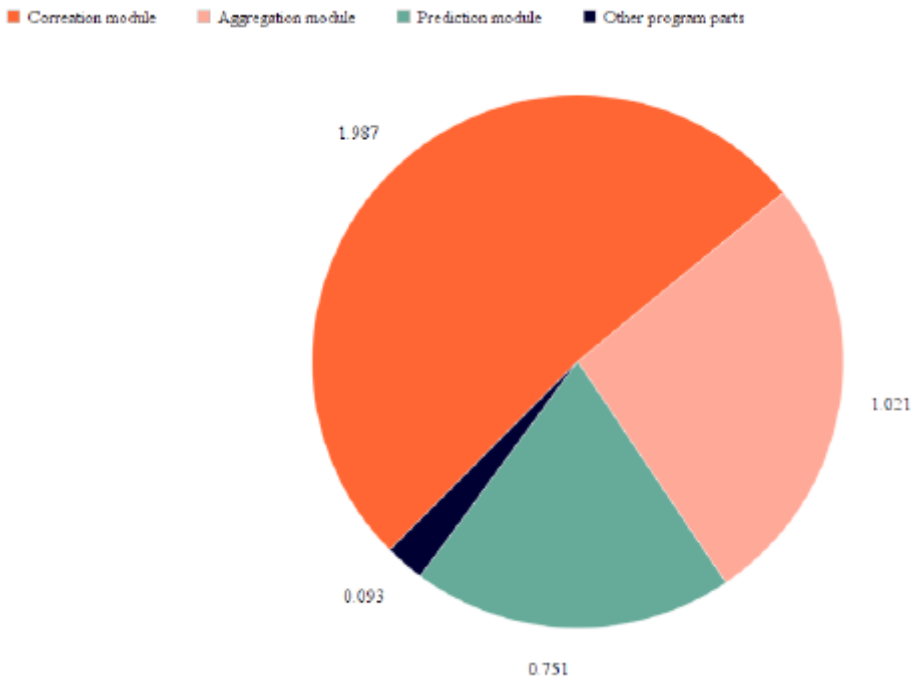


Рисунок 4.5 - Диаграмма времени выполнения модулей SIEM-системы

На диаграмме можно увидеть, что время работы модуля корреляции почти вдвое больше, чем время работы модуля агрегации и почти втрое больше работы модуля прогнозирования. Стоит заметить, что при увеличении размера графа обнаруженных событий информационной безопасности, разрыв по времени работы между модулем корреляции и модулями агрегации и

прогнозирования будет увеличиваться, из-за алгоритма поиска взаимосвязей между событиями информационной безопасности.

Таким образом, разработка и внедрение специализированной системы внутреннего аудита информационной безопасности может способствовать повышение общего уровня защищенности на предприятии, за счет обнаружения отдельных событий информационной безопасности и поиска взаимосвязей между ними.

По результатам имитационного моделирования и оценки эффективности, можно сделать вывод об успешном выполнении SIEM-системой всех возложенных на нее функций. Более того, применяя разработанную SIEM-систему, можно существенно сократить потребление программных и аппаратных ресурсов на защиту информационной системы. Это позволит либо сократить расходы на потреблении ресурсов, либо внедрить дополнительный уровень защиты, повысив общий уровень защищенности всей информационной системы.

Заключение

В качестве объекта исследования в работе выступает компания ТОО «KARCHER». Информационную систему компании включают, в основном, данные о перевозимых грузах, схемах перевозок, перевозимом товаре. Учет всей входной информации осуществляется с помощью ряда компонентов – программ.

Основной целью проведения внутреннего аудита информационной безопасности компании является определение перечня возможных угроз предприятия. Выделяют два типа нарушителей: внутренние и внешние. Для оценки угроз применяется система уровней защищенности.

В целях проведения аудита информационной безопасности сетевой инфраструктуры осуществляется сбор и анализ большого массива данных за определенный период времени. Так же требуется периодически осуществлять повторение процедур сбора и анализа сетевых данных для более полного представления о возможных проблемах в сети.

Наиболее распространенной системой внутреннего аудита выступает система типа SIEM (Security information and event management), которые позволяют осуществлять процедуры аудита сетевой инфраструктуры в процессе ее эксплуатации непрерывно. Целью данного типа аудита является определение того, на сколько сетевая инфраструктура соответствует предъявляемым к ней требованиям информационной безопасности (ИБ). Таким образом определяется так же уровень защищённости информационных сетевых компонентов корпоративной информационной системы (КИС) предприятия.

Формирование и применение при проведении аудита ИБ оценки соответствия для защитных мер и оценки возможности для процессов управления ИБ создаст наиболее адекватные информационные потребности для улучшения и совершенствования ИБ объекта.

Разработка и внедрение специализированной системы внутреннего аудита информационной безопасности может способствовать повышение общего

уровня защищенности на предприятии, за счет обнаружения отдельных событий информационной безопасности и поиска взаимосвязей между ними.

Помимо этого, успешное решение задачи разработки SIEM-системы с учетом векторов кибератак позволяет помимо самого факта обнаружения взаимосвязей между событиями информационной безопасности, сопоставить эти события признакам целевых атак и спрогнозировать дальнейшее развитие таких атак. Такой подход существенно ускоряет ответные действия, направленные на локализацию ущерба от атаки и блокирование дальнейшего ее развития.

По результатам имитационного моделирования и оценки эффективности, можно сделать вывод об успешном выполнении SIEM-системой всех возложенных на нее функций. Более того, применяя разработанную SIEM-систему, можно существенно сократить потребление программных и аппаратных ресурсов на защиту информационной системы. Это позволит либо сократить расходы на потреблении ресурсов, либо внедрить дополнительный уровень защиты, повысив общий уровень защищенности всей информационной системы.

Список используемых источников

1. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения
2. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных от 14.02.2008.
3. Методика определения угроз безопасности информации в информационных системах, проект 2015 г
4. Аджиева А.И., Тхагапсова С.К.Г. Роль внутреннего аудита в системе экономической безопасности предприятия // Естественно-гуманитарные исследования. - 2020. - № 31 (5). - С. 322-325.
5. Афанасьев А.Д., Маринов А.А. Методика построение практического занятия в виде деловой игры для дисциплины «аудит информационной безопасности» // Современные проблемы профессионального образования: опыт и пути решения. - 2020. - С. 43-46.
6. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных от 15.02.2008.
7. Баранова А.Е. Цифровизация аудита информационной безопасности бухгалтерии в страховом бизнесе // XCII МЕЖДУНАРОДНЫЕ НАУЧНЫЕ ЧТЕНИЯ (ПАМЯТИ П.П. ЛАЗАРЕВА). - 2020. С. 10-14.
8. Борубаев М.Ч., Омурзаков Т.У., Джапаров А.А. Применение метода тестирования при проведении внутреннего аудита информационной безопасности // Современные проблемы механики. - 2019. - № 38 (4). - С. 39-45.
9. Бойченко О.В. Аудит защищенности данных в политике информационной безопасности предприятия // Проблемы информационной безопасности. - 2020. - С. 3-6.
10. Вакуленко А.А. Аудит информационной безопасности предприятия // Стратегии и инструменты управления экономикой: отраслевой и региональный аспект. - 2019. - № 7. - С. 218-223.

11. Вакуленко А.А. Аудит информационной безопасности предприятия // Стратегии и инструменты управления экономикой: отраслевой и региональный аспект. - 2019. - № 8. - С. 218-223.

12. Великанова Л.О., Luís De.S.C. Методические подходы к оценке рисков информационной безопасности организации при проведении финансового аудита // Институциональные преобразования АПК России в условиях глобальных вызовов. - 2020. - С. 58-59.

13. Глеске Д.О. Понятие аудита информационной безопасности // Вестник научных конференций. - 2020. - № 11-4 (63). - С. 26-27.

14. Гулак М.Л., Рытов М.Ю., Голембиовская О.М. Аудит информационной безопасности. Прикладная статистика: учебное пособие / Москва, 2020. – 455 с.

15. Еломанов И.Д. Научно-методическое обеспечение аудита информационной безопасности информационных систем // Радиоэлектроника, электротехника и энергетика. Тезисы докладов. - 2020. - С. 319.

16. Ермаков А.С. Концепция аудита сложных сигналов при проведении мероприятий по аттестации информационных систем по требованиям безопасности информации // Фундаментальные проблемы информационной безопасности в условиях цифровой трансформации. - 2020. - С. 149-154.

17. Курбатов А.М. Методы и средства аудита сетевой безопасности корпоративных информационных систем малых и средних производственных предприятий // Радиоэлектроника, электротехника и энергетика. Тезисы докладов. - 2020. - С. 327.

18. Ложкова А.А. Аудит информационной безопасности на предприятии // МОЛОДЕЖЬ XXI ВЕКА: ШАГ В БУДУЩЕЕ. - 2020. - № 5. - С. 120-121.

19. Палканов И.С., Рачков В.Е. Внутренний аудит информационной безопасности как инструмент получения объективных оценок состояния информационной безопасности организации // Студенческая наука для развития информационного общества. - 2019. - № 7. - С. 153-161.

20. Петренко С.А., Курбатов В.А., Петренко А.С. Автоматизация аудита информационной безопасности на основе sap etd // The 2019 Symposium on Cybersecurity of the Digital Economy - CDE'19. - 2019. - С. 228-234. 2

21. Погудин А.А., Салита Д.С. Аудит информационной безопасности предприятия и его основные этапы // Проблемы правовой и технической защиты информации. - 2020. - №9. - С. 31-33.

22. Подтопельный В.В. Сравнительный анализ технологий аудита информационной безопасности сетевой инфраструктуры диспетчерского уровня АСУТП // Балтийский морской форум. - 2020. - № 7. - С. 306-311.

23. Самарин А. Аудит информационной безопасности ico проекта // Системный администратор. - 2019. - № 5 (198). - С. 42-47.

24. Смирнов Г.Е., Макаренко С.И. Актуальные вопросы развития теории и практики аудита информационной безопасности // Фундаментальные проблемы информационной безопасности в условиях цифровой трансформации- 2020. - № 7. - С. 192-197.

25. Стандарт Банка России СТО БР ИББС-1.3-2016 “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Сбор и анализ технических данных при реагировании на инциденты информационной безопасности при осуществлении переводов денежных средств” (принят и введен в действие приказом ЦБР от 30 ноября 2016 г. № ОД-4234).

26. Сучалкина Е.А. Роль аудита в системе экономической безопасности предприятия // Актуальные проблемы менеджмента, экономики и экономической безопасности. - 2020. - №8. - С. 228-231.

27. Финтисов М.И. Аудит информационной безопасности в организации // Новые направления научной мысли. - 2017. - С. 58-60.

28. Хубиева З.Б. Аудит информационной безопасности – основа эффективной защиты предприятия // Актуальные проблемы развития аудита и финансового консалтинга в России. - 2017. - С. 121-125.

29. Чекулаева Е.Н., Кубашева Е.С. Методика аудита информационной безопасности предприятия с использованием причинно-следственной диаграммы // Вестник Поволжского государственного технологического университета. - 2020. - № 1 (45). - С. 58-68.

30. Шин С.А. Взаимосвязь информационной безопасности и внутреннего аудита компании: региональное исследование // Вестник Атырауского Университета имени Х.Досмухамедова. - 2019. - № 4. - С. 158-167.

31. Шистко Н.Е., Великанова Л.О. Оценка рисков информационной безопасности организации при проведении финансового аудита // Цифровизация экономики: направления, методы, инструменты. - 2020.С. 92-96.

32. 802.3.2-2019 - IEEE Standard for Ethernet - YANG Data Model Definitions. – URL: http://www.ieee802.org/3/ (дата обращения 16.02.2021).

33. About the BSIMM. [Электронный ресурс] URL: https://www.bsimm.com/about.html (дата обращения 01.12.2020).

34. Andrew Hay, Daniel Cid OSSEC Host-Based Intrusion Detection Guide/ Hay A. URL: http://index-of.co.uk/Hacking-Coleccion/OSSEC%20Host-Based%20Intrusion%20Detection%20Guide.pdf (Дата обращения: 5.02.2021).

35. Neomatica [Электронный ресурс]. – URL: https://www.neomatica.com/

36. OWASP. [Электронный ресурс] URL: https://ru.wikipedia.org/wiki/OWASP (дата обращения: 01.12.2020).

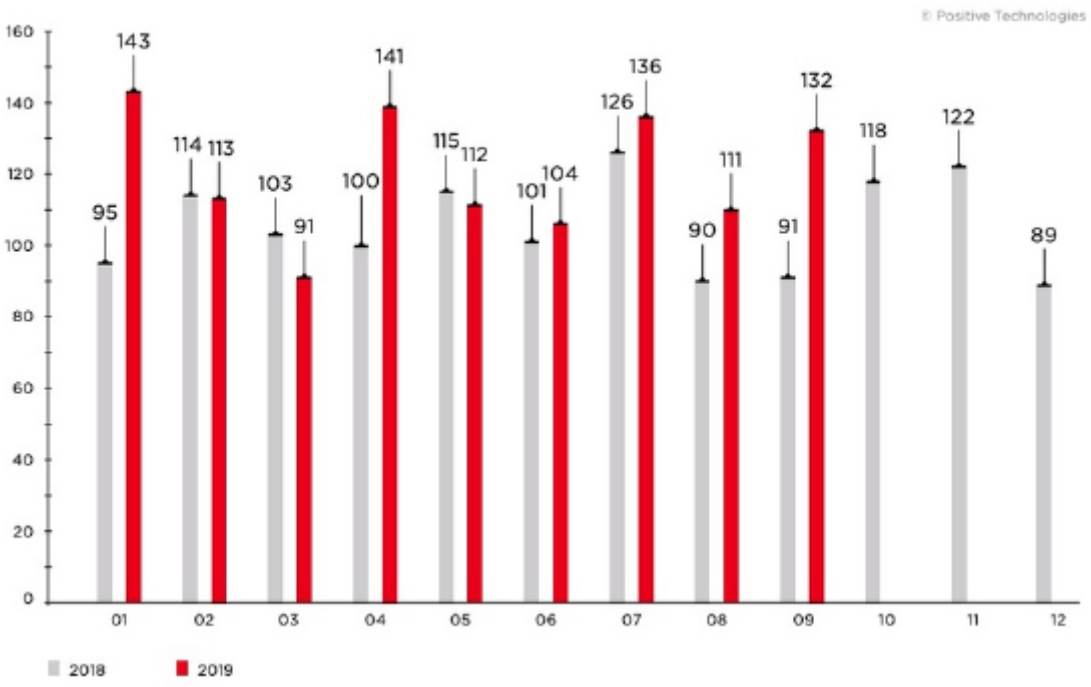
37. Scikit-learn: Библиотека машинного обучения для языка программирования Python [Элек-тронный ресурс]. – 2020. – URL: https://scikit-learn.org/stable/user_guide.html (дата обращения 17.02.2021).

38. Software Assurance Maturity Model. [Электронный ресурс] URL: https://www.opensamm.org/ (дата обращения 01.12.2020).

39. T. Hastie; R. Tibshirani; J. Friedman. The Elements of Statistical Learning – Stanford: Springer, 2018. – 764 с.

40. Годовой отчет ТОО «KARCHER» за 2020 год

Приложение А Статистика роста целевых атак



Приложение Б Блок-схема алгоритма работы программы