Санкт-Петербургский государственный университет
Экономический факультет
Кафедра информационных систем в экономике

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

По направлению 080500 – «Бизнес-информатика»

РАЗРАБОТКА МОДУЛЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ ДЛЯ АНАЛИЗА И ПРЕДОТВРАЩЕНИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Выполнил:
Бакалавриант 4 курса
Кулаков Александр Сергеевич
_____/_____/
Научный руководитель:
Ассистент
Салтан Андрей Анатольевич,
_____/_____/

Санкт-Петербург
2016

Оглавление

Введение

Актуальность

Информационные технологии все быстрее и быстрее входят нашу жизнь и охватывают различные области деятельности экономических субъектов, с целью повышения их эффективности. Практически каждое программное решение имеет в себе модуль, отвечающий за ведение журналов, в которых, с разной степенью подробности, регистрируются системные данные.

На сегодняшний день существует достаточно развитый рынок, связанный с оказанием услуг и поставкой товаров, программных средств, в области информационной безопасности. По оценкам аналитического центра TAdviser, объем рынка информационной безопасности в России по итогам 2014 года составил 59 млрд. рублей (TAdviser, 2015).

С другой стороны, согласно статье из аналитического издания в области информационных технологий Computer Weekly, ежегодно по всему миру распространяется пиратское программное обеспечение и вредоносные продукты, позволяющие выполнять сложные атаки на разного вида системы, суммарной стоимостью 2 млрд долларов (Ashford, 2014), что достаточно внушительно.

В независимости от сферы бизнеса и интересов компании, предприятия нуждаются в защите информации, хранящейся в их корпоративных сетях, для достижения которой, требуется выполнение ряда операций, в частности осуществления мониторинга основных событий и инцидентов в системе. В рамках дисциплины информационная безопасность существует отдельное направление - SIEM (Security Information and Event Management), что, в общем виде, представляет собой анализ событийной информации, поступающей из различных подсистем, модулей, в рамках всей системы информационной безопасности и дальнейшего выявления отклонений от норм по каким-либо заранее определённым критериям.

SIEM-системы существуют уже почти 10 лет, но их активное продвижение и развитие началось лишь в последние годы, в большей степени из-за возросшего количества актуальных угроз. (Парфентьев, 2014). Несмотря на внушительный размер рынка SIEM-систем (Дрозд, 2014), по причине широкого разнообразия и высокого уровня спецификации каждой отдельной компании-клиента, разных задач и источников информации для SIEM систем в рамках отдельных предприятий, на данный момент процесс внедрения требует значительных усилий, то есть для каждого отдельного предприятия необходимо разрабатывать отдельный, уникальный модуль, о чем говорят вендоры и компании интеграторы (AltirixSystems, 2015).

Цели и задачи

Основной целью данной работы является разработка модуля информационной системы ИБ, благодаря которому сотрудники компании, занимающиеся анализом и предотвращением угроз в области ИБ, смогут оперативно, в режиме реального времени получать информацию, содержащую статистику о работе системы ИБ, и с помощью которой будут принимать управленческие решения, относительно таких вопросов как: установка новых правил в политике безопасности, обновление ПО, обработка возникших с инцидентов и анализ угроз.

Для достижения цели были поставлены и решены следующие задачи:

- Систематизация походов к организации ИБ на предприятии, с целью выявления основных угроз и возможных вариантов их предотвращения
- Анализ работы системы логирования и структуры формирования лог-файлов шлюза безопасности на базе программного обеспечения компании Check Point, с целью выявления основных полей и структурных особенностей лог-сообщений системы
- Выбор информационной системы для разработки модуля на основе критериев функциональности систем
- Разработка информационной панели (dashboard) для мониторинга работы системы ИБ и принятия управленческих решений, посредством обогащения лог-информации данными из общедоступных БД угроз и сканера уязвимостей в рамках одного модуля

Глава 1. Информационная безопасность

1.1. Понятие информационной и сетевой безопасности

На сегодняшний день существует множество подходов к определению понятия информационной безопасности (Peltier, 2013) и поэтому в различных контекстах данный термин может иметь разный смысл.

Наиболее общим и понятным является определение, используемое в государственном стандарте о защите информации, где под информационной безопасностью или безопасностью информации подразумевается такое состояние информации (данных), при котором обеспечены три основных свойства (Рисунок 1), а именно: конфиденциальность, доступность и целостность, где конфиденциальность – запрет на использование информации третьими лицами, доступность – возможность получения информации некоторому кругу лиц за определенное время, целостность – сохранение логических связей и отсутствие искажений (ГОСТ-50922-2006).

Рисунок 1 - Концепция ИБ

Система мероприятий, целью которых является обеспечение информационной безопасности, называется защитой информации (Кривцов А.Н., 2006). Так же можно сказать, что защита информации это процесс подержания приемлемого уровня риска угрозы, так как не существует такой системы, которая находилась бы в полной безопасности (Vacca, 2013). Представленное в ГОСТе определение является всеобъемлющим и может относится к различным предметным областям как например к

защите информации в СМИ, так и защите цифровой, компьютерной информации. В данной работе подробнее рассматривается вопрос защиты компьютерной информации, а именно сетевой безопасности.

Под сетевой безопасностью понимается соблюдение тех же, что и в определении информационной безопасности требований таких как, свойства конфиденциальности, целостности и доступности, с одним лишь отличием, что все эти требования применяются в большей степени к инфраструктуре компьютерной сети предприятия и политикам работы в ней, при четком соблюдении которых достигается защита ресурсов сети от вредоносного воздействия (Anti-Malware, 2015).

В своей работе Малик утверждает, что, как правило, приемлемый уровень сетевой безопасности достигается при выполнение определенных шагов, каждый из которых направлен на изучение взаимоотношений между атаками и противодействующим им мерами (Malik, 2002):

1. Понимание инфраструктуры сети, то есть того, что нужно защищать
2. Выявление основных типов угроз
3. Оценка вероятности возникновения угрозы и осуществление превентивных мер
4. Мониторинг системы и устранение неполадок

Хотелось бы отметить, что данный подход не является единственным и правильным, существуют и другие подходы (YourPrivateNetwork, 2009), позволяющие достигнуть приемлемый уровень безопасности системы, однако, является наиболее подходящим, для описания рассматриваемой предметной области. Далее подробно рассматриваются отдельные составляющие данного подхода.

1.2. Инфраструктура корпоративной сети

Сетевая инфраструктура небольшой компании с распределённой структурой, в составе которой содержаться различные подразделения, такие как финансовый отдел, отдел кадров, склад, в каждом из которых может работать своя информационная система с различными целями и задачами может иметь следующий вид (см. Рисунок 2).

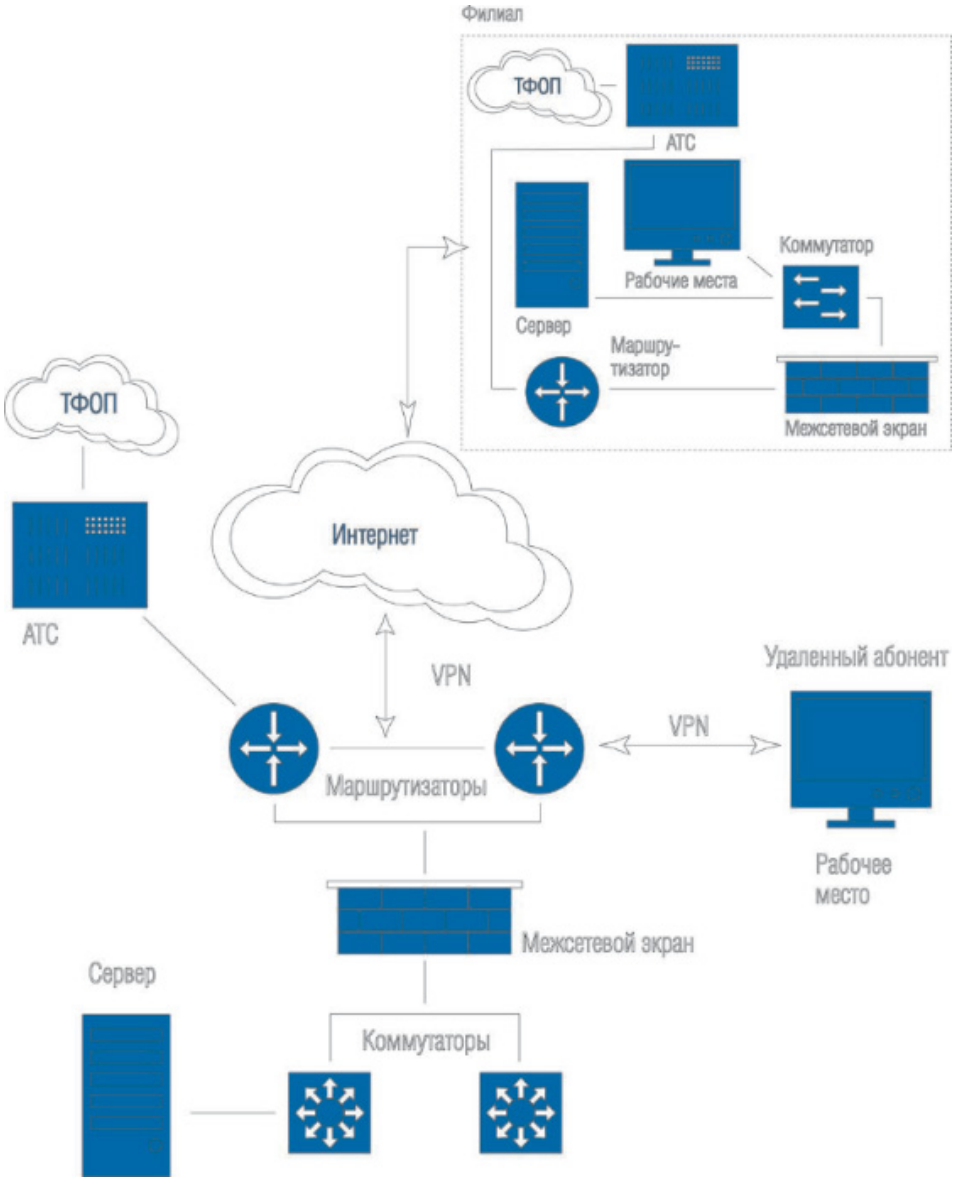


Рисунок 2 – Типовая сетевая инфраструктура малого предприятия[1]

Несмотря на то, что представленная выше схема содержит в себе все основный компоненты корпоративной сети малого предприятия, она не является универсальной и может варьироваться в зависимости от специфики каждой отдельной компании. Данная инфраструктура позволяет выполнять различные операции такие как: содержание в единой

[1] Источник: http://www.atlon.ru/direction/index.php?SECTION_ID=3612

базе данных основных ресурсов компании, использование ip-телефонии, организация удаленного доступа и прочее. Понятно, что угроза безопасности может возникнуть абсолютно на любом участке данной схемы, однако, наибольший интерес, в рамках данного исследования, представляет участок, соединяющий коммутаторы и маршрутизаторы, а именно межсетевой экран, который служит своего рода фильтром, контролирующим, согласно политике безопасности потоки проходящих через него сетевых пакетов.

Несмотря на то, что сегодня, помимо межсетевого экрана, изображенного на предыдущей схеме существует целый ряд других, как программных, так и аппаратных решений в области сетевой безопасности (TAdviser, 2015), в рамках данного исследования рассматривается сетевая инфраструктура, использующая для защиты, в большей степени аппаратные средства, одним из примеров которых является шлюз безопасности (см. Рисунок 3), содержащий различные блейды (самостоятельные модули), подключаемые в зависимости от реальной потребности пользователя в конкретном функционале.

Шлюзы безопасности имеют широкий диапазон производительности, позволяющей обеспечивать безопасность в информационных системах различного размера – от небольшого офиса, удаленного подразделения или филиала до центра обработки и хранения данных или телекоммуникационной компании, а также большой набор дополнительных аксессуаров, позволяющих увеличить их возможности и производительность (Орлов, 2010).

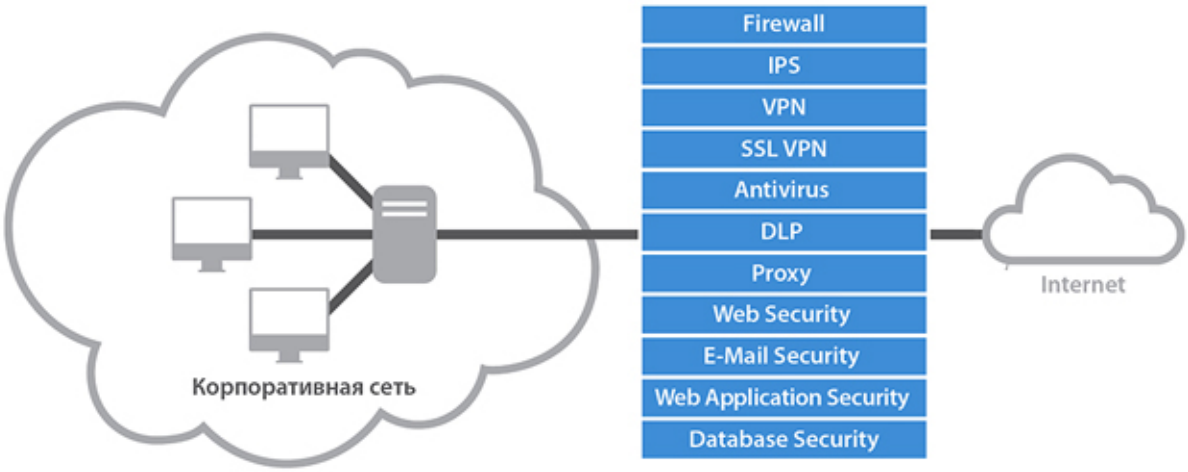


Рисунок 3 – Шлюз безопасности[2]

Сегодня на рынке средств защиты информации, существует много различных предложений от разных компаний по данному типу продуктов от таких производителей как Cisco, Zyxel, Check Point, Huawei, Sophos, Fortinet которые имеют достаточно схожий

[2] Источник: http://security-microtest.ru/resheniya/network-security/utm/

общий функционал (Романов, 2013). В данном исследовании подробно рассматривается функционал и возможности решения, производимого компанией Check Point, которая, согласно исследованию компании Gartner, на протяжении последних лет является одним из лидеров на данном сегменте рынка (Adam Hils, 2015).

1.3. Основные угрозы сетевой безопасности

Для того, чтобы получить понимание как компании выстраивают защиту, какие системы и методы защиты используют, первоначально, согласно, описанному подходу (Malik, 2002) нужно выделить основные угрозы сетевой безопасности.

Из определения информационной безопасности (ГОСТ-50922-2006) следует, что все возможные угрозы можно разделить на три вида: нарушение целостности, доступности или конфиденциальности, что подразумевает довольно широкий спектр угроз в различных областях, как например: потеря информации из-за неправильного хранения данных, сбои и отказы аппаратной части компьютера, некорректная работа программного обеспечения. Перечисленные угрозы являются следствием той или иной случайности, то есть являются угрозами случайного характера. Помимо случайных угроз, существуют и преднамеренные (Лапонина, 2009): внедрение вирусов или вредоносного программного обеспечения, умышленная порча информации или ее полное уничтожение, злоупотребление полномочиям.

Наибольший интерес, в большей степени из-за своей распространённости, представляют неслучайные программные угрозы, которые могут быть систематизированы следующим образом (см. Рисунок 4). Далее подробно рассматриваются основные представители данных классов, их особенности и разновидности.

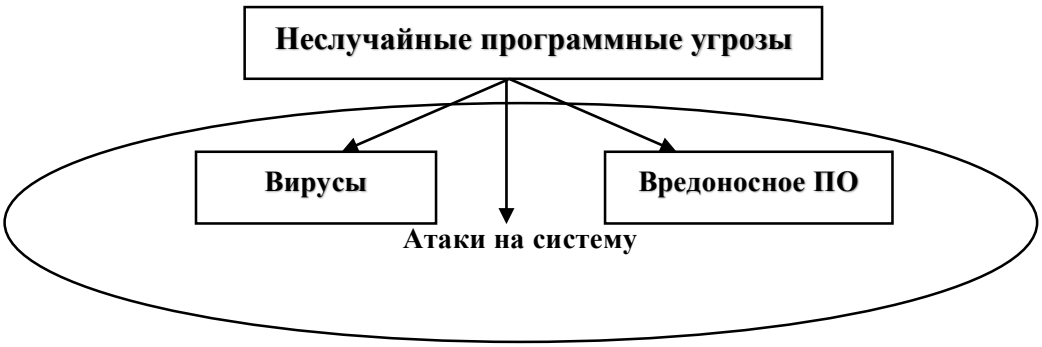


Рисунок 4 – Неслучайные программные угрозы

Компьютерные вирусы

В наши дни существует довольно широкий спектр различных угроз, однако, наиболее известная простому обывателю угроза безопасности – компьютерный вирус.

Разные авторы дают различные определения компьютерного вируса, например, что это *саморазмножающаяся часть кода, который разработан злоумышленниками* (Bruce J. Neubauer, James D. Harris, 2002) или *саморазмножающаяся компьютерная программа, которая распространяется путем присоединения себя к исполняемым файлам или к системным областям на дисках* (Nachenberg, 1997), а некоторые говорят о том, что общепринятого определения вируса не существует (Aycock, 2006).

Исходя из представленных определений, главными особенностями вируса являются такие характеристики как: способность к самовоспроизведению, самостоятельное распространение и нанесение вреда, путем изменения исходного исполняемого кода различных программ и компонентов компьютера.

Существует достаточно много различных вариантов вирусных программ известных на сегодняшний день, каждая из которых имеет свои особенности и определенное предназначение. В основе каждого типа вируса лежит алгоритм, направленный на достижение определенной задачи, так как существуют разные степени угроз и разные пути вредоносного воздействия, к примеру, один тип вируса может нести вред работе электронной почты или почтового клиента, а другой оказывает вредоносное воздействие исключительно на текстовые файлы, содержащиеся в системе. В своей книге М. Людвиг использует следующую классификацию (Ludwig, 1998):

- **Boot Sector Virus –** вирус, действие которого направлено на работу загрузочного диска системы.
- **Directory Virus** вирус, который может изменять название места хранения файла, то есть путь к файлу.
- **Program Virus** вирус, который заражает исполняемые и программные файлы типа «.exe», «.sys», «.dll».
- **Resident Virus** вирус, работающий в оперативной памяти компьютера, он повреждает файлы пока они обрабатываются в оперативной памяти.
- **Multipartite Virus** это сочетание *Directory Virus* и *Program Viruses.* Он, как правило, заражает загрузочный диск системы и при загрузке компьютера начинает заражать файлы в самой системе.
- **Polymorphic Virus** вирус, имеющий возможность изменять свой код.
- **File-deleting Virus** данный вирус предназначен для удаления конкретных файлов, программ (с соответствующими расширениями) или типов документов.
- **Mass Mailers Virus** вирус, заражающий почтовые программы, и рассылающий вирусные письма контактам из адресной книги пользователя.

Вредоносные программы

Сегодня, помимо вирусов, существует ряд других программных средств, которые имеют свои отличительные черты, но, также, как и вирусы, наносят вред пользователю. Эти программы нельзя назвать вирусами, так как некоторые из них, к примеру, не способны к самовоспроизведению или их задачи не предполагают этого. Ниже представлены основные типы программ данного класса (Ludwig, 1998):

- **Logic Bomb –** одна из самых простых разновидностей вредоносных программ, которая состоит всего из двух частей вредоносного кода и логического условия, при выполнении которого запускается вредоносный код.
- **Back Door –** вредоносная программа, которая создана для «обхода» стандартного алгоритма аутентификации.
- **Trojan Horse –** программа, которая выглядит и работает как абсолютно нормальное приложение, но содержит внутри себя вредоносный код, предназначенный для получения доступа к системным папкам, получив который, начинает реализовывать различные сценарии вредоносной деятельности.
- **Worm –** программа, которая работает подобно вирусу. Главным сходством с вирусом является то, что она способна к самовоспроизведению, а главной отличительной особенностью то, что она распространяется по всей компьютерной сети, используя недостатки безопасности.
- **Rabbit –** программа, которая быстро создает многочисленное количество копий самой себя, тем самым ухудшая производительность системы или в случае размножения процессов может просто остановить работу системы.
- **Spyware –** программа, собирающая различную личную информацию о пользователе или о работе системы. Также может осуществлять контроль доступа к системе за счет доступа к данным аутентификации.
- **Adware –** программа, распространяющая рекламные объявления, «баннеры», блокирующие рекламные окна, на основе данных пользователя.
- **Zombie –** разновидность программ, делающих компьютер пользователя инструментом вредоносного воздействия на другие компьютеры, без информирования пользователя.

- **Exploit** – широко распространённый тип вредоносной программы основной целью которой, является поиск уязвимостей в вычислительной системы с целью последующей атаки на нее.

Атаки на систему

Помимо непосредственно вирусов и вредоносных программных решений существует целый класс различных методов, стратегий и сценариев развития атак, которые могут содержать комплекс различных вредоносных программ. Ниже приведены наиболее распространенные угрозы данного типа.

- **DoS (Denial of Service) атаки**: массовая атака, вызывающая отказ от обслуживания. Изначально данная операция предназначалась для проведения тестирования программного обеспечения, сайтов и серверов, но в начале 2000-х стала распространенным методов вредоносного воздействия на систему. Суть атаки заключается в том, что, на систему поступает чрезмерное количество запросов, с которыми она не в состоянии справится. В результате чего образуется «длинная очередь» запросов и система либо не может отвечать на запросы легальных пользователей, либо зацикливается (Prince, 2013). Вторым вариантом проведения DoS-атаки является целенаправленный поиск ошибок, слабостей, уязвимостей в системе, таких как например отсутствие актуальных обновлений и после нахождения такой уязвимости осуществление атаки посредство различных эксплойтов (Зобнин, 2009). В случае атакующему не нужно иметь много ресурсов для атаки, а достаточно точно нанести удар.
- **Атака нулевого дня:** несмотря на то, что базы данных уязвимостей и вирусов постоянно обновляются, существует некоторый временной промежуток, между тем когда вредоносная программа только возникла и начала работать и тем когда был разработан противодействующий ей защитный механизм. Атакой нулевого дня называют угрозу, против которой еще не разработаны защитные механизмы. Одним из ярких и первых представителей данного типа угроз является разработанный в 2010 году компьютерный червь Stuxnet, который использовал уязвимость алгоритма обработки ярлыков операционной системы Windows (Ralph, 2011).
- **Таргетированныые или целевые атаки:** в последние годы основной тенденцией является переход злоумышленников от написания массовых вредоносных программ к созданию атак на конкретное предприятие, компанию, государственный орган, то есть на создание комплексных таргетированных атак. (Шпунт, 2015). Для

подготовки такой атаки злоумышленники проводят ряд мер по обнаружению уязвимостей, таких как сканирование портов, определение операционной системы, набора приложений, активных ip-адресов, определение топологии компьютерной сети. После чего производится отчет о найденных уязвимостях и на его основе готовится узконаправленная атака, цели которой могут широко варьироваться в зависимости от направления деятельности субъекта, на которого предназначена атака.

- **Фишинг (Fishing):** тип угрозы, основной целью которого является определение конфиденциальных данных пользователей их получение в полное распоряжение, чаще всего это аутентификационные данные пользователя. Данный тип угрозы сложно назвать атакой, так как пользователь сам предоставляет все свои данные злоумышленнику. Чаще всего фишинг это массовая атака, посредством, в большей степени, почтовых рассылок или объявлений, с последующим перенаправлением на специализированный сервис, где пользователю предлагается ввести конфиденциальную информацию по различным причинам, например по требованию администратора. Можно подумать, что данной угрозе подвержены исключительно конечные пользователи и корпоративный сектор в данном случае в находится в полной безопасности, однако существует целый ряд примеров, когда началом серьезной таргетированной атаки были как раз фишинговые письма, с помощью которых злоумышленники и получили доступ к уязвимостям сети предприятия и впоследствии реализовывали свои атаки. Одним из последних ярких примеров является фишинговая атака на бельгийский банк Crelan, которая стоила ему порядка 70 млн евро (Securitylab, 2016).

После подробного описания всех разновидностей вредоносных программ и стратегий построения атаки, а также учитывая рост вредоносной активности (DrWeb, 2015), можно сделать вывод, что на сегодняшний день корпоративные клиенты достаточно сильно нуждается в качественном программном и аппаратном обеспечении против вредоносных программ, которое должно содержать различные функции и уметь противодействовать всему спектру угроз. Одним из примеров, такого вида систем является, рассматриваемый в данном исследовании, шлюз безопасности, произведенный компанией Check Point, подробный функционал которого, будет анализируется в пятом разделе данной главы.

1.4. Основные технологии для борьбы с угрозами сетевой безопасности

После определения инфраструктуры сети предприятия и выявления основных угроз сетевой безопасности, на следующем шаге рассматриваются основные технологии и методы борьбы с описанными угрозами. Поскольку угрозы сетевой безопасности различны, то и превентивные меры, направленные на борьбу с ними также имеет свою специфику.

Первые компьютерные вирусы появились в 1960-х годах, однако первые вредоносные вирусы и соответствующие им антивирусные программы берут начало своей истории в 1980-х (Ritstein, 1992). После появления интернета и начала его массового использования отрасли вредоносных программ и средств защиты против них на столько быстро развивались, что сегодня мы имеем широкий спектр различных средств и технологий защиты от угроз сетевой безопасности. После выделения основных из них, предлагается рассмотреть следующие системы и технологии:

- **Антивирус**
- **Межсетевой экран (Firewall)**
- **Системы IDS/IPS**
- **Технология VPN**

Antivirus

Антивирусная программа или антивирус, это программа, предназначенная для противодействия или борьбы различными типами угроз. Несмотря на то, что многие разработчики до сих пор называют свои программные решения антивирусами, данные программы предназначены для борьбы не только с вирусами, которые являются малой долей от всех угроз, но и со всеми классами вредоносных программ, описанных выше. Описывая общий алгоритм работы антивирусной программы можно сказать, что каждый антивирус должен выполнять три основных процедуры (Aycock, 2006): обнаружение, классификация вируса, обезвреживание.

Обнаружение – самый важный процесс в работе антивируса. От того на сколько хорошо антивирус отличает нейтральный код от вирусного, зависит вся его дальнейшая работа. Существует большой спектр различных алгоритмов обнаружения вредоносных программ, которые делятся на два типа: статистические и динамические. Их отличие заключается в том, что статистический метод не предполагает выполнения работы вредоносной программы, он просто сканирует ее код, сравнивая его со своими вирусными базами на предмет наличия вируса, данный подход еще называют сигнатурным (Zeltser, 2011). В свою очередь, динамический метод предполагает обнаружения вируса путем исполнения кода или наблюдения за тем, как работает программа, посредством различных

алгоритмов и техник, одним из примеров которых является процесс эмуляция вредоносного кода.

После того как антивирус обнаружил вредоносную программу, он должен понять к какому типу она относится, с тем, чтобы знать, как ей противодействовать. Для этого антивирусные программы используют свои системы классификации вредоносных программ, подобные описанной в предыдущем параграфе, но имеющие свои характерные особенности, зависящие от разработчика.

На последнем этапе программа либо очищает зараженные вредоносной программой объекты, либо удаляет их вместе с вирусом, при этом существует несколько основных подходов основанных на восстановлении, «лечении» исходного кода от вирусного. Исходный код может быть, как восстановлен полностью из заранее подготовленного, так и очищен от вирусного посредством различных техник, основанных на том, что вирусные программы достаточно специфичны, с точки зрения, как самого кода, так и воздействия, которое они осуществляют, также они имеют схожие алгоритмы распространения и внедрения. Однако, иногда «лечение» файла может быть невозможно, поскольку исходных код не подлежит постановлению.

Firewall (Межсетевой экран)

В 2000 году межсетевой экран представлял собой набор компонентов, расположенных между двумя участками сети, который пропускает или останавливает пакеты данных между ними в соответствии с некоторой политикой безопасности (Sotiris Ioannidis, 2000). В наше время межсетевой экран помимо сканирования портов , ip-адресов и проверки пакетов данных, проходящих через него, обладает внушительным набором различных функций и технологий таких как:

IDS/IPS

IDS (Intrusion Detection System) – система обнаружения вторжений, которая может быть реализована как программным, так и аппаратным способом, где под вторжением понимается нарушений одного из трех свойств информационной безопасности (Anti-Malware, 2016). Система содержит в себе три основных компоненты: источники информации, анализ информации, в соответствии с определённой конфигурацией и определение вердикта относительно поступившей информации (угроза проникновения или нет).

IPS (Intrusion Prevention System) – система предотвращения вторжений, которая является некоторым усовершенствованием системы IDS, но в отличии от IDS систем IPS, в большинстве случаев работает в реальном времени.

VPN

VPN (Virtual Private Network) – виртуальная частная сеть, то есть технология, позволяющая создавать подключение типа «точка-точка», используя специальные протоколы TCP/IP и общедоступные сети, например интернет. Для достижения приемлемого уровня безопасности пересылаемые данные шифруются. Благодаря данной технологии пользователь может удаленно обращается к серверу, используя, подобно туннель интернет. Также, во время VPN подключения происходит контроль подлинности, который может производится по различным протоколам, что, в свою очередь, увеличивает уровень безопасности.

Описанные в данном разделе технологии являются базовыми для таких решений, как корпоративный шлюз безопасности и должны обязательно присутствовать в любом продукте данного типа (Дрозд, 2014). В следующем разделе подробно рассматривается функциональные возможности шлюза безопасности

1.5. Анализ функционала шлюза безопасности компании Check Point

Средства защиты информации, предоставляемые компанией Check Point, обладают широким спектром функциональных возможностей частью функционала, где архитектура построения таких средств основана на концепции сочетания различных функциональных возможностей, определяемых пользователем, в едином техническом решении. Функционируют устройства под управлением собственной защищенной операционной системы Check Point Gaia, что также существенно повышает безопасность их использования. Основными блейдами (составными модулями) шлюза безопасности Check Point являются следующие элементы (CheckPoint, 2016):

Application Control

Данный программный блейд управления приложениями обеспечивает обнаружение работы, видимость и сканирование более чем 230 000 Web-приложений и виджетов социальных сетей, использует политику правил для разрешения, блокирования или ограничения использования Web-приложений и виджетов. При использовании совместно с программным блейдом Identity Awareness, администраторы могут создавать более детальную политику, используя информацию о пользователе, группе, машине и о местоположении для контроля над использованием приложений и виджетами с учетом содержимого трафика и пропускной способности сети.

Функционал позволяет, в частности осуществлять проверки, направленные на управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы), в частности, с веб-приложениями, размещенными в сети интернет, такими, как социальные сети Facebook, Twitter, YouTube, которые все более активно используются корпоративными пользователями в маркетинге, PR, для поиска персонала и других целей. Позволяет этот программный блейд и реализовать меры по обнаружению, идентификации и регистрации инцидентов, связанных с доступом (попыткой доступа) к сайтам, запрещенным политикой организации.

Mobile Access

Блейд Mobile Access предназначен для обеспечения надежного удаленного доступа к корпоративным ресурсам сотрудникам при одновременном снижении рисков, связанных с безопасностью, без участия администратора. Блейд просто интегрируется с другими программными блейдами, обеспечивающими безопасность работы с мобильными устройствами, и в зависимости от потребностей пользователя, обеспечивает широкий функционал, представляя собой решение «все в одном».

Для подключения удаленных работников предусмотрены следующие варианты удаленного доступа с двухфакторной аутентификацией пользователя:

- удаленный доступ с технологией полнофункционального VPN 3-го уровня, обеспечивающий аутентификацию и шифрование каждого сеанса связи IPS для защиты данных и доступа к корпоративным ресурсам;
- удаленный доступ с технологией шифрования SSL VPN для надежного шифрования при передаче информации между мобильными устройствами и корпоративной ИТ-инфраструктурой с доступом как на уровне web-интерфейса, так и на сетевом уровне, реализованном посредством SSL-шифрования с использованием практически любого Интернет-браузера.

Программный блейд DLP

Сочетание технологий и процессов, используемых в программном блейде DLP, позволяет перейти от пассивного обнаружения к активному предупреждению потери данных. Система MultiSpect выполняет классификацию данных с учетом информации о пользователе, типе данных и процессах для принятия решений, а технология UserCheck позволяет устранять инциденты информационной безопасности в режиме реального времени, что позволяет снизить объем работы IT-персонала и сотрудников службы информационной безопасности по обработке инцидентов и обучать пользователей информационной системы корпоративным правилам работы с информацией, предотвращая как преднамеренные, так и непреднамеренные потери данных.

Технология Check Point UserCheck уведомляет пользователей о предполагаемых нарушениях политик (правил) безопасности, позволяет предотвратить возможное и оперативно устранить возникшее нарушение, не допустить утечки данных, в том числе дает возможность пользователям самостоятельно избежать нарушения, получив соответствующее уведомление со ссылкой на установленные правила или устранить возникший инцидент информационной безопасности с возможностью отправки, отмены или пересмотра случившегося события. Уведомление о возможном нарушении правил безопасности приходит в режиме реального времени в виде всплывающего сообщения или электронного письма (не требует установки клиентского ПО). Такой подход позволяет перейти от обнаружения к предотвращению потери данных, способствует росту уровня осведомленности персонала в вопросах информационной безопасности, повышает дисциплину работы в сети.

Программный блейд URL Filtering

Программный блейд Check Point URL Filtering защищает корпоративные информационные системы и их пользователей путем использования облачной классификации свыше 100 миллионов web-сайтов, разрешая, блокируя или ограничивая доступ. URL Filtering позволяет предотвратить возможность обхода через внешние прокси-серверы, обеспечивает интеграцию принудительного использования политик с Application Control и использование UserCheck для расширения возможностей и обучения пользователей политике использования интернета в режиме реального времени. Кроме того, он позволяет сканировать шифрованный SSL-трафик внутри шлюза и обеспечивает принудительную проверку всего трафика, даже при перемещении внутри нестандартных портов.

Виртуальные системы (VS)

Виртуальные системы позволяют консолидировать инфраструктуру путем создания нескольких виртуальных шлюзов безопасности на одном аппаратном устройстве, что позволяет сэкономить затраты, консолидировать инфраструктуру и упростить реализацию корпоративной политики за счет создания индивидуальных политик для каждой сети и каждой виртуальной системы.

Программный блейд Anti-Bot

Программный блейд Check Point Anti-Bot является частью решения Check Point Threat Prevention и обнаруживает бот-инфицированные машины и предотвращает деятельность бота путем блокирования соединений от серверов злоумышленника, для чего используется постоянно обновляемый список серверов «Команд и Управления» (C&C) злоумышленников из ThreatCloud - облачной базы знаний угроз безопасности, работающей в режиме реального времени. Программный блейд Anti-Bot обнаруживает скрытых ботов прежде, чем они смогут нанести ущерб, и затронут пользователей.

Программный блейд Anti-Bot обнаруживает бот-инфицированные машины при помощи собственного движка ThreatSpect, использующего многоуровневую технологию обнаружения. ThreatSpect коррелирует информацию для точного обнаружения бота:

- адреса удаленного управления, включая IP, DNS и URL-адреса;
- обнаружение уникальных шаблонов соединений ботнета;
- обнаружение атак, таких как спам или «кликовое мошенничество».

Check Point Endpoint Security

Endpoint Security является централизованно управляемым с помощью модуля Endpoint Management агентом. Модуль входит в состав программного блейда Smart Center, который осуществляет управление другими программными блейдами и регистрацию (логирование) событий. Решение сочетает основные функции защиты конечных точек сети с простым для пользователей режимом функционирования и предусматривает установку следующих программных блейдов на рабочей станции, работающей под управлением операционной системы MS Windows:

- Персональный межсетевой экран, обеспечивающий проактивную защиту входящего и исходящего трафика, блокирование атаки и нежелательного трафика, регулирующий возможность запуска программного обеспечения на конечной точке, проверяющий целостность файлов с использованием хэш-функции и значений реестра, формирующий по заданным правилам реакцию при несоответствии файлов/ключей/софта и блокирующий доступ к корпоративному интранету вплоть до полного отключения сетевой карты, формирующий сообщения пользователю о выявленных несоответствиях, обеспечивающий при наличии соответствующей политики загрузку и установку необходимого программного обеспечения;
- Защита от вредоносного ПО (Anti-Virus & Anti-Malware), обнаруживающий и удаляющий вредоносные программы с конечных точек с проверкой по базам данных четырех различных производителей антивирусных средств;
- VPN для предоставления пользователю безопасного и непрерывного доступа к корпоративной сети и ресурсам во время удаленной работы;
- WebCheck, защищающий от новейших интернет-угроз, включая файловые загрузки, фишинговые сайты и атаки нулевого дня, позволяющий запускать виртуальный браузер как тонкий клиент, который имеет функции чистки кэша и оперативной памяти после завершения сессии;
- Full Disk Encryption для шифрования всего содержимого диска;
- Media Encryption & Port Protection для шифрования данных на носителях, обеспечивающий централизованное шифрование съемных носителей, централизованное управление всеми внешними интерфейсами конечных точек, в том числе централизованное протоколирование активности на них;

Таблица 1 – Соотношение угроз и превентивных мер

Угроза	**Методы борьбы**	**Реализация в Check Point**
Вирус, вредоносное ПО	Антивирус	Check Point Endpoint Security
Dos- атака	Firewall	Check Point Firewall/Anti-bot
Атака нулевого дня	IPS/IDS	Check Point IPS, URL Filtering
Таргетированная атака	IPS/IDS	Check Point IPS, URL Filtering
Фишинг	DLP/Antispam	Check Point Antispam, DLP

Таким образом, после подробного рассмотрения основных угроз, методов борьбы с ними и функциональными возможностями шлюза информационной безопасности Check Point можно сделать вывод о наличии следующих (см. Таблицу 1) взаимосвязей между ними и убедиться, что система Check Point является универсальной и противодействует основным видам угроз. Однако, вопрос мониторинга работы системы остается достаточно актуальным, так как из-за постоянного развития уровня угроз, появления новых особенностей и направлений атак, необходимо знать основные тенденции, улучшать политику безопасности, понимать каким атакам система подвержена в большей степени и улучшать превентивные меры. Данная задача в данной работе решается посредством построения информационной панели в системе анализа машинных данных Splunk, о чем будет говорится в следующей главе.

Глава 2. Организация работы с лог-данными

2.1. Понятие лога, принципы организации системы логирования

Лог-файл или журнал событий – это файл, содержащий информацию о событиях, происходящих в системе в хронологическом порядке, который был сгенерирован некоторым устройством по заранее определенным правилам. Журнал состоит из множества записей (строк), где каждая запись (лог) содержит информацию об определенном событии, которое произошло в системе или сети. Основным практическим значением лог-файла является то, что, используя его, мы можем воссоздать картину происходящего в системе и использовать эту информацию для выявлении источников возникновения ошибок, сбоев и других неблагоприятный событий.

Лог-файлы могут быть классифицированы следующим образом (Garfinkel, 2005):

- *Информационный лог*: нейтральное сообщение о фактах работы системы, позволяющие пользователю понять, что вообще происходит в системе.
- *Лог отладки*: сообщения предназначенные для разработчиков системы, генерирующие данные о проблемах, связанных с выполнением программного кода приложения.
- *Лог предупреждения*: сообщения о ситуациях, имеющих некоторые несоответствия с правилами работы системы, но не влияющих в целом на работу программы.
- *Лог ошибки*: сообщения, содержащие информацию о событиях, приводящих к различным ошибкам в работе систем, к сожалению, большинство сообщений об ошибках не дают полной картины произошедшего, в них отсутствует информация о первопричинах ошибки.

Однако, система не всегда правильно классифицирует события правильно, ведь она может различать только те события, критерии которых были заранее запрограммированы, поэтому существует необходимость постоянного анализа происходящего с целью мониторинга и модернизации работы системы.

Как было отмечено, лог сообщение – это какая-то информация, записанная некоторым устройством, чтобы обозначить, что что-то произошло. Типичными составляющими данного сообщения являются:

- Отметка о времени
- Отметка об источнике информации
- Основные данные о событии

Сообщения могут иметь разные источники и протоколы написания, но описанные выше составные части всегда будут присутствовать в них, с другой стороны, сегодня, не существует определённого формата, регламентирующего содержание каждой части в отдельности.

К сожалению, не все сообщения бывают информативны. Одной из самых больших проблем в анализе логов является то, что многие сообщения, сформированы не лучшим образом и не предоставляют полезной для анализа информации либо из-за того, что информации в сообщении практически нет, либо из-за того, что сообщение наоборот переполнено различными полями и данными, в связи с чем его чрезвычайно сложно обрабатывать и получать информацию.

```
Jun 21 14:38:25 10.2.2.1 rlogin: connection refused
```

Анализируя данное сообщение мы не получаем никакой информации почему произошел разрыв соединения, на каком этапе это случилось. Мы имеем лишь факт возникновения проблемы, что, в свою очередь, полезно, но не понятно, как с этим бороться, поэтому разработчик, программируя формат лог-сообщения, должен очень внимательно подходить к этому аспекту.

Генерирование и основные форматы сбора лог-сообщений

Наиболее распространенным методом сбора лог-данных является стандартизированный протокол Syslog. Он изначально был создан для работы Unix системах, но сейчас широко распространен как в Windows, так и в других платформах. Принцип работы Syslog достаточно прост: разные компоненты системы создают тривиальные текстовые сообщения о произошедших в них событиях и отправляют их серверу Syslog по протоколу TCP. Правила передачи и формирования сообщений о событиях и называются протоколом Syslog. Существует максимальный размер сообщения, на сегодняшний день его размер составляет 1024 байта.

На сегодняшний день, Syslog это не единственный механизм генерации и отправки лог сообщений. Например, OS Microsoft Windows имеет собственную систему логирования и записывает информацию о входе, выходе пользователя из системы, о сообщениях приложений и о других событиях в собственном формате хранения.

Базы данных также являются удобным способом хранения данных о событиях в системе. В данном случае, сообщение вместо того чтобы генерироваться в Syslog, сразу записывается в реляционную базу данных. Этот механизм имеет большие преимущества,

особенно в части структурированного хранения и возможности анализа информации, но явный недостаток этого метода – повышенная, по сравнению с Syslog, ресурсозатратность.

Также конкретные программы и приложения имеют собственные механизмы и форматы логирования, то есть поставщик предоставляет собственный программный интерфейс или позволяет реализовать данный аспект самостоятельно. Ниже представлен список наиболее распространенных решений по генерации и хранению лог-информации:

- Syslog – основанный на UDP клиент-серверный протокол
- SNMP – протокол созданный для работы с сетевыми устройствами
- Журнал событий Windows
- Базы данных
- Security Device Event Exchange (SDEE) – расширяемая разметка Cisco
- E-Streamer – собственный протокол Sourcefire для своего IPS

2.2. Основные направления анализа лог-информации

Прежде чем приступать к анализу необходимо понять, какие цели могут преследоваться, при изучении данных, находящихся в лог-файлах. Конечно, в зависимости от предметной области, конкретные цели анализа могут отличаться, очевидно, что цели руководителей банка и цели руководителей продуктового супермаркета будут различны, однако, если говорить об основных направлениях, то они делятся на два вида: анализ того, что произошло в прошлом и анализ, направленный на прогнозирование того, что произойдет в будущем.

Если говорить непосредственно о задачах, которые можно решать с помощью анализа лог файлов то можно отметить следующие характерные примеры:

Управление ресурсами

Довольно часто, информация о каких-либо проблемах, связанных с работой с системы, появляется в лог-журналах в виде разного вида предупреждений или ошибок задолго до того, как случиться большая «неприятность», поэтому контролирование и анализ лог файлов может предотвратить нежелательные в будущем события. В свою очередь, если система все-таки дала сбой, с помощью лог-журнала можно понять, что произошло и почему в системе произошла ошибка.

Таким же образом с помощью логов можно предвосхищать не только риски и неблагоприятные явления, но и различного вида возможности, используя, например, всевозможные методы статистического прогнозирования.

Расследование различного рода злоупотреблений службами внутренней безопасности и правоохранительными органами

Лог-журнал в определенных ситуациях может стать неотъемлемой составляющей в ситуациях связанных с разного вида разбирательствами судебного или внутриорганизационного характера. Лог-сообщения дают достаточно много полезной информации такой как: что произошло, когда произошел инцидент, в какой хронологической последовательности проходили события.

Лог-файлы также могут выступать в качестве усилений других доказательств или в тех случаях, когда источники информации были удалены или очищены злоумышленником. Ярким примером является проверка лог-сообщений электронной почты, которую можно просто удалить из почтового ящика, но информация о которой долгое время хранится в лог-журналах. Например, если человек утверждает, что не получал сообщения и все претензии к нему неправомерны, лог журнал может показать обратное.

Аудит и мониторинг операционной деятельности

В некоторых штатах США аудит лог информации является такой же обыденной деятельностью как финансовая отчетность, так как данные требования заложены в нормативно правовых актах и регулирующих документах. Одним из распространённых примеров лог-аудита может служить ведение определённых типов лог-журналов транзакций кредитных карт (Skoudis, и др., 2003).

Многие компании используют лог-файлы для контроля операционной деятельности организации, с целью мониторинга текущих процессов компании. Сегодня, существуют технологии, позволяющие вести анализ лог-файлов в режиме реального времени, но пока сложно сказать на сколько это оправдано и какая должна быть задержка во времени. Существует достаточно дискуссий различного рода специалистов, которые сводятся к тому, что данная опция важна в большей степени в финансовом, банковском секторах, а в сферах деятельности несвязанных с мгновенной передачей данных пока остается не востребована.

Информационная безопасность

Информационная безопасность является одним из возможных и распространенных направлений в рамках лог-менеджмента. Одним из возможных вариантов применений является целое такое направление ка SIEM (Security Information and Event Management), которое подразумевает сбор данных из различных источников, в большинстве случаев это лог-журналы, и получение на основе этих данных ценной информации различного типа относительно работы систем безопасности.

Обнаружив в лог-журнале в большом количестве сообщений следующего типа (за короткий промежуток времени) можно сделать вывод, что в систему пытается попасть злоумышленник и нужно принимать соответствующие меры.

```
Jun 01 11:22:31 host.example.com: Failed password for illegal user Ivanov from
168.111.0.3 port 111
```

К сожалению, нельзя с уверенностью сказать была ли эта попытка успешной или нет, но сам факт возникновения вторжения безусловно важен и требует серьезного внимания со стороны ответственного за данный процесс лица.

2.3. Анализ лог-файла шлюза безопасности компании Check Point

В результате анализа функционала шлюза безопасности было выявлено, что сбором и генерацией лог-файлов со всех модулей, входящих в систему безопасности Check Point занимается отдельный блейд Checkpoint SmartCenter. Посредством специального интерфейса OPSEC LEA (Log Export API) лог-файлы из отдельных систем попадают на сервер, после чего с сервера данные через SSL соединение могут извлекаться и направляться в различные системы для аналитики или хранения, это могут быть как базы данных так и специальные BI-системы (см. Рисунок 5).

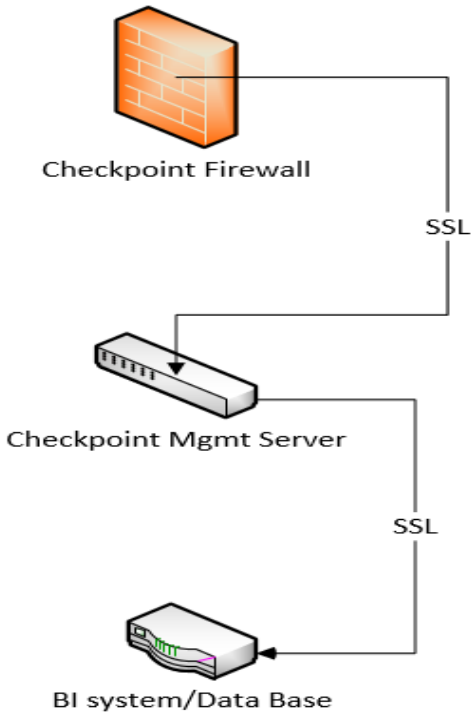


Рисунок 5 – Экспорт лог-данных из системы Check Point

Данная операция может проводиться как в режиме реального времени, так и с некоторой задержкой, по расписанию. Лог-файлы, извлекаемые из различных подсистем объединяются и поступают в BI-систему для последующей аналитики.

На Рисунке 6 представлены основные источники окончательного лог-файла системы, которые могут варьироваться в зависимости от начального функционала и решаемых задач.

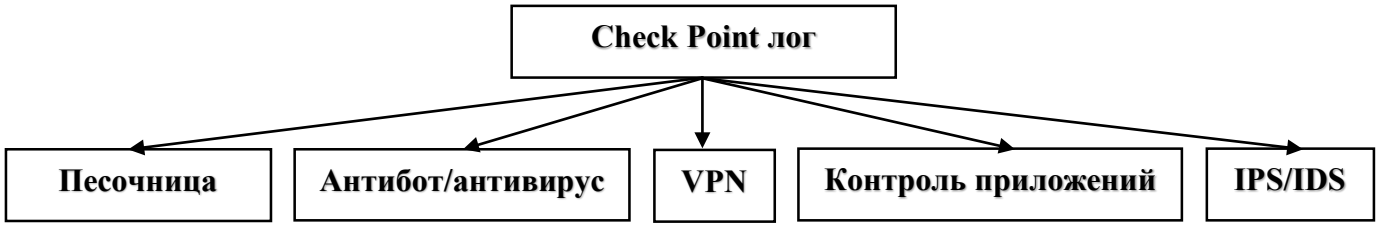


Рисунок 6 – Структура лог-файла шлюза безопасности Check Point

Исходя из того, что каждая подсистема направлена на решение определённых задач и борьбу с различными типами угроз, лог-сообщения, генерируемые на разных модулях несколько отличаются друг от друга как по структуре, так и по содержанию, поскольку каждый модуль отслеживает угрозы определенного типа. Несмотря на это, были выделены основные компоненты лог-сообщений и определены основные поля (см. Рисунок 7), по котором в дальнейшем можно проводить детальный анализ.

Поле	Описание
loc	Уникальный номер события
time	Время события
action	Действие системы при соединение (разрешить, разорвать, прервать)
dir	Направление проходящего трафика (внутренний/внешний)
app_name	Название модуля системы, обрабатывающей событие
src_ip	Исходящий ip-адрес
dst	Хост места назначения отправляемого трафика
proto	Протокол отправки трафика
app_risk	Уровень риска соединения атаки
src_user	Электронный адрес пользователя
app_category	Категория приложения
cp_bytes	Объем трафика в байтах
industry_ref	Указание номера из базы CVE
cp_machine	Электронный адрес пользователя, определённый по его компьютеру

Рисунок 7 – Основные поля лог-сообщений шлюза ИБ Check Point

Таким образом мы провели первичный анализ лог-сообщений шлюза безопасности Check Point, определили основные поля, выявили основные особенности в структуре формирования сообщений и процедуры их экспортирования из системы для последующего анализа с помощью сторонних приложений.

2.4. Обзор систем для анализа лог-файлов, их специфика

Рынок программных средств, предназначенных для управления, накопления, обработки и анализа лог-информации значительно вырос за последнее время. Набор инструментов варьируется от базовых программ, централизованно накапливающих информацию для последующей отчетности, до специализированных систем способных осуществлять мониторинг бизнес-процессов различного типа в реальном времени и высылать пользователю оповещения при определённых обстоятельствах. В данном разделе рассматривается несколько широкодоступных систем анализа лог-журналов, и делается выбор одной из них для анализа лог-файлов шлюза безопасности Check Point на основе интегральной оценки.

IBM q1Labs

Доступное решение от компании IBM для управление лог-журналами, имеющее широкий спектр возможностей и решений, связанных с организацией хранения лог-данных, построением поисковых процедур, созданием высокой функциональности отчетов. Также, с помощью дополнительного набора продуктов, она может быть расширена до полноценной системы информационной безопасности и управления событиями.

Данная система в большей степени предназначена для работы на рынке американских компаний, так как ее ключевым отличием является то, что она имеет встроенные отчеты по определенным правовым стандартам США.

На данный момент система не имеет бесплатной (пробной) версии программы, а стоимость является договорной для разного вида предметных областей.

Loggly

Программное обеспечение для анализа лог-сообщений, организованное с помощью использования облачных технологий, что является достаточно новым направлением в мире анализа лог-данных. Продукт поддерживает широкий спектр источников информации, что является одним из важнейших достоинств системы.

Основным преимуществами данной системы является наличие простого, интуитивного интерфейса и отсутствие необходимости установки какого-либо дополнительного оборудования в системе организации, для развертывания данной системы. Однако, этот же аспект, может служить и возможным ограничением, так как лог-файлы тоже будут хранится в облаке, что, в вою очередь, в некоторых предметных областях, касающихся данных, связанных с личной информацией, запрещено на правовом уровне.

Splunk

Коммерческий программный продукт, обеспечивающий большие возможности при анализе лог-журналов. Система позволяет централизованно хранить лог-данные, обрабатывая практически все возможные на сегодняшний день форматы лог-файлов, при этом данные могут находится на удаленных источниках. Splunk способен генерировать и обрабатывать терабайты лог-сообщений, при этом обладая довольно широким функционалом для реализации различного вида задач, интуитивно-понятным интерфейсом и языком поисковых запросов, а также удобной и красочной графикой при визуализации результатов анализа.

Splunk настолько быстро и эффективно обрабатывает данные, что иногда, благодаря двусторонней кроссплатформенности, то есть поддержке широкого спектра как входных, так и выходных форматов, выступает в качестве промежуточного звена между устройствами и программами генерирующими лог-сообщения и системами, которые данные лог-файлы обрабатывают (Carasso, 2012).

Основным минусом данной системы является то, что Splunk – проприетарная система, и бесплатная версия позволяет обрабатывать лишь ограниченный объем информации, однако, даже в бесплатной версии поддерживаются абсолютно весь функционал системы и доступны все дополнительные надстройки, что является, в свою очередь, большим преимуществом.

После обзора систем и выявления их основ достоинств и недостатков, совместно с заказчиком на основе экспертной оценки были сформированы следующие основные критерии оценки:

Таблица 2 – Критерии оценки системы

№	Критерий оценки
1	«Возможность DrillDown на графиках»
2	«Широкая интеграция с системой Check Point»
3	«Возможность работы с большими объемами данных»
4	«Богатство графической визуализации данных»
5	«Возможность подключения сборок, расширений, разработанных на языках программирования»
6	«Возможность анализа информации в режиме реального времени»
7	«Поддержка, возможность интеграции с другими офисными пакетами»
8	«Наличие большого количества книг, тематических сайтов»

Поскольку основной задачей для данной системы является обработка лог-файлов, генерируемых шлюзом безопасности Check Point, одним из основных критериев был

выбран такой параметр как возможность интеграции с данной системой. Также для заказчика было важно, чтобы система имела функции «DrillDown», которая позволяет при нажатие на какой-либо элемент графика, находящегося на информационной панели, переместиться непосредственно к лог-сообщению о событии и детально рассмотреть информацию. Исходя из того, что объем данных, формируемый системой безопасности внушителен, больше гигабайта в неделю, такой критерий как возможность обработки больших объемов данных был выбран как один из важных.

Для обоснования выбора BI (Business Intelligence) системы была проведена интегральная оценка эффективности Фишберна и получены следующие показатели:

Таблица 3 – Интегральная оценка Фишберна

Наименование	**Интегральная оценка Фишберна**
IBM q1Labs	0,494
Loggly	0,349
Splunk	**0,731**

Исходя из полученных результатов, был сделан вывод о том, что предпочтительной системой для данной предметной области, согласно экспертным оценкам, является система Splunk (см. Приложение).

Глава 3. Разработка приложения (панели dashboard)

3.1. Понятие информационной панели (dashboard)

Многие авторы по-разному определяют термин dashboard. К примеру, Stephen Few говорит, что это *визуальное отображение самой важной информации, необходимой для достижения одной или нескольких целей, объединенных и размещенных на одном экране, так чтобы информация могла контролироваться с одного взгляда*, a Peter McFadden (CEO of Excel Dashboard Widgets) дает следующее определение: *приборная панель представляющая собой единый экран, который отслеживает ряд ключевых показателей в режиме реального времени* (Few, 2006).

Мы будем называть определять понятие dashboard как информационную панель, содержащую визуальное представление наиболее важной и интересной для конкретного пользователя информации, включающую диаграммы, светофоры, круговые шкалы и прочее. Хорошо спроектированный dashboard позволяет быстро и качественно ориентироваться в том, что происходит в системе, а также оказывает большую аналитическую поддержку в процессе принятия решений. Иногда говорят, что dashboard – это инновация в мире бизнес-аналитики, но существует и множество оппонентов, считающих данный вид представления информации тривиальным и традиционным решением.

Говоря о преимуществах информационных панелей можно выделить следующие характерные черты:

- Dashboard позволяет конвертировать довольно большие объемы данных в небольшую страницу с краткими, но релевантными результатами, что очень сильно экономит время пользователя при анализе информации.
- Благодаря модульной архитектуре, при появлении новых требований к показателям, находящимся на информационной панели, связанных, например, с изменением бизнес-процессов организации, в dashboard могут встраиваться новые модули (показатели, графики) или удаляться старые, неинформативные элементы, то есть dashboard содержит только нужную пользователю информацию
- Dashboard – это обновляемая информационная панель. Существуют разные возможности обновления исходных данных и соответственно показателей панели. Данный процесс может быть реализован как вручную (имеется ввиду, что пользователь сам, в нужное ему время «подгружает» информацию, а система обновляет показатели), так и автоматически (система сама, в

определённые промежутки, времени обновляет данные и пересчитывает показатели). Стоит отметить, что некоторые информационные способны работать в режиме реального времени.

Основные принципы дизайна dashboard (Few, 2006)

- Вся информация располагается на одном экране, с возможностью доступа к подробному первоисточнику
- На информационной панели находятся только ключевые показатели
- Обилие репрезентативной графики с выделенными исключениями
- Информация полотно рассредоточена по всей панели

Существует множество различных средств и инструментов с помощью которых мы можем строить информационную панель: графики, диаграммы, датчики и прочее. Однако, не стоит забывать, что, несмотря на то, что мы живем в эпоху маркетинга и дизайна, где яркий и приятный интерфейс пользовательских форм играет не последнюю роль, dashboard должен быть, в первую очередь, эффективным средством анализа, поэтому все графические возможности должны быть направлены, в первую очередь, на улучшение коммуникации с пользователем, а не то, чтобы каким-либо образом развлечь его или «порадовать глаз» (Few, 2006).

К сожалению, многие разработчики забывают об этом, делая яркие, красивые и привлекающие внимание, но малоэффективные информационные панели, к которым, через некоторое время после их внедрения, теряется интерес пользователя, и они более не используются. Эффективный *dashboard* – это не продукт отдельно взятых датчиков, светофоров и счетчиков, это – результат осознанного дизайна, направленного на увеличение эффективности преодоления коммуникативных барьеров с пользователем, поэтому нужно очень серьезно подходить к вопросу выбора того или иного средства визуализации.

3.2. Проект информационной панели

Содержание лог-файлов исследуемого шлюза безопасности настолько разнообразно, что существует возможность создания не менее тридцати уникальных полей различного типа, однако, только малая доля из них представляет собой информационную и практическую ценность. Для заказчика был составлен список возможно-значимых, по мнению автора, показателей, из которых, после совместного обсуждения, были выделены наиболее интересные, с точки зрения оперативного анализа и мониторинга работы не только шлюза безопасности Check Point, но и непосредственно сотрудников организации, элементы будущей информационной панели. В результате чего было принято решение построить информационные панели в двух направлениях: анализ работы программного модуля шлюза безопасности *Check Point Application Control* и мониторинг системы предотвращения вторжений *Check Point IPS u URL Filtering*.

Исследуемые показатели (Application Control):

- Суммарное количество событий (соединений), совершенных пользователями с разбиением по приложениям (протоколам), для получения информации, о том, какими ресурсами пользуются сотрудники компании
- Суммарный объем скаченного с разбиением по пользователям
- Статистика о количестве нежелательных, опасных приложений, с указанием категории и названия приложения, где под нежелательным, подразумевается приложение имеющее по полю *app_risk* значение больше 3, с разделением по пользователям
- Суммарное количество событий (соединений), совершенных пользователями с разбиением по уровню риска для системы, для понимания общей картины угроз
- Статистика по каждому отдельному пользователю по таким показателям как: суммарный объем скаченного, суммарное количество посещений каждого отдельного сайта (домена), временной график по запросам пользователя и использованию трафика, объем трафика с разделением по протоколам и категориям приложений

Для каждого из вышеперечисленных показателей необходимо реализовать возможность фильтрации по различным офисам компании и непосредственно по сотруднику компании для получения более детальной информации.

Исследуемые показатели (IPS и URL Filtering):

- Статистика атак во времени с разделением на различные типы и категории для получения информации об текущем состоянии системы с точки зрения количества вредоносных действий из внешней среды
- Суммарное количество атака на каждый сервер компании с информацией по каждому типу угрозы (матрица сервер-угроза)
- Статистика атак с информацией об источнике угрозы (ip-адрес откуда пришли пакеты) и ее месте назначения (внутренний ip-адрес) с возможностью фильтрации по типу действий системы (отклонить, прервать, перенаправить)
- Статистика атак из базы CVE, обогащенная информацией из общедоступных баз данных и сканера уязвимостей Nessus

Одной из основных проблем в мониторинге работы шлюза безопасности Check Point в исследуемой компании, является чрезвычайно большой объем сообщений о различных видах атак, многие из которых не представляют реальной угрозы для предприятия. Данная ситуация возникает из-за того, что большинство атак реализованы посредством автоматических скриптов и не являются целевыми, а атакуют всех подряд, с целью найти уязвимость. К примеру, если все компьютеры предприятия работают на операционной системы Lunix, а атака производится на систему Windows, шлюз безопасности запишет соответствующее сообщение как одну из атак, хотя она и не могла нанести вреда предприятию. В связи с этим, сотрудники компании имеют такое количество событий с атаками, которое из-за нехватки времени не может быть детально рассмотрено и изучено, поэтому одним из важных моментов в построении информационной панели является выделения действительно важных угроз, посредством обогащения данных лог-файла информацией об угрозах из общедоступных баз данных и путем дополнительного сканирования системы с помощью общедоступного сканера уязвимостей Nessus.

В качестве основных источников информации об угрозах, были выбраны такие всемирные общедоступные базы данных угроз как CVE (Common Vulnerabilities and Exposures), CWE (Common Weakness Enumeration), CVSS (Common Vulnerability Scoring System) благодаря которым удалось обогатить лог-сообщения об атаках и выделить наиболее важные угрозы, путем интеграции вышеперечисленных баз данных в систему Splunk, и тем самым сократить количество угроз для приемлемого, с точки зрения возможности обработки уровня.

3.3. Описание разработанного инструментария

Как было описано выше, основным результатом выполнения данной работы является информационная панель реагирования (dashboard), предназначенная для мониторинга работы шлюза информационной безопасности CheckPoint. В данном параграфе подробно описываются основные этапы работы над этим проектом.

Реализация ввода данных в систему, создание полей

На первом этапе работы системы требуется загрузить данные для анализа в систему. Эту операцию возможно сделать либо простым добавлением файлов, указывая тип и источник информации, что важно для системы, либо произвести отладку автоматической загрузки данных в систему исходя из возможностей системы, генерирующей лог-данные. В случае с со шлюзом безопасности Check Point использовался шифрованный SSL протокол, как было описано в предыдущей главе.

После того как данные поступили в систему Splunk, следующей задачей является подготовка загруженных данных к обработке, а именно решение проблемы, связанной с созданием новых полей, потому что несмотря на то, что система сама создает большинство полей автоматически, некоторые специфические особенности, которые могут встречаться лишь в конкретной предметной, остаются без внимания.

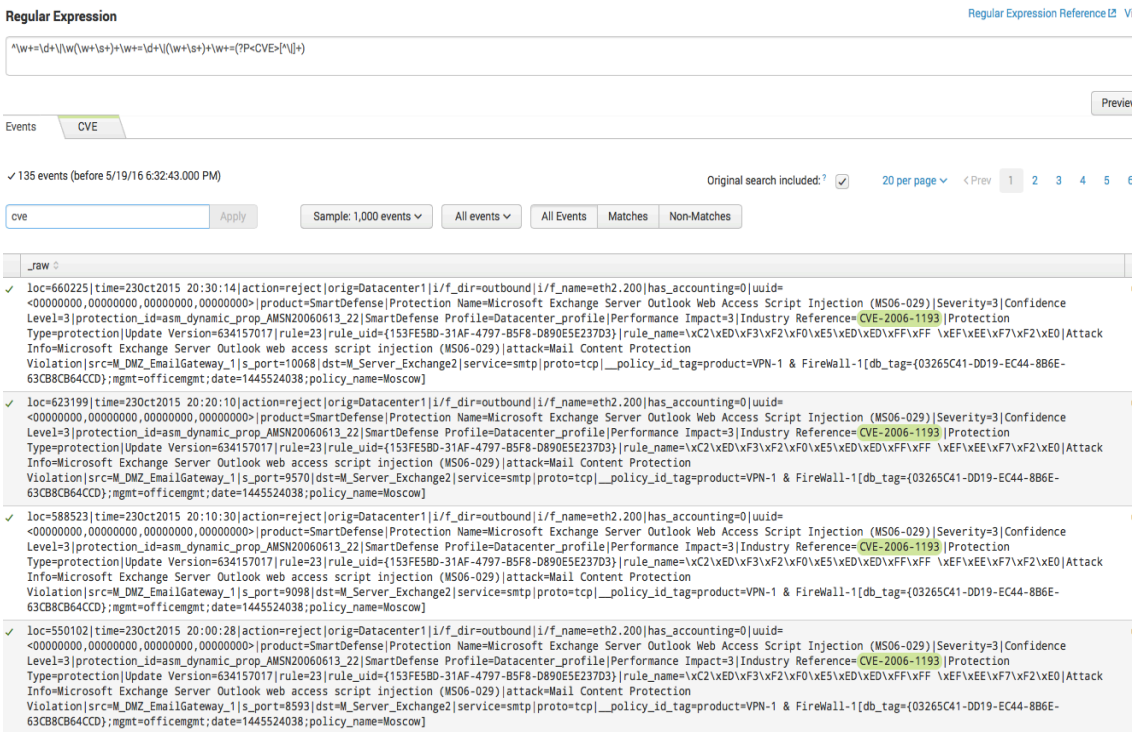


Рисунок 8 - Создание нового поля на основе регулярного выражения

На Рисунке 8 представлен пример реализации данной задачи, на котором можно увидеть, как система выделяет будущие поля, на основе регулярного выражения, давая пользователю проверить правильность формирования.

Данная процедура в большинстве случаев не обязательна, так как система способна Splunk в сама, в автоматическом режиме, правильно формировать поля, но несмотря на это, пользователю все таки требуется контролировать данный процесс и вносить некоторые правки, такие как настройка формата отображения даты и времени, выделение полей полностью, а не только их частичные составляющие, что, в свою очередь, требует времени и внимания.

Реализация процедуры обогащения данных, интеграция с внешними БД

После того как данные загружены в систему и определены основные поля, на следующем шаге было произведено объединение таких баз данных как CVE, CVSS, CWE и интеграцию с системой Splunk, для чего была использована надстройка Splunk DB Connect. Ниже представлена схема объединённой базы данных об угрозах (см. Рисунок 9).

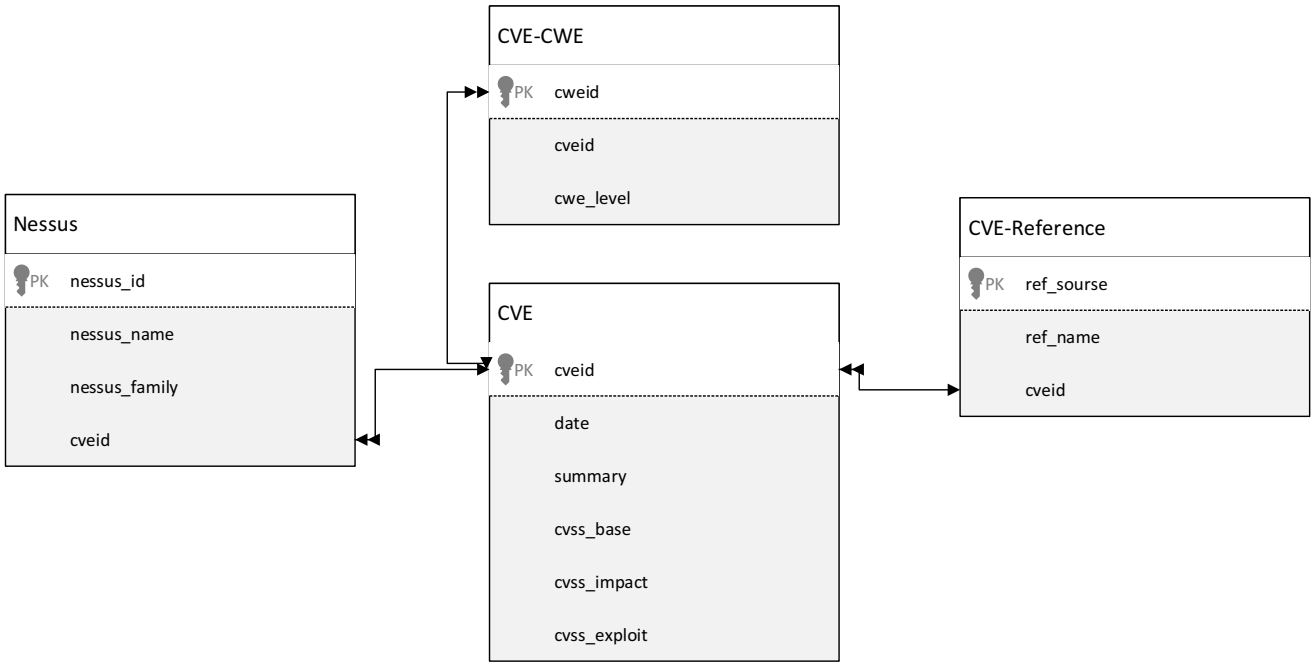


Рисунок 9 – Схема БД угроз

На основе данной информации в ходе построения запросов создаются новые поля, происходит процесс обогащения лог-данных и рассчитываются искомые показатели, к примеру для каждого лог-сообщения содержащего в себе информацию с номером угрозы CVE, мы можем определить на что направлена данная атака, рассчитать ее уровень опасности, а также предоставить пользователю информацию о том, как бороться с данной угрозой.

Также, в качестве еще одного дополнительного источника данных о системе, был взят сканер уязвимостей Nessus, в рамках которого был налажен процесс ежедневного сканирования ip-адресов системы на предмет различных уязвимостей со стороны. Злоумышленники поступает примерно таким же образом (сканируют ip-адреса, отдельные порты), чтобы найти уязвимости. После чего была настроена автоматическая отправка результатов сканирования в систему Splunk, по средствам протокола REST (Representational State Transfer).

Построение SPL запросов и их графическая визуализация

Основным инструментов работы в системе Splunk являются запросы, реализуемые посредство встроенного языка SPL запросов (Search Processing Language). Ниже представлен вид стартового окна (см. Рисунок 10), после реализации описанных выше итераций, где сверху располагается строка поисковых запросов, справа – сформированные поля, в центре лог-сообщения импортированные в систему.

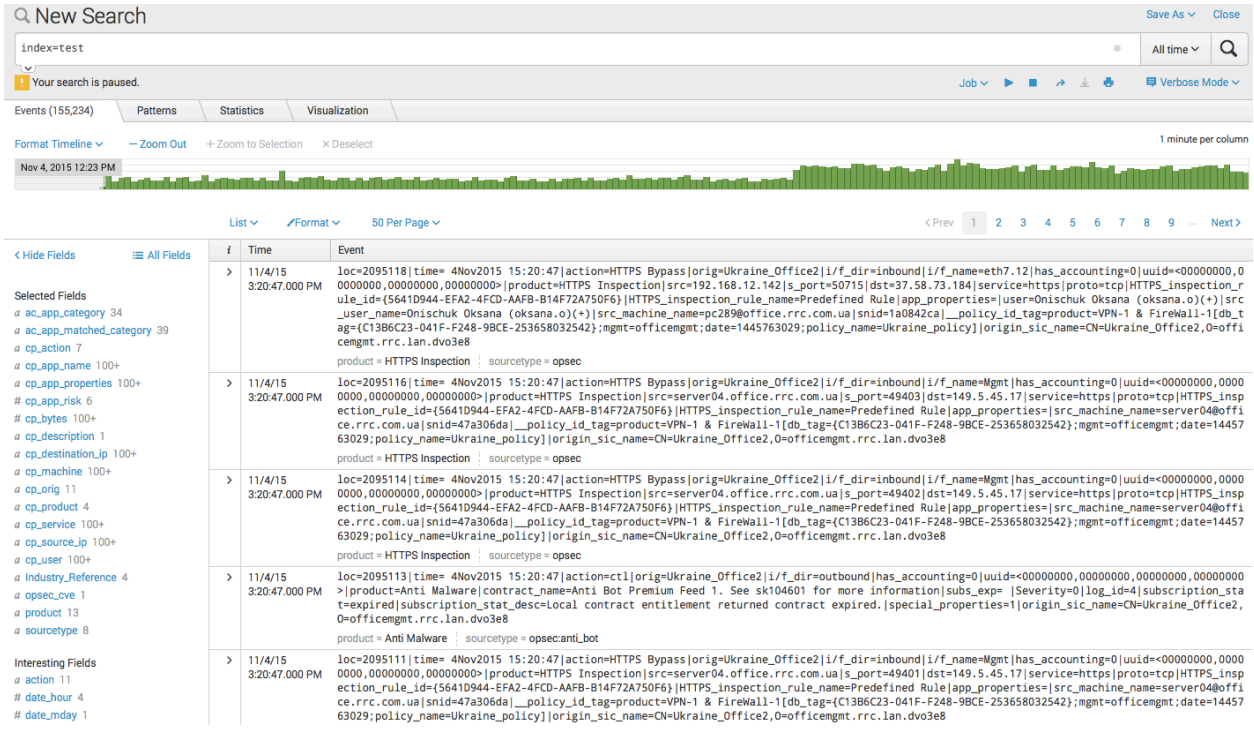


Рисунок 10 – Окно поиска системы Splunk

После того как данные загружены в систему и определены основные поля, а также настроена интеграция с дополнительными источниками были построены следующие запросы и соответствующие им информационные панели:

- **Контроль работы приложений**
- **Контроль работы пользователей**
- **Мониторинг системы IPS**
- **Атаки и уязвимости из базы CVE**

Контроль работы приложений

В правом верхнем углу данной панели (см Рисунок 11) размещена круговая диаграмма показывающая распределение событий по приложениям и протоколам, с помощью которой можно сделать вывод о том, какими приложениями работники пользуются и в каком количестве. Слева представлена диаграмма, на которой показано суммарное количество событий с разбиением по уровню риска для системы, что предоставляет возможность отслеживать количество наиболее опасных событий.

На нижнем уровне размещена статистика по ip-адресам пользователей с информацией о количестве используемого трафика, используемых приложений с разбиением по категориям и названиям.

В верхней части панели пользователь может выбрать интересующие его офиса и произвести соответствующую фильтрацию. Нажатие на конкретный ip-адрес перенесет пользователя на следующую информационную панель (см. Рисунок 12), где будет предоставлена информация по выбранному с помощью ip-адреса работнику.

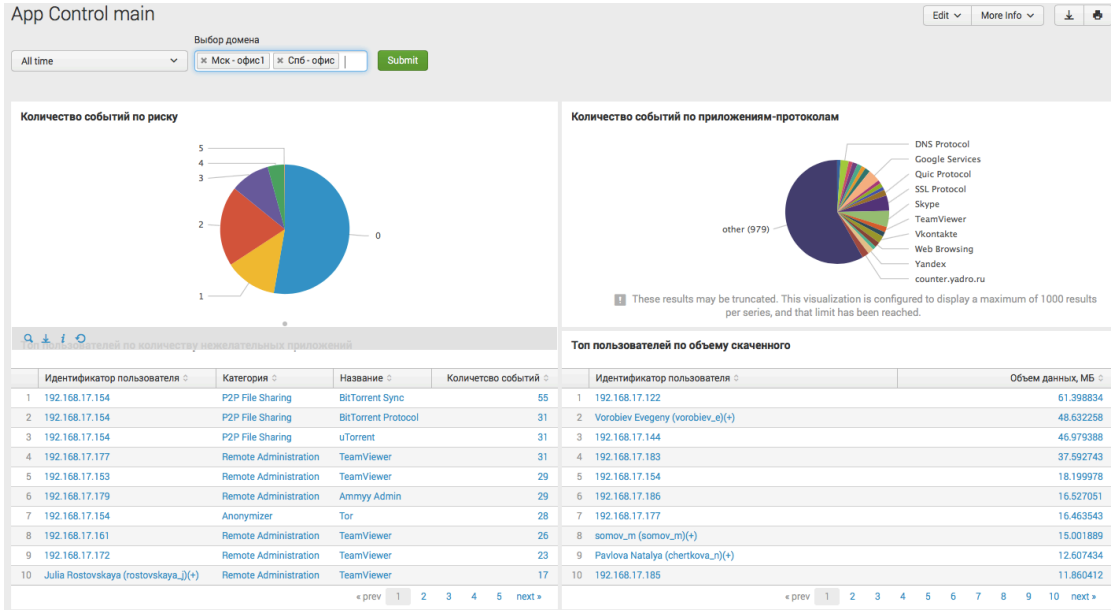


Рисунок 11 – Контроль работы приложений

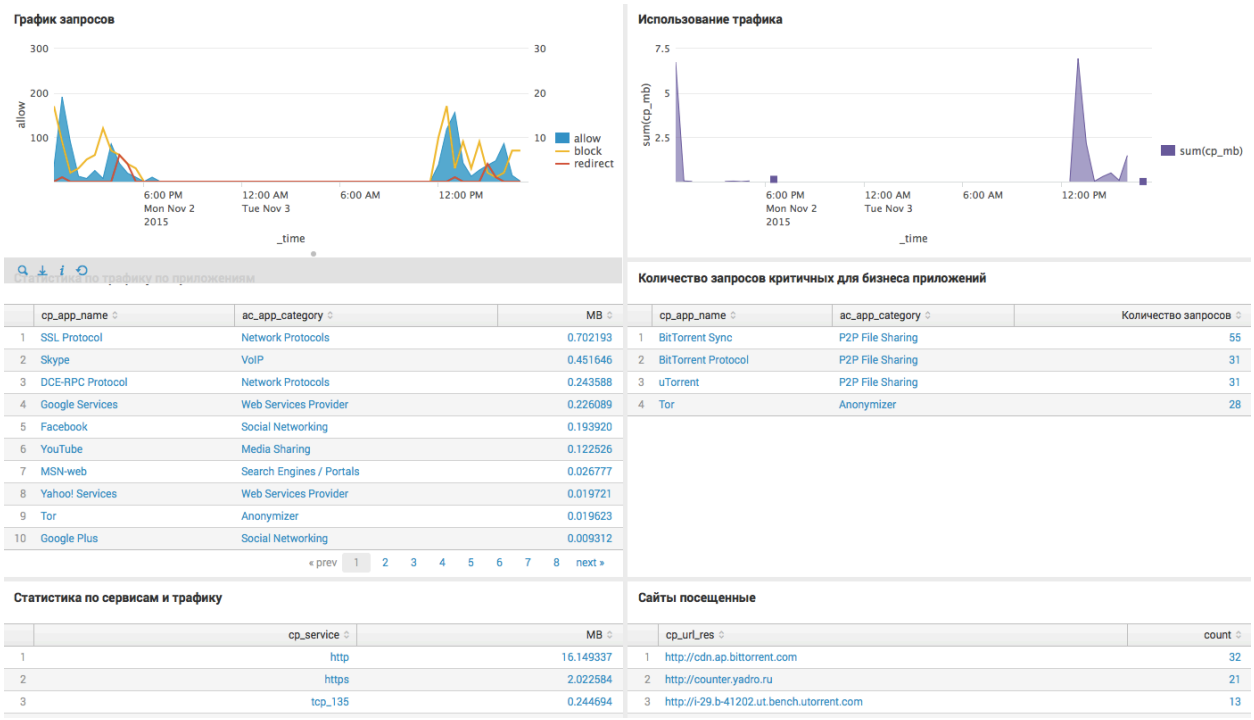
Программный код, включая SPL запросы, посредством которых реализована данная информационная панель представлен в приложении (см. Приложение 2).

Контроль работы пользователей

В верхней части данной информационной панели (см. Рисунок 12) представлена информация и количестве запросов пользователя, действие системы относительно данных запросов и информация о количестве используемого пользователем трафика. Графики представлены в ретроспективной форме, то есть на оси абсцисс располагается временная шкала.

В центральной части представлена статистика по приложениям, которые использовал пользователь с информацией о суммарном количестве трафика по каждой категории приложений. Также на данной панели содержится информация о количестве используемых пользователем нежелательных, с точки зрения уровня риска, приложений.

В нижней части расположена статистика по протоколам (суммарное количество трафика) и суммарная информация по по посещению конкретных url- адресов.



	cp_app_name	ac_app_category	MB
1	SSL Protocol	Network Protocols	0.702193
2	Skype	VoIP	0.451646
3	DCE-RPC Protocol	Network Protocols	0.243588
4	Google Services	Web Services Provider	0.226089
5	Facebook	Social Networking	0.193920
6	YouTube	Media Sharing	0.122526
7	MSN-web	Search Engines / Portals	0.026777
8	Yahoo! Services	Web Services Provider	0.019721
9	Tor	Anonymizer	0.019623
10	Google Plus	Social Networking	0.009312

« prev 1 2 3 4 5 6 7 8 next »

	cp_app_name	ac_app_category	Количество запросов
1	BitTorrent Sync	P2P File Sharing	55
2	BitTorrent Protocol	P2P File Sharing	31
3	uTorrent	P2P File Sharing	31
4	Tor	Anonymizer	28

	cp_service	MB
1	http	16.149337
2	https	2.022584
3	tcp_135	0.244694

	cp_url_res	count
1	http://cdn.ap.bittorrent.com	32
2	http://counter.yadro.ru	21
3	http://i-29.b-41202.ut.bench.utorrent.com	13

Рисунок 12 – Контроль работы пользователей

Программный код, включая SPL запросы, посредством которых реализована данная информационная панель представлен в приложении (см. Приложение 3).

Мониторинг системы IPS

Данная информационная панель (см. Рисунок 13) предназначена для получения оперативно информации о работе системы IPS. В верхней части находится диаграмма, содержащая информацию о количестве атак во времени с разделением по типам атак.

В центральной части расположена статистика работы системы с информацией о типах атак, действии системы, ip-адресах назначения атак и их количестве. Данная панель содержит общий обзор о системе и предоставляет возможность в режиме реального времени контролировать работу системы.

В правом нижнем углу расположена таблица с информацией об основных типах атак с разбиением по конкретным офисам компании, что позволяет более детально анализировать состояние системы и возможные угрозы.

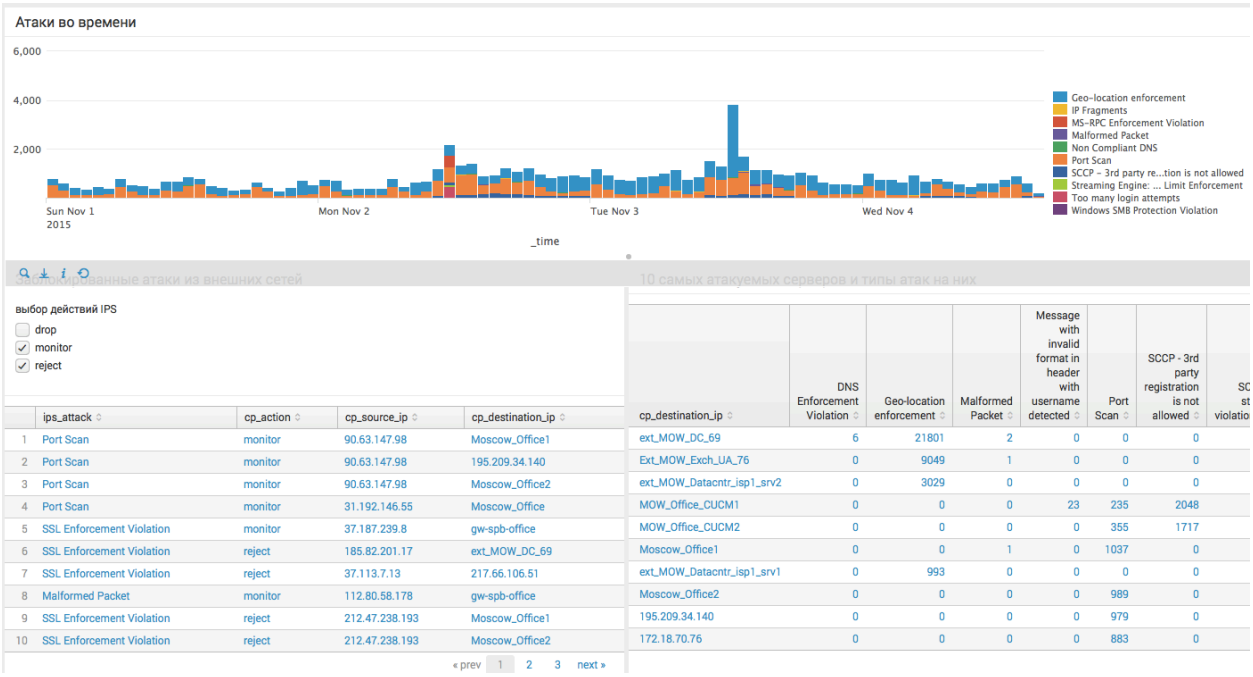


Рисунок 13 – Мониторинг системы IPS

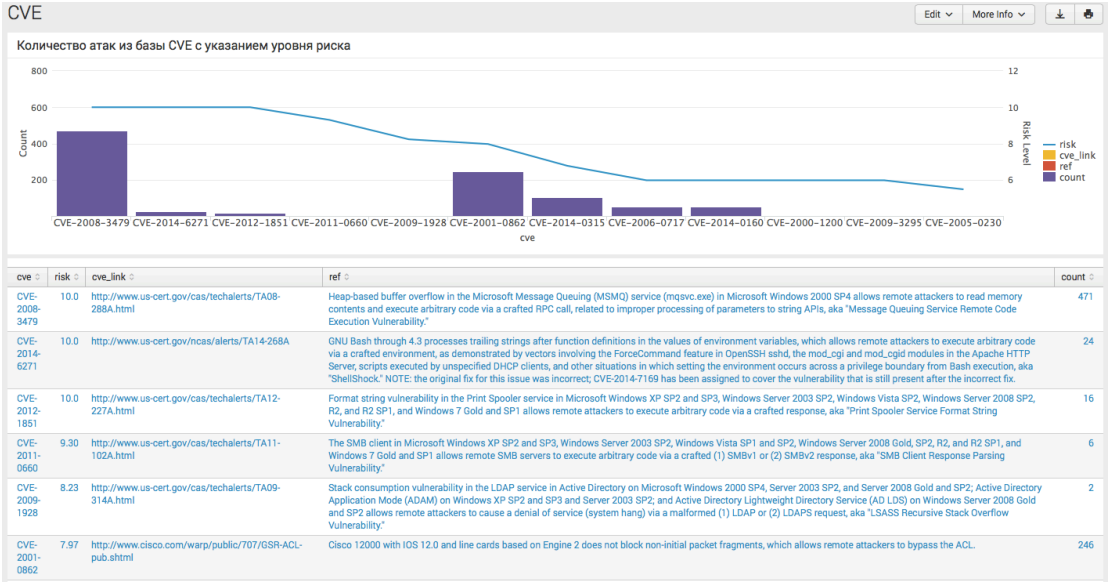
Программный код, включая SPL запросы, посредством которых реализована данная информационная панель представлен в приложении (см. Приложение 4).

Атаки и уязвимости из базы CVE

Представленная ниже информационная панель (см. Рисунок 14) является результатом обогащения лог-сообщений об атаках посредством общедоступных баз данных угроз. На графике по оси абсцисс указаны CVE коды атак, а по оси ординат их количество. Также с помощью кривой отображается уровень риска по каждой атаке посчитанный как среднее арифметическое от оценок угрозы из разных источников (CVSS, CWE).

В нижней части панели содержится статистика по каждой угрозе с указанием краткой информации о ней и ссылкой на официальный сайт разработчика программного обеспечения, где указаны возможные методы борьбы, действия для предотвращения, ссылки на обновление ПО.

Данная панель содержит наиболее опасные и важные угрозы, которые подлежат дальнейшему детальному анализу и обработке. На графике видно, что за выбранный промежуток времени (2 дня) пользователю предлагается рассмотреть порядка 5 угроз из нескольких тысяч лог-сообщений.



cve	risk	cve_link	ref	count
CVE-2008-3479	10.0	http://www.us-cert.gov/cas/techalerts/TA08-288A.html	Heap-based buffer overflow in the Microsoft Message Queuing (MSMQ) service (mqsvc.exe) in Microsoft Windows 2000 SP4 allows remote attackers to read memory contents and execute arbitrary code via a crafted RPC call, related to improper processing of parameters to string APIs, aka "Message Queuing Service Remote Code Execution Vulnerability."	471
CVE-2014-6271	10.0	http://www.us-cert.gov/ncas/alerts/TA14-268A	GNU Bash through 4.3 processes trailing strings after function definitions in the values of environment variables, which allows remote attackers to execute arbitrary code via a crafted environment, as demonstrated by vectors involving the ForceCommand feature in OpenSSH sshd, the mod_cgi and mod_cgid modules in the Apache HTTP Server, scripts executed by unspecified DHCP clients, and other situations in which setting the environment occurs across a privilege boundary from Bash execution, aka "ShellShock." NOTE: the original fix for this issue was incorrect; CVE-2014-7169 has been assigned to cover the vulnerability that is still present after the incorrect fix.	24
CVE-2012-1851	10.0	http://www.us-cert.gov/cas/techalerts/TA12-227A.html	Format string vulnerability in the Print Spooler service in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote attackers to execute arbitrary code via a crafted response, aka "Print Spooler Service Format String Vulnerability."	16
CVE-2011-0660	9.30	http://www.us-cert.gov/cas/techalerts/TA11-102A.html	The SMB client in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote SMB servers to execute arbitrary code via a crafted (1) SMBv1 or (2) SMBv2 response, aka "SMB Client Response Parsing Vulnerability."	6
CVE-2009-1928	8.23	http://www.us-cert.gov/cas/techalerts/TA09-314A.html	Stack consumption vulnerability in the LDAP service in Active Directory on Microsoft Windows 2000 SP4, Server 2003 SP2, and Server 2008 Gold and SP2; Active Directory Application Mode (ADAM) on Windows XP SP2 and SP3 and Server 2003 SP2; and Active Directory Lightweight Directory Service (AD LDS) on Windows Server 2008 Gold and SP2 allows remote attackers to cause a denial of service (system hang) via a malformed (1) LDAP or (2) LDAPS request, aka "LSASS Recursive Stack Overflow Vulnerability."	2
CVE-2001-0862	7.97	http://www.cisco.com/warp/public/707/GSR-ACL-pub.shtml	Cisco 12000 with IOS 12.0 and line cards based on Engine 2 does not block non-initial packet fragments, which allows remote attackers to bypass the ACL.	246

Рисунок 14 – Атаки и уязвимости из базы CVE

Таким образом, разработанный в рамках данного исследования модуль, содержащий описанные выше информационные панели, способен обеспечивать информационную поддержку работы шлюза информационной безопасности Check Point, контролировать возникновение различных угроз, отслеживать их ключевые показатели и предоставлять возможность информацию аналитику для принятия соответствующих управленческих решений.

Заключение

В результате данного исследования было разработано приложение, представляющее собой набор информационных панелей реагирования, предназначенных для мониторинга работы шлюза безопасности Check Point и принятия управленческих решений, реализованное посредством системы анализа лог-данных Splunk. Данное приложение может использоваться аналитиками отдела безопасности среднего предприятия для анализа работы системы, выявления закономерностей и критических ошибок системы с целью предотвращения угроз безопасности. Также разработанный модуль предоставляет возможность осуществлять контроль за действиями сотрудников компании в интернете, в частности позволяет получать информацию о посещенных сайтах, используемых приложениях и объеме трафика.

Для достижения поставленной цели данной выпускной квалификационной работы были выявлены и систематизированы основные типы программных угроз информационной безопасности, методы и технологии борьбы с ними и произведен анализ функциональных возможностей шлюза безопасности Check Point, в результате чего удалось выявить необходимость проведения процедур мониторинга работы системы, с целью выявления основных атак и улучшения превентивных мер.

Исходя из того, что разработанная информационная панель построена на основе лог-данных, генерируемых системой безопасности Check Point, в ходе данной работы был произведен подробный анализ структуры лог-сообщений данной системы и выявлены основные поля, на основе которых были разработаны исследуемые показатели.

Для разработки информационной панели, в соответствии с выделенными критериями, была выбрана система анализа лог-данных Splunk, в рамках которой, с помощью интеграции с общедоступными базами данных угроз (CVE, CVSS, CWE) и сканером уязвимостей Nessus, был произведен процесс обогащения лог-данных и практически решена проблема избыточности информации о нерелевантных атаках на систему.

В качестве перспектив для дальнейшего исследования в данной области можно выделить такие вопросы как доработка разработанного модуля, в частности улучшение алгоритма фильтрации наиболее важных угроз, добавление новых источников данных об уязвимостях системы, создание системы уведомлений для оперативного контроля.

Список литературы

1 **Adam Hils Greg Young, Jeremy D'Hoinne** Magic Quadrant for Enterprise Network Firewalls [В Интернете] // Garnter. - Garnter, 22 April 2015 г.. - 11 March 2016 г.. - https://www.gartner.com/doc/3035319?ref=SiteSearch&sthkw=firewall&fnl=search&srcId=1-3478922254.

2 **AltirixSystems** Внедрение системы управления информационной безопасностью [В Интернете] // Альтирикс системс. - 2015 г.. - 10 Апрель 2016 г.. - http://altirix.ru/index.php/services/vnedrenie-sistemy-upravleniya.

3 **Anti-Malware** Intrusion Detection/Prevention System (IDS/IPS) [В Интернете] // Anti-Malware. - 2016 г.. - 2 Май 2016 г.. - https://www.anti-malware.ru/IDS_IPS.

4 **Anti-Malware** Сетевая безопасность (Network security) [В Интернете]. - 2015 г.. - 9 март 2016 г.. - https://www.anti-malware.ru/network_security#.

5 **Ashford Warwick** Malware deliberately loaded into pirated or counterfeit software is expected cost enterprises $491bn in 2014 [В Интернете] // ComputerWeekly. - 19 04 2014 г.. - 15 01 2016 г.. - http://www.computerweekly.com/news/2240216380/Pirated-software-malware-to-cost-business-491-in-2014-study-shows.

6 **AV-Comparatieves** IT Security Survey [В Интернете] // Infepemdet Test of Anti-Virus Software. - 15 March 2013 г.. - http://www.av-comparatives.org/wp-content/uploads/2013/03/security_survey2013_en.pdf.

7 **AV-Comparatives** Опрос по вопросам безопасности за 2015 год [В Интернете] // Infepemdet Test of Anti-Virus Software. - 18 Март 2015 г.. - http://www.av-comparatives.org/wp-content/uploads/2015/03/security_survey2015_ru.pdf.

8 **Aycock John** Computer Viruses and Malware [Книга]. - Calgary : Springer, 2006.

9 **Bruce J. Neubauer, James D. Harris** Protection of computer systems from computer viruses: ethical and practical issues [Журнал] // Journal of Computing Sciences in Colleges. - 2002 г.. - стр. 270.

10 **CBS Interactive Inc** Most popular in Antivirus Software [В Интернете] // Cnet. - 5 November 2015 г.. - http://download.cnet.com/windows/antivirus-software/most-popular/3101-2239_4-0.html.

11 **CheckPoint** Next Generation Threat Prevention Software Bundles [В Интернете] // Check Point. - 1 January 2016 г.. - 10 April 2016 г.. - https://www.checkpoint.com/products/next-generation-threat-prevention/index.html.

12 **DrWeb** «Доктор Веб»: обзор вирусной активности в августе 2015 года [В Интернете] // DrWeb. - 28 Август 2015 г.. - http://news.drweb.ru/show/review/?lng=ru&i=9541.

13 **Few S.** Common pitfalls in Dashboard Design [Книга]. - Boise : Perceptual Edge, 2006.

14 **Few S.** Information Dashboard Desigh. The effective Visual Communacation of Data [Книга]. - Sebastopol : O'REILLY, 2006.

15 **Дрозд Алексей** Обзор SIEM-систем на мировом и российском рынке [В Интернете] // Anti-Malware. - 6 Июнь 2014 г.. - 14 Март 2016 г.. - https://www.anti-malware.ru/analytics/Technology_Analysis/Overview_SECURITY_systems_global_and_Russian_market.

16 **Kaspersky Lab** Регулярные обновления антивирусных программ [В Интернете] // Kaspersky Lab. - 7 Ноябрь 2015 г.. - http://www.kaspersky.ru/internet-security-center/internet-safety/antivirus-updates.

17 **Kaspersky Lab** О вирусах: Общая информация [В Интернете] // Kaspersky Lab. - 19 Август 2013 г.. - http://support.kaspersky.ru/viruses/general/1870.

18 **Ludwig Mark A.** The Giant Black Book of Computer Viruses [Книга]. - [б.м.] : American Eagle, 1998.

19 **Malik S.** Network Security Principles and Practices [Книга]. - Indianapolis, USA : Cisco Press, 2002.

20 **Mick Jason** Windows 10 Hits 75 Million Users; Grows Nearly 4x as Fast as Windows 7 [В Интернете] // DailyTech. - 28 August 2015 г.. - http://www.dailytech.com/Windows+10+Hits+75+Million+Users+Grows+Nearly+4x+as+Fast+as+Windows+7/article37476.htm.

21 **Nachenberg Carey** Computer virus-antivirus coevolution [Журнал] // Communications of the ACM. - 1997 г.. - стр. 46-47.

22 **OPSWAT Inc** OPSWAT Market Share Reports [В Интернете] // OPSWAT. - January 2015 г.. - https://www.opswat.com/resources/reports/antivirus-and-compromised-device-january-2015.

23 **Peltier Thomas R.** Information Security Fundamentals [Книга]. - [б.м.] : CRC Press, 2013.

24 **Peter Firstbrook, John Girard, Neil MacDonald** Magic Quadrant for Endpoint Protection Platforms [В Интернете] // Gartner. - 22 December 2014 г. http://www.gartner.com/technology/reprints.do?id=1-26F1285&ct=141223&st=sb.

25 **Prince Matthew** The DDoS That Almost Broke the Internet [В Интернете] // CloudFrare. - 27 March 2013 г.. - 7 April 2016 г.. - https://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet/.

26 **Ralph Langner** Stuxnet: Dissecting a Cyberwarfare Weapon [Статья] // IEEE Security & Privacy. - [б.м.] : IEEE, 2011 г.. - 3 : Т. 9.

27 **Ritstein Charles** Executive Guide to Computer Viruses [Книга]. - [б.м.] : DIANE Publishing, 1992.

28 **Rivera Janessa** Gartner Says Worldwide Security Software Market Grew 5.3 Percent in 2014 [В Интернете] // Gartner. - 27 May 2015 г.. - http://www.gartner.com/newsroom/id/3062017.

29 **Securitylab** Невероятно простой трюк социальной инженерии стоил банку 70 млн евро [В Интернете] // Securitylab by Positive Technologies. - 26 Январь 2016 г.. - 10 Апрель 2016 г.. - http://www.securitylab.ru/news/478953.php.

30 **Sotiris Ioannidis Angelos D. Keromytis, Steve M. Bellovin, Jonathan M. Smith** 7th ACM conference on Computer and communications security [Конференция] // Implementing a distributed firewall. - [б.м.] : ACM, 2000.

31 **TAdviser** Информационная безопасность (рынок России) [В Интернете]. - 10 08 2015 http://www.tadviser.ru/index.php/Статья:Информационная_безопасность_рынок_России

32 **Vacca John R.** Computer and Information Security [Книга]. - Waltham : Elsevier, 2013.

33 **YourPrivateNetwork** Обеспечение информационной безопасности сетей [В Интернете] // Лаборатория Сетевой Безопасности. - 9 Август 2009 г.. - 13 Апрель 2016 г.. - http://ypn.ru/146/securing-networking-information/.

34 **Zeltser Lenny** How antivirus software works: Virus detection techniques [В Интернете] // TechTarget. - October 2011 г.. - http://searchsecurity.techtarget.com/tip/How-antivirus-software-works-Virus-detection-techniques.

35 **ГОСТ-50922-2006** Защита информации. Основные термины и определения.

36 **Горобец А.А., Куницкий А.В., Парфентий А.Н., Чувило О.А.** Проблемы антивирусной индустрии, методы борьбы с компьютерными угрозами и ближайшие перспективы развития [Журнал] // Радиоэлектроника и информатика. - 2006 г.. - стр. 38-43.

37 **Зобнин Евгений** Методы борьбы с DoS-атаками [В Интернете] // Журнал «Хакер». - 14 Октябрь 2009 г.. - 21 Февраль 2016 г.. - https://xakep.ru/2009/10/14/49752/.

38 **Кривцов А.Н. Гультяев А.К., Ткаченко Б.И.** Безопасность информационных систем [Книга]. - Санкт-Петербург : ОЦЭиМ, 2006.

39 **Лапонина О. Р.** Основы сетевой безопасности. Криптографические алгоритмы и протоколы взаимодействия [Книга]. - Москва : Бином, 2009.

40 **Орлов Сергей** Шлюзы безопасности: новая волна [В Интернете] // Журнал сетевых решений LAN. - 2010 г.. - 1 Март 2016 г.. - http://www.osp.ru/lan/2010/09/13004319/.

41 **Парфентьев Алексей** Обзор SIEM-систем на мировом и российском рынке [В Интернете] // Anti-Malware. - 06 07 2014 г.. - https://www.anti-

malware.ru/analytics/Technology_Analysis/Overview_SECURITY_systems_global_and_Russian_market#.

42 **Романов Михаил** Рынок систем сетевой безопасности, аппаратных средств двухфакторной аутентификации и инструментальных средств анализа защищенности в России [В Интернете] // Anti-Malware. - 12 Апрель 2013 г.. - 2 Май 2016 г.. - https://www.anti-malware.ru/node/11550.

43 **Шпунт Яков** Таргетированные атаки и как с ними бороться [В Интернете] // Intelligent Enterprise. - 05 Февраль 2015 г.. - 1 Март 2016 г.. - http://www.iemag.ru/analitics/detail.php?ID=32831.

Приложение

Приложение 1. Интегральная оценка Фишберна

Для оценки систем, в ходе обсуждения заказчиком ключевых критериев оценивания, были выбраны следующие факторы:

1. «Поддержка, возможность интеграции с другими офисными пакетами»;
2. «Богатство графической визуализации данных»;
3. «Возможность подключения сборок, расширений, разработанных на языках программирования»;
4. «Возможность работы с большими объемами данных»;
5. «Возможность DrillDown на графиках»;
6. «Возможность анализа информации в режиме реального времени»;
7. «Широкая интеграция с системой Check Point»;
8. «Наличие большого количества книг, тематических сайтов».

Из данных факторов были сформированы следующие группы:

1. B_1– основные факторы (4,5,7);
2. B_2– важные факторы (2,3);
3. B_3– вспомогательные факторы (1,6);
4. B_4– несущественные факторы (8).

Была произведена количественная оценка каждого фактора:

Критерий оценки	**Количественная оценка важности**
«Возможность DrillDown на графиках»	0,145
«Широкая интеграция с системой Check Point»	0,145
«Возможность работы с большими объемами данных»	0,145
«Богатство графической визуализации данных»	0,127
«Возможность подключения сборок, расширений, разработанных на языках программирования»	0,127
«Возможность анализа информации в режиме реального времени»	0,11
«Поддержка, возможность интеграции с другими офисными пакетами»	0,11
«Наличие большого количества книг, тематических сайтов»	0,09

Факторы были сгруппированы по степени их учета в системе:

1. G_1– группа факторов, явно учитываемых в системе (2,4,5,7);
2. G_2– группа факторов, учитываемых в системе не явно (3,6);
3. G_3– группа факторов, учитываемых для перспективы развития системы (1);
4. G_4– группа факторов, не учитываемая в системе (8).

Далее были определены и пронумерованы количественные оценки Фишберна степени учета факторов:

Группа	Оценка	Нормированная оценка
B_1	0,4	1
B_2	0,3	0,7
B_3	0,2	0,3
B_4	0,1	0

Далее на основе конкретных систем был произведен расчет интегральной оценки:

Наименование системы	Интегральная оценка Фишберна
IBM q1Labs	0,494
Loggly	0,349
Splunk	**0,731**

Приложение 2. Информационная панель «Контроль работы приложений»

```
<form>
  <label>App Control main</label>
  <fieldset submitButton="true">
    <input type="time" token="field1" searchWhenChanged="true">
      <label></label>
      <default>
        <earliest>0</earliest>
        <latest></latest>
      </default>
    </input>
    <input type="multiselect" token="field_orig"
searchWhenChanged="true">
      <label>Выбор домена</label>
      <choice value="gw-spb-warehouse">Спб – склад</choice>
      <choice value="gw-spb-office">Спб – офис</choice>
      <choice value="gw_MOW_warehouse1">Мск – склад</choice>
      <choice value="Moscow_Office1">Мск – офис1</choice>
      <choice value="Moscow_Office2">Мск – офис2</choice>
      <choice value="Ukraine_warehouse">Украина – склад</choice>
      <choice value="Ukraine_Office1">Украина – офис1</choice>
      <choice value="Ukraine_Office2">Украина – офис2</choice>
      <choice value="gw-almaty">Алма-ата – офис</choice>
      <choice value="Datacenter1">ЦОД1</choice>
```

```
      <choice value="Datacenter2">ЦОД2</choice>
      <delimiter> OR </delimiter>
    </input>
  </fieldset>
  <row>
    <panel>
      <chart>
        <title>Количество событий по риску</title>
        <search>
          <query>index=test sourcetype=opsec:application_control
OR sourcetype=opsec:url_filtering $field_orig$ | stats count by
cp_app_risk</query>
          <earliest>0</earliest>
        </search>
        <option name="charting.chart">pie</option>
        <option
name="charting.axisLabelsX.majorLabelStyle.overflowMode">ellipsi
sNone</option>
        <option
name="charting.axisLabelsX.majorLabelStyle.rotation">0</option>
        <option
name="charting.axisTitleX.visibility">visible</option>
        <option
name="charting.axisTitleY.visibility">visible</option>
        <option
name="charting.axisTitleY2.visibility">visible</option>
        <option name="charting.axisX.scale">linear</option>
        <option name="charting.axisY.scale">linear</option>
        <option name="charting.axisY2.enabled">0</option>
        <option name="charting.axisY2.scale">inherit</option>
        <option
name="charting.chart.bubbleMaximumSize">50</option>
        <option
name="charting.chart.bubbleMinimumSize">10</option>
        <option name="charting.chart.bubbleSizeBy">area</option>
        <option
name="charting.chart.nullValueMode">gaps</option>
        <option
name="charting.chart.showDataLabels">none</option>
        <option
name="charting.chart.sliceCollapsingThreshold">0.01</option>
        <option name="charting.chart.stackMode">default</option>
        <option name="charting.chart.style">shiny</option>
        <option name="charting.drilldown">all</option>
        <option name="charting.layout.splitSeries">0</option>
        <option
name="charting.layout.splitSeries.allowIndependentYRanges">0</op
tion>
        <option
name="charting.legend.labelStyle.overflowMode">ellipsisMiddle</o
ption>
        <option name="charting.legend.placement">right</option>
      </chart>
    </panel>
```

```
    <panel>
      <chart>
        <title>Количество событий по приложениям-протоколам</title>
        <search>
          <query>index=test sourcetype=opsec:application_control
OR sourcetype=opsec:url_filtering $field_orig$ | stats count by
cp_app_name</query>
          <earliest>0</earliest>
        </search>
        <option name="charting.chart">pie</option>
        <option
name="charting.axisLabelsX.majorLabelStyle.overflowMode">ellipsi
sNone</option>
        <option
name="charting.axisLabelsX.majorLabelStyle.rotation">0</option>
        <option
name="charting.axisTitleX.visibility">visible</option>
        <option
name="charting.axisTitleY.visibility">visible</option>
        <option
name="charting.axisTitleY2.visibility">visible</option>
        <option name="charting.axisX.scale">linear</option>
        <option name="charting.axisY.scale">linear</option>
        <option name="charting.axisY2.enabled">0</option>
        <option name="charting.axisY2.scale">inherit</option>
        <option
name="charting.chart.bubbleMaximumSize">50</option>
        <option
name="charting.chart.bubbleMinimumSize">10</option>
        <option name="charting.chart.bubbleSizeBy">area</option>
        <option
name="charting.chart.nullValueMode">gaps</option>
        <option
name="charting.chart.showDataLabels">none</option>
        <option
name="charting.chart.sliceCollapsingThreshold">0.01</option>
        <option name="charting.chart.stackMode">default</option>
        <option name="charting.chart.style">shiny</option>
        <option name="charting.drilldown">all</option>
        <option name="charting.layout.splitSeries">0</option>
        <option
name="charting.layout.splitSeries.allowIndependentYRanges">0</op
tion>
        <option
name="charting.legend.labelStyle.overflowMode">ellipsisMiddle</o
ption>
        <option name="charting.legend.placement">right</option>
      </chart>
    </panel>
  </row>
  <row>
    <panel>
      <table>
        <title>Топ пользователей по количеству нежелательных
```

```
приложений</title>
        <search>
          <query>index=test sourcetype =
opsec:application_control OR sourcetype = opsec:url_filtering
cp_app_risk&gt;3 gw-spb-warehouse OR gw-spb-office | eval
user_rep = if ( isnotnull ( cp_user ) , cp_user , cp_source_ip )
| stats count by user_rep, ac_app_category, cp_app_name | sort -
count | rename count as "Количетсво событий", user_rep AS
"Идентификатор пользователя", ac_app_category AS "Категория",
cp_app_name AS "Название"</query>
          <earliest>0</earliest>
          <latest></latest>
        </search>
        <option name="wrap">undefined</option>
        <option name="rowNumbers">undefined</option>
        <option name="drilldown">row</option>
        <option name="dataOverlayMode">none</option>
        <option name="count">10</option>
        <drilldown target="My New Window">

<link>user_appctrl_url_report?form.user_field=$click.value$</lin
k>
        </drilldown>
      </table>
    </panel>
    <panel>
      <table>
        <title>Топ пользователей по объему скаченного</title>
        <search>
          <query>index=test sourcetype =
opsec:application_control OR sourcetype = opsec:url_filtering
$field_orig$ | eval user_rep = if ( isnotnull ( cp_user ) ,
cp_user , cp_source_ip ) | eval cp_mb = cp_bytes/1024/1024 |
stats sum(cp_mb) AS SumMB by user_rep | sort -SumMB | rename
user_rep as "Идентификатор пользователя", SumMB as "Объем данных,
МБ"</query>
          <earliest>0</earliest>
          <latest></latest>
        </search>
        <option name="wrap">undefined</option>
        <option name="rowNumbers">undefined</option>
        <option name="drilldown">row</option>
        <drilldown target="My New Window">

<link>user_appctrl_url_report?form.user_field=$click.value$</lin
k>
        </drilldown>
        <option name="dataOverlayMode">none</option>
        <option name="count">10</option>
      </table>
    </panel>
  </row>
    </form>
```

Приложение 3. Информационная панель «Контроль работы пользователей»

```
<form>
  <label>User_appctrl_url_report</label>
  <fieldset submitButton="true">
    <input type="text" token="user_field">
      <label>User name / IP</label>
    </input>
    <input type="time" token="field3">
      <label></label>
      <default>
        <earliest>0</earliest>
        <latest></latest>
      </default>
    </input>
  </fieldset>
  <row>
    <panel>
      <chart>
        <title>График запросов</title>
        <search>
          <query>index=* sourcetype=opsec:application_control OR
sourcetype = opsec:url_filtering | eval
user_rep=if(isnotnull(cp_user), cp_user, cp_source_ip) | eval
cp_mb = cp_bytes/1024/1024 | search user_rep="$user_field$" |
timechart count by cp_action</query>
          <earliest>0</earliest>
        </search>
        <option name="charting.chart">area</option>
        <option name="charting.axisY2.enabled">1</option>
        <option
name="charting.axisLabelsX.majorLabelStyle.overflowMode">ellipsi
sNone</option>
        <option
name="charting.axisLabelsX.majorLabelStyle.rotation">0</option>
        <option
name="charting.axisTitleX.visibility">visible</option>
        <option
name="charting.axisTitleY.visibility">visible</option>
        <option
name="charting.axisTitleY2.visibility">visible</option>
        <option name="charting.axisX.scale">linear</option>
        <option name="charting.axisY.scale">linear</option>
        <option name="charting.axisY2.scale">linear</option>
        <option
name="charting.chart.bubbleMaximumSize">50</option>
        <option
name="charting.chart.bubbleMinimumSize">10</option>
        <option name="charting.chart.bubbleSizeBy">area</option>
        <option
name="charting.chart.nullValueMode">connect</option>
        <option
name="charting.chart.sliceCollapsingThreshold">0.01</option>
        <option name="charting.chart.stackMode">default</option>
        <option name="charting.chart.style">shiny</option>
```

```
        <option name="charting.drilldown">none</option>
        <option name="charting.layout.splitSeries">0</option>
        <option
name="charting.legend.labelStyle.overflowMode">ellipsisMiddle</o
ption>
        <option name="charting.legend.placement">right</option>
        <option
name="charting.chart.showDataLabels">none</option>
        <option
name="charting.layout.splitSeries.allowIndependentYRanges">0</op
tion>
        <option
name="charting.chart.overlayFields">inform,block,redirect</optio
n>
      </chart>
    </panel>
    <panel>
      <chart>
        <title>Использование трафика</title>
        <search>
          <query>index=* sourcetype=opsec:application_control OR
sourcetype = opsec:url_filtering | eval
user_rep=if(isnotnull(cp_user), cp_user, cp_source_ip) | eval
cp_mb = cp_bytes/1024/1024 | search user_rep="$user_field$" |
timechart sum(cp_mb)</query>
          <earliest>0</earliest>
        </search>
        <option name="wrap">undefined</option>
        <option name="rowNumbers">undefined</option>
        <option
name="charting.axisLabelsX.majorLabelStyle.overflowMode">ellipsi
sNone</option>
        <option
name="charting.axisLabelsX.majorLabelStyle.rotation">0</option>
        <option
name="charting.axisTitleX.visibility">visible</option>
        <option
name="charting.axisTitleY.visibility">visible</option>
        <option
name="charting.axisTitleY2.visibility">visible</option>
        <option name="charting.axisX.scale">linear</option>
        <option name="charting.axisY.scale">linear</option>
        <option name="charting.axisY2.enabled">0</option>
        <option name="charting.axisY2.scale">inherit</option>
        <option name="charting.chart">area</option>
        <option
name="charting.chart.bubbleMaximumSize">50</option>
        <option
name="charting.chart.bubbleMinimumSize">10</option>
        <option name="charting.chart.bubbleSizeBy">area</option>
        <option
name="charting.chart.nullValueMode">gaps</option>
        <option
name="charting.chart.sliceCollapsingThreshold">0.01</option>
```

```
        <option name="charting.chart.stackMode">default</option>
        <option name="charting.chart.style">shiny</option>
        <option name="charting.drilldown">all</option>
        <option name="charting.layout.splitSeries">0</option>
        <option
name="charting.legend.labelStyle.overflowMode">ellipsisMiddle</o
ption>
        <option name="charting.legend.placement">right</option>
        <option
name="charting.chart.showDataLabels">none</option>
        <option
name="charting.layout.splitSeries.allowIndependentYRanges">0</op
tion>
      </chart>
    </panel>
  </row>
  <row>
    <panel>
      <table>
        <title>Статистика по трафику по приложениям</title>
        <search>
          <query>index=* sourcetype=opsec:application_control OR
sourcetype = opsec:url_filtering | eval
user_rep=if(isnotnull(cp_user), cp_user, cp_source_ip) | eval
cp_mb = cp_bytes/1024/1024 | search user_rep="$user_field$" |
stats sum(cp_mb) AS MB by cp_app_name, ac_app_category | sort -
MB</query>
          <earliest>0</earliest>
          <latest></latest>
        </search>
        <option name="wrap">undefined</option>
        <option name="rowNumbers">undefined</option>
        <option name="drilldown">row</option>
        <option name="dataOverlayMode">none</option>
        <option name="count">10</option>
      </table>
    </panel>
    <panel>
      <table>
        <title>Количество запросов критичных для бизнеса
приложений</title>
        <search>
          <query>index=* sourcetype=opsec:application_control OR
sourcetype = opsec:url_filtering | eval
user_rep=if(isnotnull(cp_user), cp_user, cp_source_ip) | eval
cp_mb = cp_bytes/1024/1024 | search user_rep="$user_field$"
cp_app_risk&amp;gt;3 | stats count AS "Количество запросов" by
cp_app_name, ac_app_category | sort -"Количество
запросов"</query>
          <earliest>0</earliest>
          <latest></latest>
        </search>
        <option name="wrap">undefined</option>
        <option name="rowNumbers">undefined</option>
```

```
        <option name="drilldown">row</option>
        <option name="dataOverlayMode">none</option>
        <option name="count">10</option>
      </table>
    </panel>
  </row>
  <row>
    <panel>
      <table>
        <title>Статистика по сервисам и трафику</title>
        <search>
          <query>index=* sourcetype=opsec:application_control OR
sourcetype = opsec:url_filtering | eval
user_rep=if(isnotnull(cp_user), cp_user, cp_source_ip) | eval
cp_mb = cp_bytes/1024/1024 | search user_rep="$user_field$" |
stats sum(cp_mb) AS MB by cp_service | sort -MB</query>
          <earliest>0</earliest>
          <latest></latest>
        </search>
        <option name="wrap">undefined</option>
        <option name="rowNumbers">undefined</option>
</table>
    </panel>
    <panel>
      <table>
        <title>Сайты посещенные</title>
        <search>
          <query>index=* sourcetype=opsec:application_control OR
sourcetype = opsec:url_filtering | eval
user_rep=if(isnotnull(cp_user), cp_user, cp_source_ip) | eval
cp_mb = cp_bytes/1024/1024 | search user_rep="$user_field$" |
rex field=cp_resource
"(?&lt;cp_url_res&gt;(http)s*(\:\/\/)[^\/]*)" | stats count by
cp_url_res | sort -count</query>
          <earliest>0</earliest>
          <latest></latest>
        </search>
        <option name="wrap">undefined</option>
        <option name="rowNumbers">undefined</option>
<option name="count">10</option>
      </table>
    </panel>
  </row>
</form>
```

Приложение 4. Информационная панель «Контроль работы пользователей»

```
<form>
  <label>IPS обзор</label>
  <fieldset submitButton="true" autoRun="false">
    <input type="time" token="field1" searchWhenChanged="true">
      <label></label>
      <default>
        <earliest></earliest>
        <latest></latest>
      </default>
    </input>
  </fieldset>
  <row>
    <panel>
      <title>Атаки во времени</title>
      <chart>
        <search>
          <query>index=test sourcetype = "opsec:ips" | timechart
count by ips_attack usenull=f useother=f</query>
        </search>
        <option
name="charting.axisLabelsX.majorLabelStyle.overflowMode">ellipsi
sNone</option>
        <option
name="charting.axisLabelsX.majorLabelStyle.rotation">0</option>
        <option
name="charting.axisTitleX.visibility">visible</option>
        <option
name="charting.axisTitleY.visibility">visible</option>
        <option
name="charting.axisTitleY2.visibility">visible</option>
        <option name="charting.axisX.scale">linear</option>
        <option name="charting.axisY.scale">linear</option>
        <option name="charting.axisY2.enabled">0</option>
        <option name="charting.axisY2.scale">inherit</option>
        <option name="charting.chart">column</option>
        <option
name="charting.chart.bubbleMaximumSize">50</option>
        <option
name="charting.chart.bubbleMinimumSize">10</option>
        <option name="charting.chart.bubbleSizeBy">area</option>
        <option
name="charting.chart.nullValueMode">gaps</option>
        <option
name="charting.chart.showDataLabels">none</option>
        <option
name="charting.chart.sliceCollapsingThreshold">0.01</option>
        <option name="charting.chart.stackMode">stacked</option>
        <option name="charting.chart.style">shiny</option>
        <option name="charting.drilldown">all</option>
        <option name="charting.layout.splitSeries">0</option>
        <option
name="charting.layout.splitSeries.allowIndependentYRanges">0</op
tion>
```

```
        <option
name="charting.legend.labelStyle.overflowMode">ellipsisMiddle</o
ption>
        <option name="charting.legend.placement">right</option>
      </chart>
    </panel>
  </row>
  <row>
    <panel>
      <title>Заблокированные атаки из внешних сетей</title>
      <input type="checkbox" token="field_inp_act_ips">
        <label>выбор действий IPS</label>
        <choice value="drop">drop</choice>
        <choice value="monitor">monitor</choice>
        <choice value="reject">reject</choice>
        <delimiter> OR </delimiter>
      </input>
      <table>
        <search>
          <query>index=test sourcetype = "opsec:ips"
cp_action=$field_inp_act_ips$ | regex cp_source_ip !=
"(192.168)|(172.(1[8-9]|2[0-9]|3[0-1]))|(10)|[a-zA-Z]" | dedup
ips_attack cp_action cp_destination_ip | table ips_attack,
cp_action, cp_source_ip, cp_destination_ip</query>
          <earliest></earliest>
          <latest></latest>
        </search>
        <option name="wrap">true</option>
        <option name="rowNumbers">true</option>
        <option name="dataOverlayMode">none</option>
        <option name="drilldown">cell</option>
        <option name="count">10</option>
      </table>
    </panel>
    <panel>
      <title>10 самых атакуемых серверов и типы атак на
них</title>
      <table>
        <search>
          <query>index=test sourcetype = "opsec:ips" [ search
index=test sourcetype = "opsec:ips" | top 10 cp_destination_ip |
fields + cp_destination_ip ] | chart count over
cp_destination_ip by ips_attack | addtotals fieldname=total |
sort -total  | fields - total</query>
          <earliest>0</earliest>
        </search>
        <option
name="charting.axisLabelsX.majorLabelStyle.overflowMode">ellipsi
sNone</option>
        <option
name="charting.axisLabelsX.majorLabelStyle.rotation">0</option>
        <option
name="charting.axisTitleX.visibility">visible</option>
        <option
```

```
name="charting.axisTitleY.visibility">visible</option>
        <option
name="charting.axisTitleY2.visibility">visible</option>
        <option name="charting.axisX.scale">linear</option>
        <option name="charting.axisY.scale">linear</option>
        <option name="charting.axisY2.enabled">0</option>
        <option name="charting.axisY2.scale">inherit</option>
        <option name="charting.chart">column</option>
        <option
name="charting.chart.bubbleMaximumSize">50</option>
        <option
name="charting.chart.bubbleMinimumSize">10</option>
        <option name="charting.chart.bubbleSizeBy">area</option>
        <option
name="charting.chart.nullValueMode">gaps</option>
        <option
name="charting.chart.showDataLabels">none</option>
        <option
name="charting.chart.sliceCollapsingThreshold">0.01</option>
        <option name="charting.chart.stackMode">stacked</option>
        <option name="charting.chart.style">shiny</option>
        <option name="charting.drilldown">all</option>
        <option name="charting.layout.splitSeries">0</option>
        <option
name="charting.layout.splitSeries.allowIndependentYRanges">0</op
tion>
        <option
name="charting.legend.labelStyle.overflowMode">ellipsisMiddle</o
ption>
        <option name="charting.legend.placement">right</option>
          <option name="drilldown">cell</option>
      </table>
    </panel>
  </row>
  <row>
    <panel>
      <title>Атаки из базы CVE</title>
      <table>
        <search>
          <query>index = test sourcetype = "opsec:ips"
ips_industry_reference=* | top ips_industry_reference,
ips_protection_name, cp_source_ip, cp_destination_ip limit=20 |
fields - percent | rename count as "Количество
срабатываний"</query>
          <earliest>0</earliest>
          <latest></latest>
        </search>
        <option name="wrap">true</option>
        <option name="dataOverlayMode">none</option>
        <option name="count">10</option>
      </table>
    </panel>
  </row>
</form>
```