УДК 004.056.53
Doi: 10.31772/2587-6066-2018-19-3-412-422

Для цитирования: Кулясов Н. В., Исаев С. В. Исследование сетевых аномалий корпоративной сети Красноярского научного центра // Сибирский журнал науки и технологий. 2018. Т. 19, № 3. С. 412–422. Doi: 10.31772/2587-6066-2018-19-3-412-422

For citation: Kulyasov N. V., Isaev S. V. [Investigation of the network anomalies of the corporate network of Krasnoyarsk scientific center]. *Siberian Journal of Science and Technology*. 2018, Vol. 19, No. 3, P. 412–422 (In Russ.). Doi: 10.31772/2587-6066-2018-19-3-412-422

ИССЛЕДОВАНИЕ СЕТЕВЫХ АНОМАЛИЙ КОРПОРАТИВНОЙ СЕТИ КРАСНОЯРСКОГО НАУЧНОГО ЦЕНТРА

Н. В. Кулясов*, С. В. Исаев

Институт вычислительного моделирования СО РАН
Российская Федерация, 660036, г. Красноярск, Академгородок, 50/44
*E-mail: razor@icm.krasn.ru

Решается задача обеспечения безопасности корпоративной сети научно-исследовательской организации. Обоснована актуальность поддержки превентивных мер защиты сетевых ресурсов для организаций, выполняющих научную поддержку высокотехнологичного производства, проведения космических исследований и создания наукоемкого оборудования, где потеря конфиденциальных данных при несанкционированных внешних воздействиях может привести к существенным последствиям. Для решения задачи предложено проводить анализ аномалий сетевого трафика, которые могут свидетельствовать о возникновении киберугроз.

Выполнен обзор существующих методов и программных продуктов, предназначенных для анализа сетевых аномалий. На их основе предложен собственный оригинальный программный инструмент, позволяющий автоматически выполнять обнаружение аномалий и проводить последующий детальный анализ журналов сетевых служб по выбранным администратором метрикам. Программный инструмент разработан в виде веб-приложения, интегрированного в действующую инфраструктуру корпоративной сети научной организации. Внедрение веб-приложения показало актуальность и востребованность развития системы обнаружения аномалий.

Для дальнейшего расширения методов защиты корпоративной сети разработано полнофункциональное программное обеспечение – автономная система анализа журналов, которая выполняет автоматический анализ и агрегацию данных сетевых служб и предоставляет интерактивные средства визуализации результатов. Система имеет удобный графический интерфейс, позволяющий наглядно оценивать статистику обнаруженных аномалий. При помощи программного инструмента администратор может выявлять наиболее критичные инциденты и пресекать их в дальнейшем, изменяя конфигурацию активных систем защиты.

Программное обеспечение содержит инструменты для построения диаграмм, отображающих количество аномалий за периоды времени, их распределение по наблюдаемым сервисам, источникам угроз. Оно показывает данные по активным клиентам, подверженным угрозам, частоту запросов по выбранным протоколам, отслеживает превышение пороговых значений и пр.

Применение разработанного программного обеспечения позволяет выполнять конфигурацию первой линии защиты от сетевых атак, повышает оперативность реагирования и эффективность предотвращения вторжений за счет выявления пропущенных стандартными средствами защиты инцидентов.

Ключевые слова: сетевые аномалии, кибербезопасность, система обнаружения аномалий, система обнаружения вторжений.

INVESTIGATION OF THE NETWORK ANOMALIES OF THE CORPORATE NETWORK OF KRASNOYARSK SCIENTIFIC CENTER

N. V. Kulyasov*, S. V. Isaev

Institute of Computational Modelling SB RAS
50/44, Academgorodok, Krasnoyarsk, 660036, Russian Federation
*E-mail: razor@icm.krasn.ru

The problem of securing the corporate network of a research organization is being solved. The urgency of supporting preventive measures for protecting network resources for the organizations performing scientific support of high-tech production, conducting space researches and creating high-tech equipment is grounded, where the loss of confi-

dential data with unauthorized external influence can lead to significant consequences. To solve the problem, it is suggested to analyze the anomalies of network traffic, which can indicate the occurrence of cyberthreats.

The paper reviews the existing methods and software products designed to analyze anomalies. On their basis, we propose our own original software tool that allows automatic detection of anomalies and subsequent detailed analysis of network service logs according to the metrics chosen by the administrator. The software tool is designed as a web application integrated into the existing infrastructure of the corporate network of a scientific organization. The implementation of the web application showed topicality and relevance of the development of an anomaly detection system.

To further expand the methods of protecting the corporate network, full-featured software has been developed (Autonomous Log Analysis System) that performs automatic analysis and aggregation of network services data and provides interactive means of visualizing results. The system has a convenient graphical interface that allows you to visually evaluate the statistics of detected anomalies. With the help of a software tool, the administrator can identify the most critical incidents and suppress them in the future, changing the configuration of active protection systems.

The software contains tools for constructing diagrams that show the number of anomalies over time periods, their distribution by observable services, sources of threats. It shows data on active clients exposed to threats, frequency of requests for selected protocols, monitors the exceeding of thresholds.

The application of the developed software allows the configuration of the first line of protection against network attacks, improves responsiveness and the effectiveness of intrusion prevention by detecting missed by standard means of protection of incidents.

Keywords: network anomalies, cybersecurity, anomaly detection system, intrusion detection system.

Введение. Развитие современных информационных технологий приводит к повышению уровня «цифровизации» и переводу в киберпространство научных и производственных процессов. Глобальные компьютерные сети глубоко интегрированы в деятельность различных предприятий. Оперативность доступа к информации способствует сокращению издержек производства, повышает эффективность и рентабельность компаний. С другой стороны, такая интеграция может привести к возникновению проблем и потере конфиденциальности данных при несанкционированных внешних воздействиях. Особенно актуальна такая проблема для высокотехнологичных производств, таких как космические исследовательские проекты, для которых обеспечение безопасности данных является одной из приоритетных задач сохранения конкурентоспособности отечественных космических разработок. В этой связи повышается нагрузка на корпоративные системы безопасности как предприятий космической отрасли, так и научно-исследовательских институтов, ведущих широкую научную работу с такими предприятиями. Например, в федеральном исследовательском центре «Красноярский научный центр Сибирского отделения Российской академии наук» на протяжении многих лет поддерживается тесное сотрудничество между научными подразделениями и предприятиями космической отрасли. Анализ сетевых угроз корпоративной сети научного центра [1] и обеспечение защиты сетевых ресурсов от несанкционированных вмешательств является актуальной задачей.

В данной статье предложены методы обнаружения сетевых угроз и описано программное обеспечение, предназначенное для формирования превентивных мер по защите корпоративной сети научного центра. Работа основана на исследовании аномалий сетевого трафика. Аномалия – это отступление или уклонение от общепринятых норм, поэтому аномальным называют все отступающее или уклоняющееся от правильного или нормального. Под сетевыми аномалиями понимаются отклонения в использовании сетевых ресурсов, доступ к которым предоставляется посредством веб-сервисов и сетевых приложений.

Обнаружение аномалий на сегодняшний день является одним из активно развивающихся направлений в области обеспечения кибербезопасности. Это связано с тем, что аномалии в большинстве случаев являются начальной стадией сетевых атак, которые могут повлечь как негативные нематериальные последствия, так и финансовые убытки для организаций, имеющих существенное представительство в киберпространстве. Как правило, такие аномалии являются результатом разведки или «пробой силы» для дальнейшего использования обнаруженных проблем в системе безопасности с целью получения коммерческой выгоды. Выявление и классификация аномалий предполагает непрерывный процесс мониторинга событий в компьютерных системах и сетях, в связи с чем требуется обработка больших объёмов данных, генерируемых этими источниками. Для этих целей используются автоматизированные системы обнаружения вторжений [2]. Существуют коммерческие программные продукты, которые позволяют анализировать трафик на предмет аномалий и угроз в реальном времени. Ограничивающими факторами использования таких систем является высокая стоимость и закрытая архитектура, что затрудняет их адаптацию под инфраструктуру организации.

Методам анализа аномалий сетевого трафика посвящен целый ряд современных научных исследований. Описываются современные типы систем обнаружения и различные техники детектирования сетевых атак и перспективные направления их развития [3]. Недостатками существующих систем также являются высокий уровень ложных срабатываний и сложность создания обучающей выборки. Использование обобщённой классификации [4] позволяет частично компенсировать первый недостаток, предоставляя

прозрачный набор признаков для идентификации аномалии. Для точного обнаружения аномалий используются различные аналитические алгоритмы. Например, метод каскадной кластеризации в объединении с деревьями решений [5] позволяет достигать высокой точности на экспериментальных данных с уровнем обнаружения аномалий выше 90 %. Гибридные методы обнаружения аномалий, основанные на нейронечетких и иммунных классификаторах [6], позволяют найти компромиссное решение между точностью обнаружения аномалий и поиском неизвестных типов угроз. Методы мультифакторного анализа временных рядов загруженности процессора [7] не показали высоких результатов и требуют точного подбора параметров для анализа. В работе [8] применялся метод кластеризации, использующий оценку плотности в пространстве характеристик событий. Построенная функция плотности позволила выделять области кластеров нормальных событий, и в случае, если событие не удовлетворяет ни одному кластеру, то классифицировать его как аномальное. Большинство рассмотренных работ имеют теоретическую направленность и высокий уровень сложности реализации предлагаемых методов и алгоритмов, что накладывает существенные ограничения при решении с их помощью практических задач обеспечения информационной безопасности.

В этой статье предложены программные средства для выполнения первичной автоматической классификации по источникам возникновения аномалий и инструменты для детального анализа по заданным метрикам. Такой подход потребовал разработки веб-приложения анализа журналов сетевых служб [9], интегрированного в действующую инфраструктуру корпоративной сети научного центра и обеспечивающего работу с минимальными затратами ресурсов. Построение веб-приложения анализа журналов и применение его на реальных данных показало актуальность развития подобных средств обеспечения веб-безопасности в корпоративной сети. Развитием данного подхода стало полнофункциональное программное обеспечение – автономная система анализа журналов сетевых служб. Новое программное обеспечение расширяет существующие средства обеспечения безопасности дополнительными сервисами, предназначенными для выявления аномалий на граничных участках инфраструктуры корпоративной сети. Использование этой системы позволяет выполнять конфигурацию первой линии защиты от сетевых атак за счет выявления пропущенных стандартными средствами защиты инцидентов, что повышает качество ее работы и оперативность реагирования.

Инструмент анализа журналов сетевых служб. Основой для создания веб-приложения анализа журналов сетевых служб служит дополненная модель обеспечения информационной безопасности (рис. 1). Модель расширяет существующую модель информационной безопасности научного центра за счет включения системы обработки журналов сетевых служб, предназначенной для обнаружения аномалий и выявления их источников.

Задача обеспечения информационной безопасности требует учитывать ограничения, основанные на политике безопасности организации [10], её технических средствах и финансовых ограничениях. Входным параметром данной модели служит взаимодействие пользователя с сетевыми службами организации, которое документируется в журналах обращений (лог-файлах). В свою очередь исполнителями выступают администраторы служб, уже интегрированные системы определения/предотвращения вторжений и предлагаемая система обработки журналов сетевых служб. В результате мы получаем список IP-адресов источников аномалий и потенциальных угроз безопасности.

Реализация модели информационной безопасности выполнена в виде сервисного программного обеспечения – инструмента анализа журналов сетевых служб. Программный инструмент выполняет анализ поведения пользователей сетевых ресурсов на соответствие существующим легитимным сценариям. Основополагающим требованием к разрабатываемому инструменту являлась совместимость с программным обеспечением, используемым в инфраструктуре корпоративной сети Красноярского научного центра, в частности, операционные системы Unix и веб-сервер Apache. Для построения приложения была предложена модель функционирования инструмента анализа журналов сетевых служб (рис. 2).

Модель содержит блоки предобработки данных, группировки по адресам и сверки параметров сетевых аномалий с параметрами выделенных групп, которые должен обнаруживать инструмент анализа. На вход модели поступают журналы веб-сервисов, а результатом работы программного инструмента являются IP-адреса провайдеров аномалий. Инструмент анализа адаптирован для обработки журналов веб-сервера Apache. Имена для доступа к файлам журналов на локальной машине указываются в веб-интерфейсе, таким образом можно анализировать журналы нескольких виртуальных хостов, размещённых на одном веб-сервере. Записи журналов сервера группируются по признаку «IP-адрес источника» и в дальнейшем проходят сверку с заданными администратором метриками, изменяемыми в интерфейсе. В случае если группа удовлетворяет описанной метрике, она помечается как группа риска и отображается в интерфейсе. Интерфейс программного обеспечения показан на рис. 3.

Разработанный инструмент успешно показал себя на реальных данных журналов корпоративной сети. Были успешно выявлены попытки probe, xss, r2l угроз [11], а также выделена группа риска с источниками угроз (рис. 4).

Полученные результаты подтвердили актуальность развития модели обеспечения кибербезопасности корпоративной сети Красноярского научного центра и необходимость проведения дальнейших исследований в данном направлении. Результатом развития модели безопасности стала автономная система обнаружения аномалий.

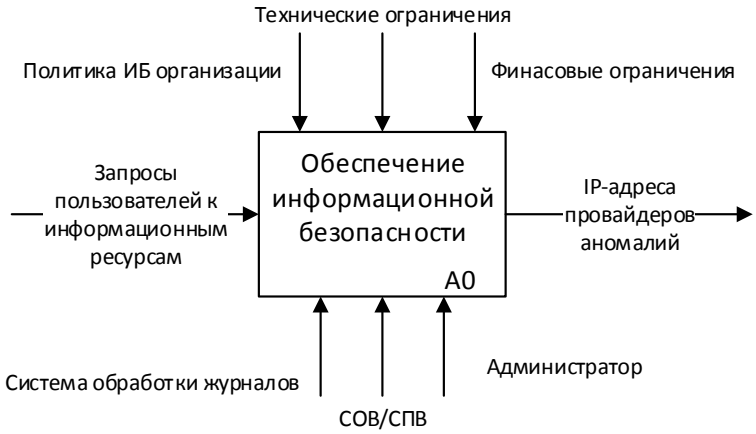

Рис. 1. Модель обеспечения информационной безопасности с системой обработки журналов

Fig. 1. The model of information security with a system of processing logs

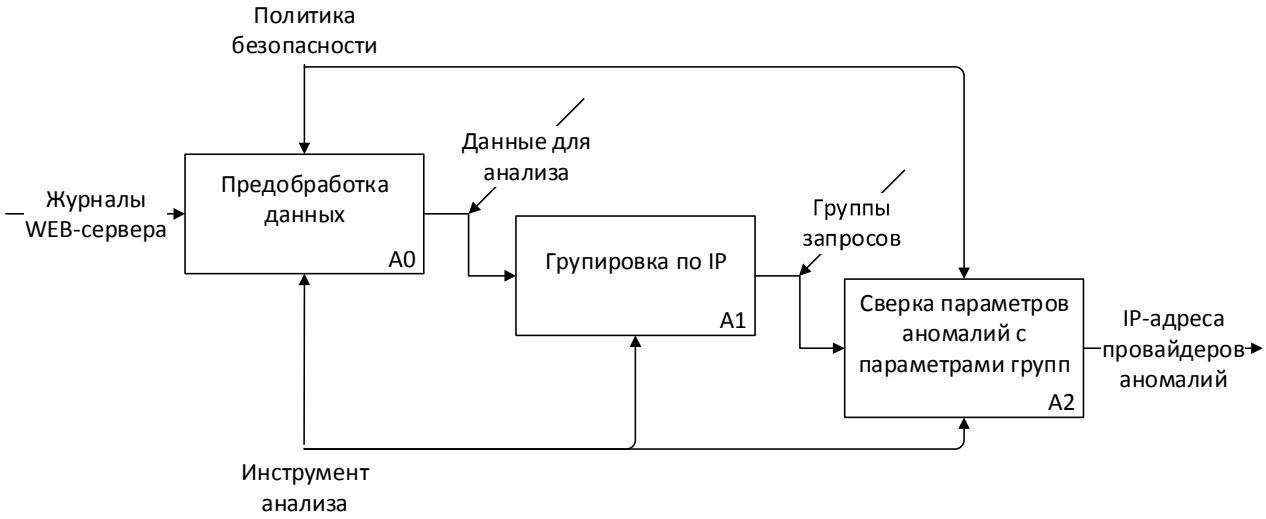

Рис. 2. Модель функционирования инструмента анализа журналов сетевых служб

Fig. 2. The model of the functioning of the tool for analyzing the logs of network services

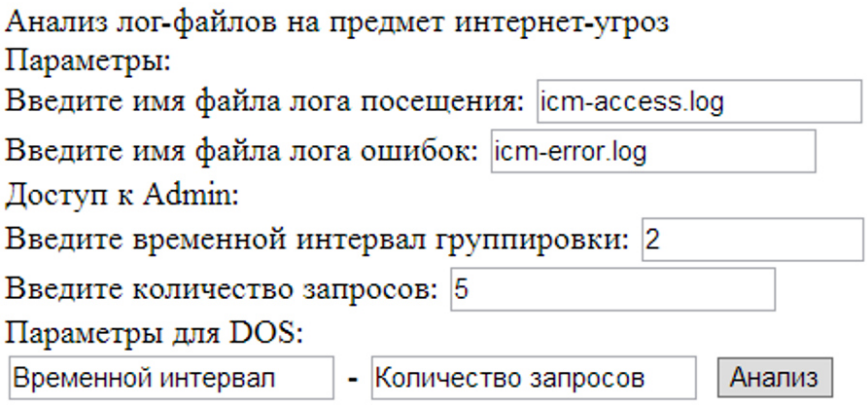

Рис. 3. Инструмент анализа журналов сетевых служб

Fig. 3. Network Services Log Analysis Tool

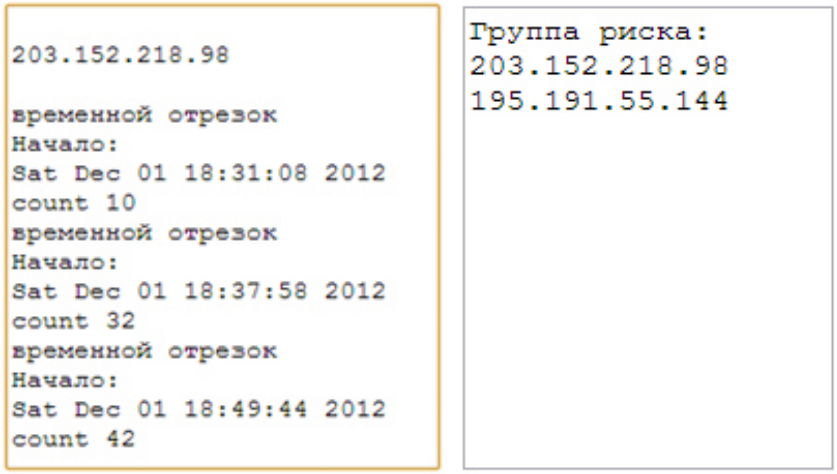

Рис. 4. Результаты анализа журналов сетевых служб

Fig. 4. Results of the analysis of network service logs

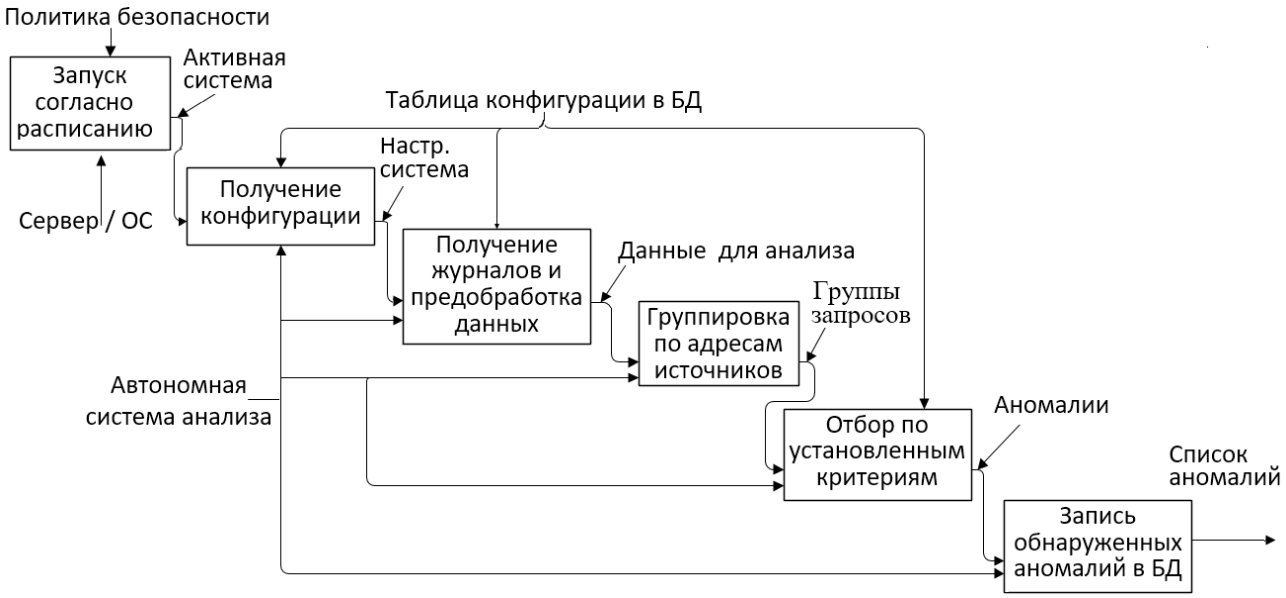

Рис. 5. Модель функционирования системы

Fig. 5. Model of the system functioning

Автономная система обнаружения аномалий. Ключевыми задачами создания автономной системы обнаружения аномалий являются:

1) автоматизация процессов анализа журналов сетевых служб;

2) агрегация данных с нескольких сетевых служб и сервисов;

3) создание интерактивного интерфейса для отображения данных и результатов анализа.

Решение поставленных задач позволяет построить систему, аналогичную по функционалу узловым системам обнаружения вторжений [12]. Для обнаружения и анализа угроз рассматриваются журналы сетевых служб – веб-сервера, ftp-сервера и файервола (межсетевого экрана).

Предложена модель функционирования автономной системы обнаружения аномалий, представленная на рис. 5.

Модель описывает функциональные блоки, ответственные за автоматизацию, получение конфигурации системы анализа из СУБД, получение, предобработку и анализ данных, запись обнаруженных аномалий в таблицу СУБД.

Поддерживается кроссплатформенная реализация программного обеспечения для его дальнейшего использования под управлением операционных систем семейства Windows и Unix. Хранение данных системы выполняется в кроссплатформенной СУБД MySQL.

Автоматизация. Для автоматизации используются утилиты управления задачами cron [13] (для Unix) или «Планировщик заданий» (для Windows). Эти планировщики интегрированы в большинстве дистрибутивов операционных систем. Они позволяют гибко задавать расписание запуска приложения, минимизировать участие пользователя в процессе выполнения

программы после ее установки и настройки и тем самым обеспечивают требуемую автоматизацию процессов обработки данных.

Получение конфигурации. В конфигурационной таблице базы данных содержатся следующие параметры работы системы: IP-адрес наблюдаемого узла, имя сервиса, учётные данные для получения журналов сервиса, расположение журналов в файловой системе, имена журналов веб-сервера, имена журналов ftp-сервера, имя журнала файрвола, тип используемого программного обеспечения, параметры аномалий, характерные для данного сервиса, список допустимых адресов, определенных администратором. Конфигурирование системы производится через дополнительную страницу веб-интерфейса (рис. 6).

Получение журналов и предобработка данных. После запуска приложение обращается к базе за списком источников с последующим получением журналов по протоколу ftp. При получении одного из журналов в фоновом режиме запускается программа его анализа и выполняется переход к следующему журналу в списке конфигурации. Таким образом, при получении *n* журналов выполняется *n* работающих экземпляров приложения, которые позволяют обеспечить параллельную обработку данных, тем самым ускорив процесс анализа и функционирования системы в целом.

Группировка данных по адресам и отбор по установленным критериям. Для группировки данных по заданным критериям выполняется их фильтрация при помощи утилиты grep [14]. Фильтрация выполняется по IP-адресам локальных служб организации, которые входят в список допустимых адресов, определенных администратором. Кроме того, могут задаваться периоды времени для выбора данных журналов. После фильтрации в локальной копии файла журнала остаются только записи требуемого периода, за который необходимо произвести анализ. На следующем этапе записи группируются по адресу источника и сверяются с установленными в конфигурации метриками аномалий. В случае, если группа запросов удовлетворяет или превышает установленные значения, то её источник отмечается как источник аномалии и производится соответствующая запись в таблицу аномалий. Таблица аномалий обеспечивает хранение информации об обнаруженных инцидентах и содержит следующие поля: IP-адрес источника аномалии, тип аномалии, название сервиса, на котором обнаружена аномалия, дата и время начала аномальной активности, количество превышений порога, количество запросов к сервису и продолжительность аномальной активности. Результаты анализа аномалий отображаются в интерфейсе программного обеспечения.

Описанные выше процессы позволяют достичь агрегации данных с нескольких сетевых служб и сервисов.

Разработка интерфейса программного обеспечения. При реализации интерфейса использованы следующие программные инструменты: языки HTML, CSS, JS, PHP и библиотеки для взаимодействия с данными – Jquery, D3.js, DC.js. Разработанное программное обеспечение имеет веб-интерфейс [15] и может встраиваться в существующие информационные сервисы корпоративной сети.

Для обеспечения безопасности системы и поддержки целостности собранных данных производится экспорт записей в файл формата csv. Интерфейс программного обеспечения взаимодействует с данными, представленными в файле csv.

С помощью инструментов библиотек d3, dc.js реализованы интерактивные диаграммы, отображающие количество обнаруженных аномалий за периоды времени, а также диаграммы распределения источников угроз. Примеры диаграмм показаны на рис. 7.

Address	Folder	Access log	HTTP server	FTP log	Type FTP	SYS log	Type SYS	DOS time	DOS quantity
172.16.*.*	datamask	photo-access.log	apa	-	-	-	-	60	10
172.16.*.*	datamask	professors-access.log	apa	-	-	-	-	60	200
172.16.*.*	datamask	tcmp-access.log	apa	-	-	-	-	60	500
172.16.*.*	datamask	icm-access.log	apa	-	-	system.log	ipfw	60	500
172.16.*.*	/var/log/***	mail-access.log	apa	dFTP.log	pure	-	-	60	350
172.16.*.*	datamask	modernproblems-access.log	apa	-	-	sys.log	ufw	60	600
172.16.*.*	/var/log/***	tcmp-access.log	apa	-	-	-	-	60	300
172.16.*.*	/log/	web.log	iss	ftp.log	w3c	security.log	win	60	200

Рис. 6. Пример интерфейса конфигурирования системы

Fig. 6. Example of the system configuration interface

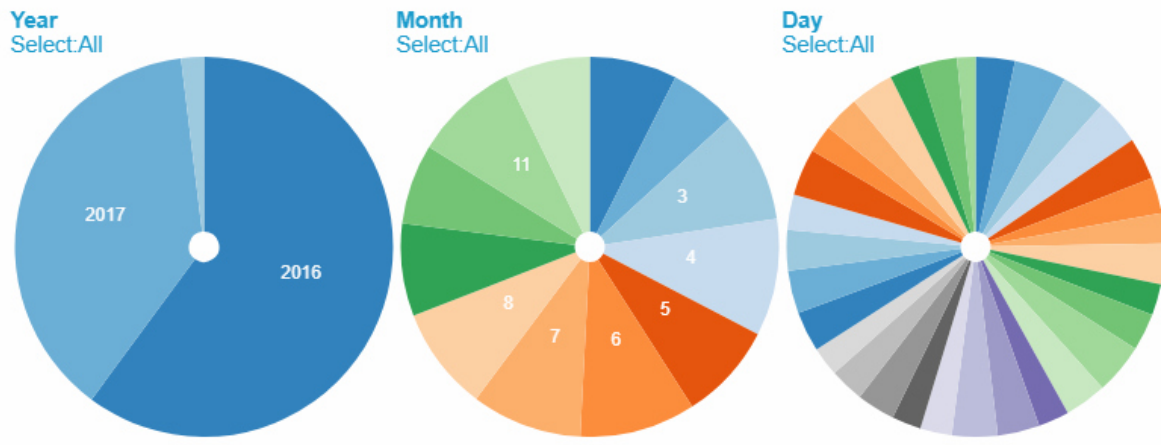

Рис. 7. Примеры диаграмм количества обнаруженных аномалий

Fig. 7. Examples of diagrams of the number of detected anomalies

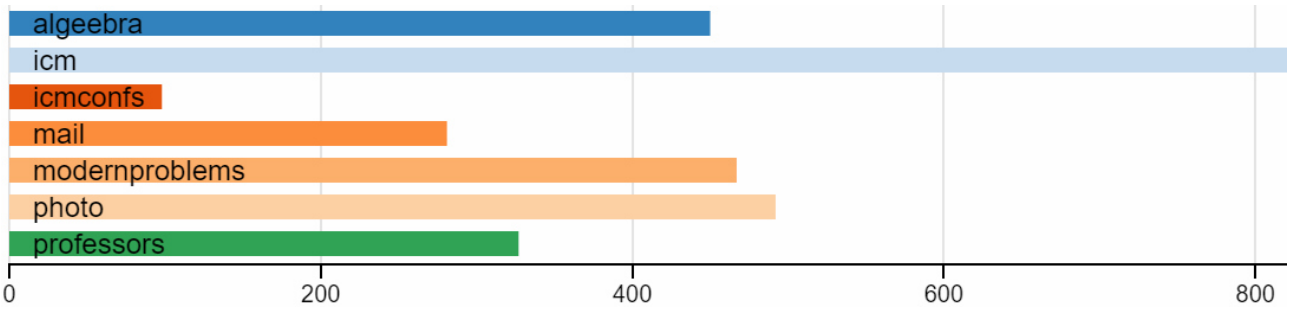

Рис. 8. Пример гистограммы аномалий на наблюдаемых сервисах

Fig. 8. An example of an anomaly histogram on the monitored services

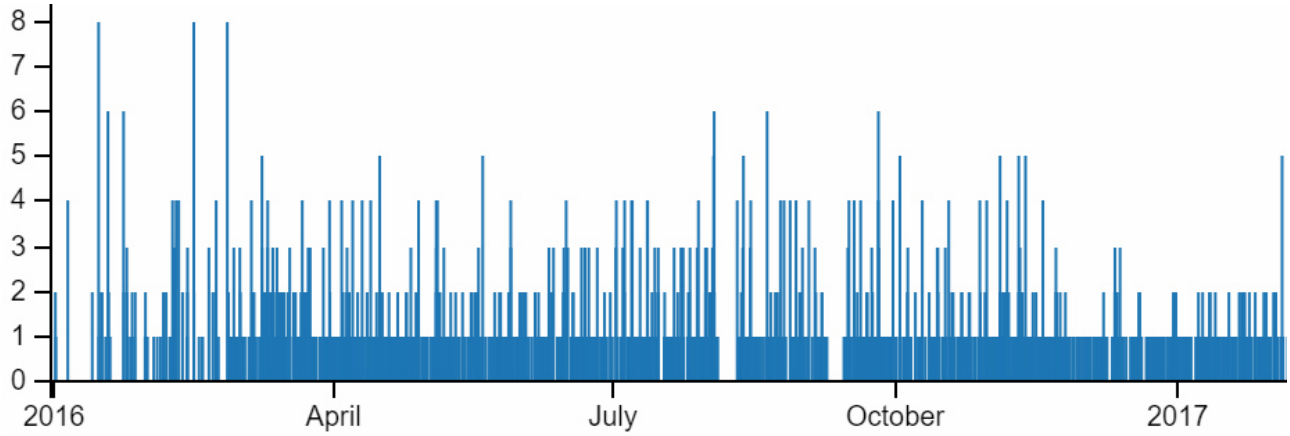

Рис. 9. Пример графика распределения аномалий на временном отрезке

Fig. 9. An example of the distribution of anomalies in a time interval

Построены гистограммы по количеству аномалий на наблюдаемых сервисах и по типу аномалий (рис. 8).

Программное обеспечение позволяет строить графики распределения активности аномалий по периодам времени. Пример графика за период с 2016 года по текущий момент показан на рис. 9.

Наибольшее число анализируемых данных содержится в журналах файервола, поэтому для анализа этих данных программное обеспечение предоставляет дополнительные возможности. Результаты анализа журналов файервола отображаются на отдельной странице интерфейса программного обеспечения, которая содержит развернутую статистику с возможностью сравнения нескольких показателей, а также инструмент дополнительных статистических исследований. Для обеспечения работы с большим объемом

данных реализована возможность выбора периода обработки, благодаря чему интерфейс сохраняет допустимую скорость отклика и поддерживает комфортность взаимодействия с пользователями.

Система визуализирует статистику анализа журналов за выбранный временной период. Пользователь может изменять параметры отображения, выбирая величину, относительно которой будут строиться графики: количество превышений порогового значения или суммарное количество обращений за период инцидента. Статистика по самым активным клиентам, подверженным угрозам, показывается в виде столбчатых диаграмм. Детализация информации выполняется при наведении курсора на столбец диаграммы (рис. 10).

Программное обеспечение позволяет рассматривать диаграммы статистики активности агентов угроз на портах сетевого интерфейса. Пример диаграммы, показывающей 20 наиболее нагруженных портов, показан на рис. 11. Программа позволяет выбирать данные по отдельным клиентам из 30 наиболее активных и обращаться к сервису Whois для получения детальной информации об источниках аномалий [16].

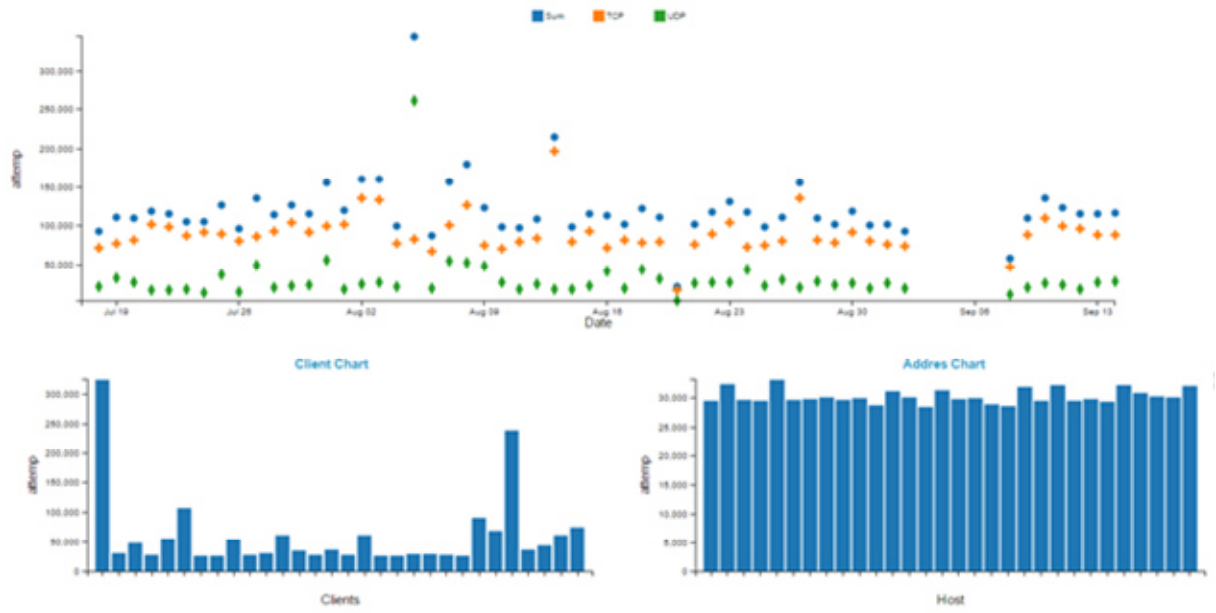

Рис. 10. Графики распределения аномалий по временному отрезку, хостам и клиентам

Fig. 10. Graphs of the distribution of anomalies by time interval, hosts and clients

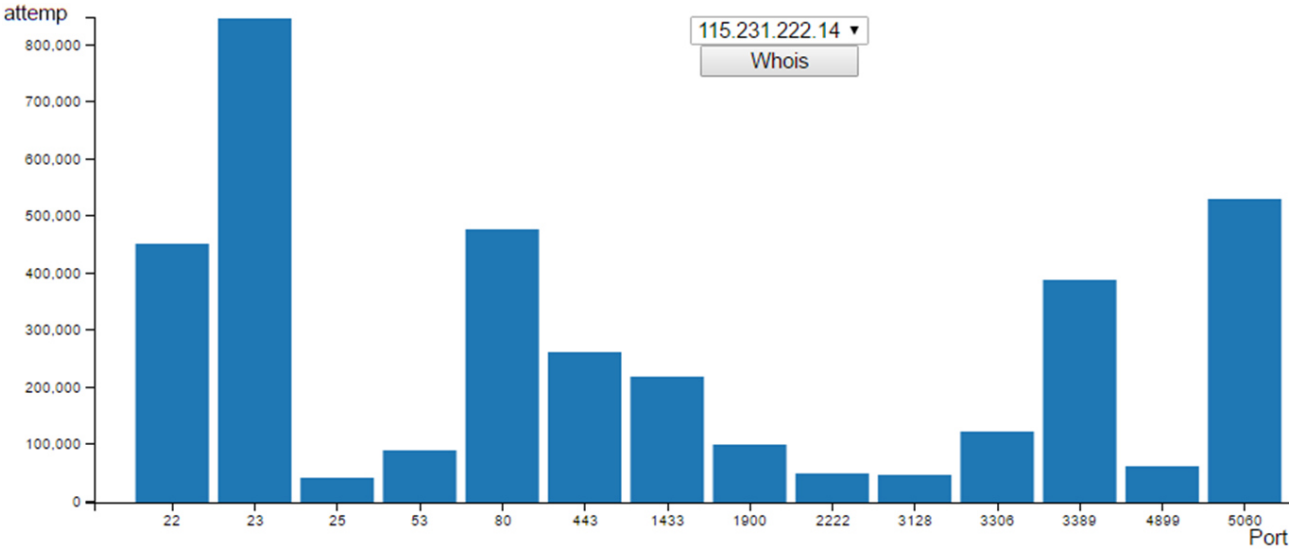

Рис. 11. График аномалий для портов сетевых интерфейсов

Fig. 11. Anomaly graph for network interface ports

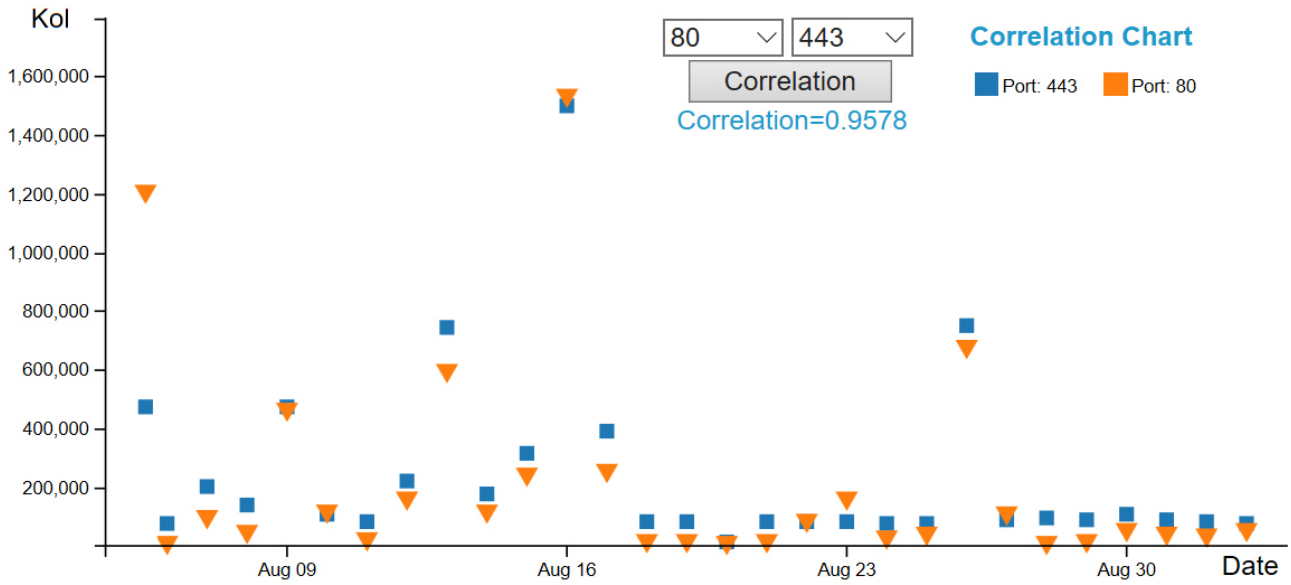

Рис. 12. График корреляции подверженных аномалиям сервисов

Fig. 12. Graph of correlation between services

Коэффициент линейной корреляции для отдельных сервисов

	HTTP	HTTPS	Telnet	HTTPa	SIP	RDP	SSH	mSQL	Radmin	MySQL
HTTP	1	0,957	-0,2	0,016	-0,104	0,202	-0,072	-0,114	-0,06	-0,017
HTTPS	0,957	1	-0,189	-0,036	-0,086	0,208	-0,03	-0,115	-0,06	0,054
Telnet	-0,2	-0,189	1	-0,17	0,179	-0,191	0,067	0,367	0,027	-0,163
HTTPa	0,016	-0,036	-0,17	1	0,134	-0,031	0,607	-0,351	0,295	0,468
SIP	-0,104	-0,086	0,179	0,134	1	0,464	0,27	0,386	0,4	0,174
RDP	0,202	0,208	-0,191	-0,031	0,464	1	0,279	-0,036	0,241	0,153
SSH	-0,072	-0,03	0,067	0,607	0,27	0,279	1	0,286	0,191	0,618
mSQL	-0,114	-0,115	0,367	-0,351	0,386	-0,036	0,286	1	0,014	-0,204
Radmin	-0,06	-0,06	0,027	0,295	0,4	0,241	0,191	0,014	1	-0,06
MySQL	-0,017	0,054	-0,163	0,468	0,174	0,153	0,618	-0,204	-0,06	1

Для выявления возможных взаимосвязей событий на различных портах сетевых интерфейсов выполняется расчёт коэффициентов корреляции и построение графиков для выбранных портов (рис. 12). Событием при этом считается количество зафиксированных попыток доступа к порту за период времени либо количество превышений установленного в конфигурации порога.

Для расширенного анализа рассмотрены сервисы, наиболее подверженные угрозам, и выполнен расчет зависимостей между ними (коэффициентов линейной корреляции Пирсона). Результаты приведены в таблице.

Исходя из результатов проведенного анализа, можно сделать выводы о существовании взаимосвязи событий между следующими интернет-сервисами:

– HTTP–HTTPS – обнаружение веб-серверов по открытому и защищенному соединению (0,957);

– SSH–HTTPa – согласованные попытки обнаружения сервисов удаленного входа и прокси-серверов (0,607);

– MySQL–SSH – согласованные попытки обнаружения сетевой базы данных и входа на удаленный сервер (0,618).

Таким образом, существует сильная связь между сетевыми службами, работающими по протоколам HTTP-HTTPS, и при обращении к одной из них велика вероятность попытки доступа ко второй. В свою очередь, доступ по этим протоколам не коррелирует с остальными протоколами, и можно сделать вывод о существенно различных источниках угроз. Среди остальных сервисов наиболее показательным по попыткам доступа является протокол SSH (Secure Shell), доступ к которому может служить индикатором попыток обнаружения слабозащищенных сервисов из второй группы (SSH, MYSQL, HTTPa, SMTP).

Полученная с помощью системы информация и выводы на основе ее дальнейшего анализа могут быть использованы для корректировки конфигурации активных систем информационной безопасности и для предотвращения в дальнейшем инцидентов, характеризующихся подобными событиями.

Заключение. В статье проведено исследование сетевых аномалий для журналов интернет-служб. Предложена модифицированная модель обеспечения информационной безопасности корпоративной сети. Реализация модели в виде веб-приложения позволила провести анализ угроз и выявить актуальность развития систем анализа аномалий и интеграции их в инфраструктуру организации.

Результатом работы стало полнофункциональное программное обеспечение – автономная система анализа журналов сетевых служб. Система расширила существующие средства обеспечения безопасности корпоративной сети дополнительными сервисами, предназначенными для выявления сетевых аномалий на граничных участках инфраструктуры.

Разработанная система содержит аналитические инструменты для обнаружения и изучения потенциально опасных сетевых аномалий. Она позволяет выполнять группировку и агрегацию данных, строить диаграммы статистики активности агентов угроз, вычислять зависимости между событиями возникновения аномалий и рассчитывать коэффициенты линейной корреляции для отдельных сервисов. Аналитические функции, реализованные в интерактивном интерфейсе программного обеспечения, позволяют получать детальное представление об исследуемой аномалии в режиме реального времени. Созданные программные компоненты повышают эффективность использования стандартных систем обнаружения и предотвращения вторжений за счет выявления и учета новых нестандартных факторов и зависимостей.

Выполнена апробация и внедрение автономной системы анализа журналов сетевых служб в инфраструктуру корпоративной сети Красноярского научного центра. Ее применение позволило произвести конфигурацию первой линии защиты от сетевых атак с учетом выявленных инцидентов и источников угроз, ранее не рассматриваемых в стандартных средствах защиты, что повысило оперативность реагирования на возникающие угрозы и уровень кибербезопасности организации в целом.

Библиографические ссылки

1. Исаев С. В. Кибербезопасность научного учреждения – активы и угрозы // Информатизация и связь. 2015. № 1. С. 53–57.

2. Papadaki M. IDS or IPS: what is best? // Network Security. 2004. Vol. 7. P. 15–19.

3. Котов В. Д., Васильев В. И. Современное состояние проблемы обнаружения сетевых вторжений // Вестник УГАТУ. 2012. № 3(48). С. 198–204.

4. Микова С. Ю., Оладько В. С., Нестеренко М. А. Подход к классификации аномалий сетевого трафика // Инновационная наука. 2015. № 11-2. С. 78–80.

5. Muniyandi A. P. Network Anomaly Detection by Cascading K-Means Clustering and C4.5 decision Tree algorithm // Procedia Engineering. 2012. Vol. 30. P. 174–182.

6. Браницкий А. А., Котенко И. В. Обнаружение сетевых атак на основе комплексирования нейронных, иммунных и нейронечетких классификаторов // Информационно-управляющие системы. 2015. № 4 (77). С. 69–77.

7. Басараб М. А., Строганов И. С. Обнаружение аномалий в информационных процессах на основе мультифрактального анализа // Вопросы кибербезопасности. 2014. № 4 (7). С. 30–40.

8. Нестеренко В. А. Построение и использование функции плотности в пространстве характеристик для выявления аномальных событий // Известия ЮФУ. Технические науки. 2008. № 8. С. 130–134.

9. Кононов Д. Д. Критерии оценки аспектов безопасности при разработке веб-приложений // Решетневские чтения : материалы XXI Междунар. науч. конф. (8–10 нояб. 2017, г. Красноярск) : в 2 ч. / под общ. ред. Ю. Ю. Логинова ; Сиб. гос. аэрокосмич. ун-т. Красноярск, 2017. С. 413–414.

10. Подкорытов Д. А. Модель политики безопасности вычислительных систем // Информационно-управляющие системы. 2004. № 1. С. 41–49.

11. Бабенко Г. В. Анализ современных угроз безопасности информации, возникающих при сетевом взаимодействии // Вестник АГТУ. Сер. «Управление, вычислительная техника и информатика». 2010. № 2. С. 149–152.

12. Котов В. Д., Васильев В. И. Современное состояние проблемы обнаружения сетевых вторжений // Вестник УГАТУ. 2012. № 3(48). С. 198–204.

13. Трубачёва И. С. Почему Linux и системы реального времени? // Вестник ВУиТ. 2015. № 2(24). С. 99–106.

14. Шепелев А. Н., Букатов А. А., Пыхалов А. В. Анализ подходов и средств обработки сервисных журналов // ИВД. 2013. № 4(27). С. 15–29.

15. Иванов А. Н., Кознов Д. В., Тыжгеев М. Г. Моделирование интерфейса полнофункциональных web-приложений, интенсивно работающих с данными // Вестник СПбГУ. Сер. 10. Прикладная математика. Информатика. Процессы управления. 2009. № 3. С. 189–204.

16. Chaudri A. Internet domain names and interaction with intellectual property // Computer Law & Security Review. 2007. Vol. 23(1). P. 62–66.

References

1. Isaev S. V. [Cybersecurity of a scientific institution – assets and threats]. *Informatizatsiya i svyaz*. 2015, No. 1, P. 53–57 (In Russ.).

2. Papadaki M. IDS or IPS: what is best? *Network Security*. 2004, No. 7, P. 15–19.

3. Kotov V. D., Vasilev V. I. [The current state of the problem of detecting network intrusions]. *Vestnik UGATU*. 2012, No. 3(48), P. 198–204 (In Russ.).

4. Mikova S. Y., Oladko V. S., Nesterenko M. A. [Approach to the classification of network traffic anomalies]. *Innovatsionnaya nauka*. 2015, No. 11-2, P. 78–80 (In Russ.).

5. Muniyandi A. P. Network Anomaly Detection by Cascading K-Means Clustering and C4.5 Decision Tree algorithm. *Procedia Engineering*. 2012, No. 30, P. 174–182.

6. Branickij A. A., Kotenko I. V. [Detection of network attacks based on the integration of neural, immune and neuron-fuzzy classifiers]. *Informatsionno-upravlyayushchie sistemy*. 2015, No. 4 (77), P. 69–77 (In Russ.).

7. Basarab M. A. Stroganov I. S. [Detection of anomalies in information processes based on multifractal analysis]. *Voprosy kiberbezopasnosti.* 2014, No. 4 (7), P. 30–40 (In Russ.).

8. Nesterenko V. A. [Construction and use of the density function in the characteristic space to detect abnormal events]. *Izvestiya YuFU. Tekhnicheskie nauki.* 2008, No. 8, P. 130–134 (In Russ.).

9. Kononov D. D. [Criteria for assessing security aspects in the development of Web applications]. *Materialy XXI Mezhdunar. nauch. konf. "Reshetnevskie chteniya"* [Materials XXI Intern. Scientific. Conf "Reshetnev readings"]. Krasnoyarsk, 2017, P. 413–414 (In Russ.).

10. Podkorytov D. A. [The Computer Systems Security Policy Model]. *Informatsionno-upravlyayushchie sistemy.* 2004, No. 1, P. 41–49 (In Russ.).

11. Babenko G. V. [Analysis of current threats to information security arising from network interaction]. *Vestnik AGTU. Seriya: Upravlenie, vyichislitelnaya tekhnika i informatika*. 2010, No. 2, P. 149–152 (In Russ.).

12. Kotov V. D., Vasilev V. I. [The current state of the problem of detecting network intrusions]. *Vestnik UGATU*. 2012, No. 3(48), P. 198–204 (In Russ.).

13. Trubachova I. S. [Why Linux and real-time systems?]. *Vestnik VUiT*. 2015, No. 2(24), P. 99–106 (In Russ.).

14. Shepelev A. N., Bukatov A. A., Pyihalov A. V. [Analysis of approaches and tools for processing service logs]. *IVD*. 2013, No. 4(27), P. 15–29 (In Russ.).

15. Ivanov A. N., Koznov D. V., Tyijgeev M. G. [Modeling the interface of full-featured Web-based applications that work intensively with data]. *Vestnik SPbGU. Seriya 10. Prikladnaya matematika. Informatika. Protsessyi upravleniya*. 2009, No. 3, P. 189–204 (In Russ.).

16. Chaudri A. Internet domain names and interaction with intellectual property. *Computer Law & Security Review.* 2007, No. 23(1), P. 62–66.