УДК 681.518

Д.В. Козьмовский, В.И. Куватов, Ю.И. Синещук, Т.И. Давыдова

МЕТОД ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ НА ОСНОВЕ КОНТРОЛЯ ДЕЯТЕЛЬНОСТИ ПОЛЬЗОВАТЕЛЕЙ РАСПРЕДЕЛЕННОЙ ВЫЧИСЛИТЕЛЬНОЙ СРЕДЫ

Козьмовский Дмитрий Васильевич, *кандидат технических наук, окончил факультет математического обеспечения автоматизированных систем управления Военно-морского института радиоэлектроники им. А.С. Попова. Ведущий специалист АО «НПО «Импульс». Специализируется в области разработки, опытного производства и сопровождения специальных территориально распределенных информационно-управляющих систем. [e-mail: klimsky@rambler.ru].*

Куватов Валерий Ильич, *доктор технических наук, профессор, заслуженный работник высшей школы РФ, окончил факультет математического обеспечения АСУ Высшего военно-морского училища радиоэлектроники им. А.С. Попова. Профессор Санкт-Петербургского университета МВД России. Специализируется в области математического моделирования и информационных технологий АСУ специального назначения. Имеет статьи и монографии по заявленной проблематике. [e-mail: kyb.valery@yandex.ru].*

Синещук Юрий Иванович, *доктор технических наук, профессор, заслуженный работник высшей школы РФ, окончил факультет боевых информационных управляющих систем ВМУРЭ им. А.С. Попова. Профессор Санкт-Петербургского университета МВД России. Специализируется в области анализа и обеспечения информационной безопасности, устойчивости функционирования сложных систем. [e-mail: sinegal@rambler.ru].*

Давыдова Татьяна Ивановна, *кандидат технических наук, окончила радиотехнический факультет Ульяновского государственного технического университета. Ведущий инженер ФНПЦ АО «НПО «Марс». Имеет статьи и монографию в области расчетов надежности и эксплуатации радиотехнических средств. [e-mail: tasha_dav@inbox.ru].*

Аннотация

В статье анализируются особенности обеспечения безопасности информационных ресурсов распределенных телекоммуникационных систем. Территориально распределенная вычислительная сеть представляет собой совокупность сетевого оборудования и линий связи, предназначенных для обмена данными между рабочими местами пользователей и функциональными подсистемами. Учитывая, что более 90% информации организации ныне находится в электронном виде, проблема обеспечения защиты информации, циркулирующей в вычислительной сети, становится исключительно важной задачей. В этой связи, организация сетевой структуры сопряжена с необходимыми настройками политик безопасности пользователей сети. При этом вне поля зрения остаются наиболее реальные и многочисленные внутренние угрозы, которые есть у большинства организаций. Описаны системы, предназначенные для защиты вычислительной сети от внутреннего нарушителя и использующие контроль сетевых соединений, учет и анализ сетевого трафика. Сформулирован принцип определения фактических видов деятельности пользователей, который основывается на анализе статистических параметров сеансов по различным видам сетевой деятельности, сравнивании их с профилями пользователей и позволяет классифицировать сеансы сетевого обмена. Обоснованы этапы и алгоритм классификации сетевой деятельности и отдельных сеансов сетевого обмена по видам сетевой деятельности.

Ключевые слова: распределенная вычислительная среда, угрозы информационной безопасности, сеанс сетевого обмена, классификация деятельности пользователей.

doi: 10.35752/1991-2927-2019-3-57-29-37

INFORMATION SECURITY METHOD BASED ON USER ACTIVITY MONITORING OF DISTRIBUTED COMPUTING ENVIRONMENT

Dmitrii Vasilevich Kozmovskii, *Candidate of Science in Engineering; graduated from the Faculty of Automated Control Systems Mathematical Support at the A.S. Popov Naval Radioelectronics Institute; Lead Specialist at JSC 'RPA 'Impuls'; specializes in the field of development, pilot production and maintenance of special geographically distributed information management systems. e-mail: klimsky@rambler.ru.*

Valerii Ilich Kuvatov, *Doctor of Science in Engineering, Professor; Honored Worker of the Higher School of the Russian Federation; graduated from the Faculty of Automated Control Systems Mathematical Support at the A.S. Popov Naval Radioelectronics Institute; Professor of the St. Petersburg University of the Russian Interior Ministry; specializes in the field of mathematical modeling and information technologies of special-purpose computer-aided control systems; an author of articles and monographs on the subject. e-mail: kyb.valery@yandex.ru.*

Iurii Ivanovich Sineshchuk, *Doctor of Science in Engineering, Professor; Honored Worker of the Higher School of the Russian Federation; graduated from the Faculty of Combat Information and Management Systems of the A.S. Popov Higher Naval Radioelectronics School; Professor of the St. Petersburg University of the Russian Interior Ministry; specializes in the field of analysis and information security, stability of complex systems. e-mail: sinegal@rambler.ru.*

Tatiana Ivanovna Davydova, *Candidate of Science in Engineering; graduated from the Radioengineering Faculty of Ulyanovsk State Technical University; Leading Engineer at FRPC JSC 'RPA 'Mars'; an author of articles and monograph in the field of reliability calculations and operating of radio engineering facilities. e-mail: tasha_dav@inbox.ru.*

Abstract

The article analyzes the security features of information resources of distributed telecommunication systems. Geographically distributed computing network is a set of network equipment and communication lines designed for data exchange between user workstations and functional subsystems. Given that more than 90% of the organization's information is now in electronic form, the problem of ensuring the protection of information circulating in the computer network is becoming an extremely important task. In this regard, the organization of the network structure is associated with the necessary settings of security policies of network users. At the same time, the most real and numerous internal threats that most organizations have remain out of sight. The article describes the systems designed to protect the computer network from an internal intruder, using the control of network connections, accounting and analysis of network traffic. The principle of definition of actual types of activity of users which is based on the analysis of statistical parameters of sessions on various types of network activity, their comparison with profiles of users allowing to classify sessions of network exchange is formulated. Grounded steps and the classification algorithm network activities and separate instances of network sharing in the network activities.

Key word: distributed computing environment, information security threats, network exchange session, user activity classification.

Введение

В настоящее время существует глубокая интеграция сетевых технологий в повседневную деятельность органов управления различных иерархических уровней. Это может быть локальная сеть местного назначения, объединяющая несколько компьютеров небольшого узла связи, или состоящая из нескольких сегментов сеть вычислительного центра, к тому же с возможностью доступа в глобальную сеть Интернет. При этом система управления, как материальная основа единого информационного пространства (ЕИП) организации, по сути, представляет собой распределенную вычислительную среду (РВС) для обеспечения руководства, сотрудников и других потребителей эффективными средствами информационно-аналитической поддержки основных видов деятельности организации, например таких, как: образовательный процесс, научные исследования и управление повседневной деятельностью, реализация функционального предназначения.

РВС в рассматриваемом аспекте можно представить как сложную организационно-техническую систему, представляющую собой совокупность функциональных подсистем, имеющих между собой связи в виде отношений и потоков информации, территориально распределенной вычислительной сети и рабочих мест пользователей.

Функциональные подсистемы представляют собой совокупность взаимосвязанных программно-аппаратных средств и информационных ресурсов, обеспечивающих реализацию в рамках видов деятельности пользователей (должностных лиц органов управления) нескольких взаимосвязанных функций управления и обеспечения.

Территориально распределенная вычислительная сеть представляет собой совокупность сетевого оборудования и линий связи, предназначенных для обмена данными между рабочими местами пользователей и функциональными подсистемами РВС.

Рабочие места пользователей представляют собой подключенные к локальной вычислительной сети (ЛВС) персональные ЭВМ и периферийные устройства, за которыми пользователи выполняют свои обязанности, взаимодействуя с функциональными подсистемами.

В процессе удовлетворения информационных потребностей пользователя (лиц, принимающих решение (ЛПР)), происходит взаимодействие информационных ресурсов, как элементов ЕИП, необходимых для реализации конкретных функций управления и соответствующих информационных технологий для их накопления, обработки, представления и потребления [1].

Источники и потребители информационных ресурсов:

- органы управления МЧС, МВД, МО, ВМФ;
- органы государственного управления;
- министерства и ведомства РФ;
- организации и предприятия промышленности;
- структурные подразделения.

Виды информационных ресурсов:

- боевые документы (боевые приказы, распоряжения, директивы);
- нормативные документы (приказы, нормы, штаты);
- справочная информация (планы, программы, словари);
- учетная информация (анкеты, картотеки);
- научно-техническая информация (печатные издания, отчеты о научно-исследовательских и опытно-конструкторских работах);
- информация, циркулирующая в автоматизированных системах (базы данных, файлы, сообщения);
- другие массивы информации (карты, фонды, архивы, плакаты, отдельные файлы).

Для реализации функциональных задач и организации информационного обеспечения РВС используются следующие базовые информационные технологии:

- системы управления базами данных с возможностью реализации прикладной логики на стороне сервера (SQL-серверы);
- интранет-технология (Web-серверы);
- системы электронной почты и электронного документооборота;
- информационные хранилища.

Учитывая, что более 90% информации организации в настоящее время находится в электронном виде, проблема обеспечения защиты информации, циркулирующей в вычислительной сети, становится исключительно важной задачей. В этой связи организация сетевой структуры сопряжена с необходимыми настройками политик безопасности пользователей сети.

Часть этих задач успешно решается аппаратно-программными средствами защиты информации. Данные задачи предназначены для следующих целей:

- блокировка клавиатуры;
- блокировка загрузки с внешних носителей;
- аутентификация и идентификация пользователей на начальном этапе загрузки ПЭВМ;
- защита информации, хранящейся на жестком диске защищаемой ПЭВМ и на удаленных сетевых ресурсах, от несанкционированного доступа со стороны злоумышленников.

Это достигается путем раздельного и гибко настраиваемого разграничения доступа к файлам, каталогам, принтерам, устройствам ввода/вывода ПЭВМ и системным компонентам операционной системы от случайной или умышленной модификации, удаления, поражения вирусами [2, 3].

При этом вне поля зрения остаются наиболее реальные и многочисленные внутренние угрозы, которые есть у большинства организаций: утечка информации; злоупотребление служебным положением; публикация резюме или просмотр вакансий; общение в социальных сетях или других программах мгновенного обмена сообщениями; поиск информации в Интернете; переписка с корпоративной почты или с веб-почты (mail.ru, gmail.com и т. д.); общение на сайтах знакомств или публикация информации в блогах и многое другое.

1 Постановка задачи

Внутренний нарушитель представляет собой легитимного пользователя вычислительной сети, который обладает определенными правами на доступ к информационным ресурсам. Вследствие умышленных или ошибочных действий внутренний нарушитель может принести ущерб, зачастую больший, чем внешний злоумышленник.

Таким образом, даже при качественной организации и правильной настройке сети существует необходимость контроля деятельности пользователей. Вид деятельности – единица деятельности пользователя, связанная с исполнением функциональных задач должностного лица. Например: поиск информации на Web-серверах, загрузка данных, обмен электронной корреспонденцией и т. д. Набор видов деятельности пользователя называется профилем пользователя и определяется его должностными обязанностями.

Системы, предназначенные для защиты вычислительной сети от внутреннего нарушителя, используют

контроль сетевых соединений, учет и анализ сетевого трафика и представлены следующими классами [4–7]:

- системы DLP-класса – контентная фильтрация трафика;
- системы IRM-класса – гибрид системы контроля доступа и криптосистем;
- системы IDS-класса – сигнатурный анализ трафика.

Существующие системы анализа трафика позволяют проводить мониторинг трафика и сетевых соединений. В состав систем входят инструменты расшифровки пакетов сетевого обмена. А также имеется возможность настройки фильтров по большому количеству критериев. Ведется учет трафика по узлам, вывод статистики входящего/исходящего трафика. Большинство систем предлагают классификацию трафика, основанную на нескольких методах:

- анализ открытых портов соединений. Основывается на том, что приложения работают по умолчанию на известных портах;
- анализ полезной нагрузки пакетов сетевого трафика. Заключается в обнаружении определенных сигнатур, специфичных для сетевых приложений, в полезной нагрузке пакетов.

К недостаткам первого метода можно отнести то, что большинство приложений позволяют изменять номера портов по умолчанию на любые. Многие современные приложения предпочитают использовать случайные номера портов. Также существует тенденция использования номеров портов известных приложений.

Недостатками второго метода являются:

- необходимость ведения и обновления сигнатур, используемых сетевыми приложениями для более точного анализа трафика;
- при шифровании трафика анализ сильно затруднен;
- требуется анализ всего сетевого трафика, что может создать большие нагрузки на оборудование и вызвать ошибки в работе сети.

Проведенный анализ показывает, что с целью выявления недопустимого использования информационных ресурсов системы существует необходимость разработки метода анализа трафика, который не использует привязку сетевых приложений к портам и не проводит анализ содержимого пакетов сетевого обмена, при этом показывая высокий уровень эффективности правильной классификации трафика. По существу, в основе лежит принцип определения фактических видов деятельности пользователей РВС, который основывается на анализе сетевого трафика и сравнивании его с профилями пользователей. Другими словами, под анализом трафика будем понимать классификацию сеансов сетевого обмена.

2 Обоснование метода и алгоритм решения задачи

Решение сформулированной задачи предполагает, что весь трафик будет поделен на сеансы, каждый из которых классифицируется отдельно, то есть вычисляется вероятность принадлежности сеанса тому или иному протоколу. Под сеансом будем понимать сетевой обмен пакетами между двумя узлами в течение непрерывного времени, а трафик определим как совокупность сеансов $N = \{n_i\}$.

Для классификации сеансов по видам деятельности, которая позволит автоматизировать процесс анализа сетевого трафика, требуются статистические характеристики сеанса n_i, которые могут быть получены из заголовков пакетов сетевого обмена. При этом в набор параметров могут быть включены только те из них, относительно которых может быть получена информация, достаточная для их описания, но нецелесообразно использовать параметры, которые, хотя и имеют достаточный объем данных, неинформативны при решении поставленной задачи классификации.

К числу указанных характеристик, которые можно рассматривать как независимые и при этом успешно применять для классификации трафика, относятся:

- число внешних портов,
- число внутренних портов,
- доля исходящего трафика,
- средний размер пакета.

Эти характеристики являются непрерывными числовыми величинами.

Идея классификации основывается на применении метода Байеса [8, 9] и предполагает следующее:

- каждый сеанс можно рассматривать как объект, характеризуемый набором статистических параметров,
- для каждого сеанса собираются и анализируются значения всех параметров,
- статистическое распределение значений параметров сеансов различается в зависимости от вида деятельности.

Сложность использования метода Байеса заключается в том, что данный метод может работать либо с дискретными значениями, либо используя плотности распределения непрерывных величин. В случае применения первого варианта необходимо описать переход от фактических значений статистических параметров сеанса к вектору значений дискретных параметров классификации $X = (x_1, x_2, \ldots, x_m)$.

Классификация сетевой деятельности происходит в несколько этапов:

- захват трафика,
- формирование сеансов,
- классификация сеансов.

Классификация сеансов по видам сетевой деятельности происходит по следующему алгоритму, представленному на рисунке 1.

Классификация сеанса предполагает:

- вычисление статистических характеристик сеанса. Для каждого сеанса производится вычисление статистических параметров. Результат вычисления заносится в базу данных;
- классификация сеансов с применением обучающей выборки. Используя статистические данные обучающей выборки, происходит распределение сеансов по

Рис. 1. Блок-схема алгоритма классификации сетевого трафика

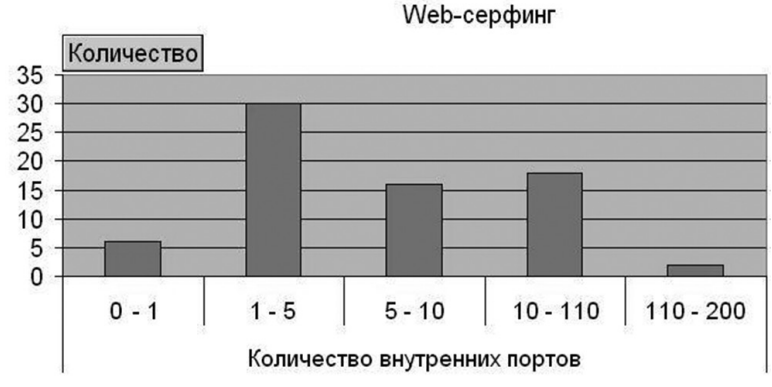

Рис. 2. Распределение значений статистического параметра «Число внутренних портов» для вида деятельности Web-серфинг

видам сетевой деятельности (типам прикладных протоколов). В качестве математического аппарата используется наивный Байесовский классификатор (НБК);

- вывод результатов классификации сеансов.

Результатом классификации являются агрегированные данные классификации сеансов для каждого узла РВС, сетевая деятельность которого подвержена анализу. Под агрегированными характеристиками понимаются данные о суммарном объеме переданной/принятой узлом информации за указанный период и распределение этих объемов по видам деятельности.

Рассмотрим ситуацию, когда мы уже имеем некоторую накопленную статистику значений статистических параметров сеансов по различным видам сетевой деятельности [10, 11]. Значения статистических параметров можно представить в виде распределения каждого из параметров сеанса на отрезке возможных значений. В качестве примера приведем распределение параметра «Количество внутренних портов» для вида деятельности Web-серфинг (рис. 2).

На приведенной диаграмме конкретные значения статистического параметра отображаются на интервалы значений. Интервалы статистических параметров сеансов формируются вручную в течение наполнения обучающей выборки, которое заключается в сборе статистической информации, то есть значений статистических параметров, по всем видам деятельности, для которых поставлена задача классификации. Количество интервалов и их размерность определяется распределением статистических данных на всем промежутке возможных значений. Процесс формирования интервалов происходит от общего к частному таким образом, чтобы по возможности получить распределения значений параметров разных видов деятельности по интервалам, при этом не допуская излишней дискретности, которая может усложнить задачу классификации.

В результате вместо фактических значений параметров в качестве параметров классификации используются интервалы промежутков возможных значений статистических параметров. Для функционирования данного метода необходимо наличие обучающей выборки по протоколам, которые будут подвергаться классификации. При наличии большой выборки по каждому протоколу, вероятность точной классификации достаточно высока.

Переход от фактических значений статистических параметров сеанса к значениям интервалов объясняется необходимостью дискретности данных, используемых в НБК, для вероятностной оценки соответствия сетевых сеансов тем или иным видам сетевой деятельности. Указанный метод классификации широко используется в системах для определения нежелательных почтовых сообщений (анти-спам системах). После некоторой модификации возможно использования НБК для классификации практически любых видов сетевых сеансов, при условии,

что в распоряжении эксперта имеется достаточная по объему обучающая выборка с образцами подобных сеансов. В основе метода лежит формула условной вероятности:

$$P(H_i \mid X) = \frac{P(X \mid H_i)P(H_i)}{\sum_{k=1}^{n} P(X \mid H_k)P(H_k)}, \quad (1)$$

где $P(H_i \mid X)$ – вероятность истинности гипотезы H_i при заданной причине X;

$P(H_i)$ – априорная вероятность гипотезы H_i;

$P(X \mid H_i)$ – вероятность присутствия причины X, если истинна гипотеза H_i;

n – число возможных гипотез.

Если причину можно представить в виде вектора: $X = (x_1, x_2, \ldots, x_m)$, каждый компонент которого имеет условную вероятность относительно гипотезы H_i $P(x_j \mid H_i)$, то для вычисления условных вероятностей $P(X \mid H_i)$ используется «наивное» предположение об условной независимости компонентов вектора X. В этом случае условная вероятность вычисляется по формуле:

$$P(X \mid H_i) = \prod_{j=1}^{m} P(x_j \mid H_i). \quad (2)$$

В случае классификации сетевых сеансов в качестве гипотез H_i выступают предположения о том, что классифицируемый сеанс соответствует i-му виду сетевой деятельности. То есть вероятность соответствия сеанса с набором параметров классификации X виду деятельности H_i равна произведению вероятностей соответствия каждого вычисленного параметра классификации виду деятельности H_i.

Применение выбранного метода классификации на основе НБК предполагает использование статистической информации. Объем статистической информации, который содержит в себе сеансы точно определенных видов деятельности, называется обучающей выборкой. А сеансы, которые содержит обучающая выборка, называются эталонными. Для каждого эталонного сеанса произведен расчет статистических значений параметров и произведено распределение данных значений по интервалам. Для каждого нового сеанса, который подвергается классификации, вычисляются значения параметров классификации и определяются диапазоны, в которые попали рассчитанные значения. Данные номера диапазонов являются параметрами классификации. Расчет соответствия параметра классификации x_j виду деятельности H_i производится по формуле:

$$P(x_j \mid H_i) = m/M, \quad (3)$$

где M – общее количество значений данного параметра x_j в обучающей выборке, накопленное эталонными сеансами вида деятельности H_i;

m – количество значений данного параметра x_j, накопленное эталонными сеансами вида деятельности H_i, в диапазоне, в который попадает вычисленное значение параметра классифицируемого сеанса.

3 Анализ результатов

Оценка достоверности классификации проводилась методом кросс-проверки [9, 10]. Исходными данными для проведения кросс-проверки являются:

- обучающая выборка, содержащая по 400 эталонных сеансов, относящихся к 4 различным видам деятельности (сумма эталонных сеансов в обучающей выборке равняется 1600);
- тестовая выборка, определенная равной примерно десяти процентам от общего объема обучающей выборки, сформированная для каждого вида деятельности.

Распределение в тестовой выборке видов деятельности и количество сетевых сеансов, приведены в таблице 1.

Таблица 1

Количество сеансов тестовой выборки

Виды сетевой деятельности для классификации	Количество сеансов тестовой выборки
Поиск информации на Web-серверах	84
Загрузка данных	42
Отправка электронной корреспонденции	36
Получение электронной корреспонденции	44
Итого	206

Количество сеансов тестовой выборки для вида сетевой деятельности «Web-серфинг» увеличено в связи с наибольшей распространенностью данного вида деятельности и повышенной сложностью его классификации.

Для каждого вида деятельности проводилась классификация и проверялась ее правильность. Отсутствие достоверного результата классификации определяется в том случае, если сеанс не был отнесен к одному из видов деятельности, то есть вероятность соответствия меньше 0,6, или если сеанс был отнесен к другому виду деятельности. Отношение числа сеансов с правиль-

Таблица 2

Результаты проведения кросс-проверки

Виды деятельности / Результаты классификации	Количество сеансов тестовой выборки	Поиск информации на Web-серверах	Загрузка данных	Отправка электронной корреспонденции	Получение электронной корреспонденции	Отсутствует достоверный результат классификации
Поиск информации на Web-серверах	84	63	0	3	2	16
Загрузка данных	42	0	41	0	0	1
Отправка электронной корреспонденции	36	0	0	30	0	6
Получение электронной корреспонденции	44	0	0	0	40	4

Таблица 3

Доля неправильно классифицированных сеансов и сеансов с недостаточной достоверностью классификации

Виды сетевой деятельности для классификации	Доля неправильно классифицируемых сеансов и сеансов с недостаточной достоверностью классификации
Поиск информации на Web-серверах	0,25
Загрузка данных	0,02381
Отправка электронной корреспонденции	0,166
Получение электронной корреспонденции	0,1

ной классификацией к общему числу сеансов данного вида деятельности рассматривалось как статистическая оценка правильности классификации.

Результаты проведения кросс-проверки отображены в таблице 2.

Число правильно классифицируемых сеансов составляет:

- 63 сеанса для вида деятельности «Поиск информации на Web-серверах»;
- 41 сеанс для вида деятельности «Загрузка данных»;
- 30 сеансов для вида деятельности «Отправка электронной корреспонденции»;
- 44 сеанса для вида деятельности «Получение электронной корреспонденции».

Доля неправильно классифицированных сеансов и сеансов с недостаточной достоверностью классификации представлена в таблице 3.

При появлении нового вида сетевой деятельности и, соответственно, класса сеансов и попытке анализа сетевой деятельности в рамках этого класса программным комплексом при отсутствии статистики по этому классу, результат анализа будет нулевым. В этом случае необходимо сформировать новый класс сеансов путем накопления статистических данных, необходимых для анализа данного вида сетевой деятельности. Накопление данных производится по тому же алгоритму, который применяется при анализе сетевой активности на предмет существующих классов сеансов. Это анализ дампа памяти сетевой активности и вычисление на его основе статистических показателей.

Методика формирования нового класса сеансов включает в себя следующие шаги:

1. Определить, какой вид деятельности пользователей порождает новый класс сетевых сеансов и место нового класса в существующей классификации. Определить все возможные действия пользователя в рамках данного вида деятельности. Произвести первичное на-

копление статистических данных по данному виду деятельности без занесения в обучающую выборку;

2. Определить, насколько это возможно, границы и правила, в которых действует данный класс сеансов в соответствии с классификацией. На основании наблюдений первичного накопления статистических данных по новому виду деятельности произвести, если это необходимо, формирование новых интервалов значений статистических параметров для успешности проведения классификации по данному виду деятельности;

3. Произвести формирование обучающей выборки данного класса сеансов, а именно накопление сеансов, которые относятся исключительно к данному виду сетевой деятельности. Формирование производится снятием дампов памяти, содержащих исключительно данный вид деятельности;

4. Проведение анализа обучающей выборки, расчет статистических показателей, характеризующих данный класс сеансов. Для проведения анализа обучающей выборки используется метод кросс-проверки;

5. Запись обучающей выборки и результатов анализа в базу данных, которая используется для дальнейшей классификации сетевых сеансов по всем видам деятельности.

Заключение

Использование описанного метода классификации трафика вычислительной сети по видам деятельности в сочетании с традиционными средствами защиты (системы контроля доступа, системы защиты на основе сигнатурного анализа) позволяет повысить эффективность процедур защиты информации в РВС.

СПИСОК ЛИТЕРАТУРЫ

1. Информационные технологии в системе управления силами ВМФ / В.Ф. Шпак, Н.Ф. Директоров, В.И. Мирошников, С.П. Навойцев [и др.]. – СПб. : «Элмор», 2005. – 832 с.

2. Синещук Ю.И. Информационная безопасность и устойчивость геоинформационных систем оперативного управления // Сб. тр. V междунар. науч.-практ. конф. ИНФОГЕО 2018 «Геоинформационное обеспечение устойчивого развития территорий». В 2 т. – СПб. : РГГМУ, 2018. – Т. 2. – С. 235–241.

3. Синещук Ю.И., Куватов В.И., Синещук М.Ю. Модель выбора рационального состава системы защиты информации критически важных, потенциально опасных объектов // Региональная информатика и информационная безопасность : сб. тр. СПОИСУ. – СПб., 2016. – Вып. 2. – С. 249–255.

4. Васенин В.А., Макаров А.А. Статистические модели трафика телекоммуникационных компьютерных сетей и их использование // Тез. докл. Всерос. науч.-метод. конф. «Телематика-97». – СПб., 1997. – С. 51.

5. Концепция построения систем анализа и фильтрации Интернет-трафика на основе методов интеллектуального анализа данных / И.В. Машечкин, М.И. Петровский, В.В. Глазкова, В.А. Масляков // Математические методы распознавания образов : сб. докл. 13-й Всерос. конф. – М. : МАКС Пресс, 2007. – С. 494.

6. Морозов Д.И. Энтропийный метод анализа аномалий сетевого трафика в ip-сетях // Информационное противодействие угрозам терроризма. – 2003. – № 7. – С. 46.

7. Урьев Г.А., Шелухин О.И., Осин А.В. Экспериментальные исследования речевых потоков в сетях VoIP // Электротехнические и информационные комплексы и системы. – 2006. – № 2. – С. 54–58.

8. Горелик А.Л. Скрипкин В.А. Методы распознавания : учеб. пособие. – М. : Изд. «Высшая школа», 1977. – 221 с.

9. Манита А.Д. Теория вероятностей и математическая статистика : учеб. пособие. – М. : Издат. отдел УНЦ ДО, 2001 – 256 с.

10. Смирнов А.С., Козьмовский Д.В., Пантиховский О.В. Проблемы безопасности информации распределенных информационных систем объектов управления // Проблемы управления рисками в техносфере. – 2011. – Т. 18, № 2. – С. 88–92.

11. Козьмовский Д.В., Куватов В.И., Пантиховский О.В. К вопросу о классификации деятельности пользователей в распределенных сетях // Региональная информатика (РИ-2010) : тр. XII Санкт-Петербург. междунар. конф. / СПОИСУ. – СПб., 2011.– С. 157–160.

REFERENCES

1. Shpak V.F., Direktorov N.F., Miroshnikov V.I., Navoitsev S.P. et al. *Informatsionnye tekhnologii v sisteme upravleniia silami VMF* [Information Technologies in Control Systems of the Naval Forces]. St. Petersburg, Elmor Publ., 2005. 832 p.

2. Sineshchuk Iu.I. Informatsionnaia bezopasnost i ustoichivost geoinformatsionnykh sistem operativnogo upravleniia [Information Security and Stability of Geographical Information Supervisory Control Systems]. *Sb. tr. V mezhdunar. nauch.-prakt. konf. INFOGEO 2018 "Geoinformatsionnoe obespechenie ustoichivogo razvitiia territorii". V 2t.* [Proc. of the 5th Int. Sci. and Practical Conf. INFOGEO 2018 on Geographic Information Support of Sustained Development of Natural Areas]. St. Petersburg, RGGMU Publ., 2018, vol. 2, pp. 235–241.

3. Sineshchuk Iu.I., Kuvatov V.I., Sineshchuk M.Iu. Model vybora ratsionalnogo sostava sistemy zashchity informatsii kriticheski vazhnykh, potentsialno opasnykh obektov [Model Selection Rational Structure of Information Protection of Critical, Potentially Dangerous Objects]. *Regionalnaia informatika i informatsionnaia bezopasnost. Sb. tr. SPOISU* [SPOISU Proc. Regional Informatics and Information Security]. St. Petersburgb., 2016, iss. 2, pp. 249–255.

4. Vasenin V.A., Makarov A.A. Statisticheskie modeli trafika telekommunikatsionnykh kompiuternykh setei i ikh

ispolzovanie [Static Models of Telecommunication Traffic of Computer Networks and its Application]. *Tez. dokl. Vseros. nauch.-metod. konf. 'Telematika-97'* [Proc. of Russian Sci. and Methodological Conference 'Telematika-97']. St. Petersburg, 1997, pp. 51.

5. Mashechkin I.V., Petrovskii M.I., Glazkova V.V., Masliakov V.A. Kontseptsiia postroeniia sistem analiza i filtratsii Internet-trafika na osnove metodov intellektualnogo analiza dannykh [Concepts for Building the Systems for Analyzing and Filtering the Internet Traffic based on Datamining Methods]. *Matematicheskie metody raspoznavaniia obrazov. Sb. dokl. 13-i Vseros. konf.* [Proc. of the 13th Russian Conf. in Mathematical Methods of Image Recognizing]. Moscow, MAKS Press, 2007, pp. 494.

6. Morozov D.I. Entropiinyi metod analiza anomalii setevogo trafika v ip-setiakh [Entropy Analytical Procedure of Network Traffic in IP-Networks]. *Informatsionnoe protivodeistvie ugrozam terrorizma* [Information Countermeasures against Terrorism Threat], 2003, no. 7, pp. 46.

7. Urev G.A., Shelukhin O.I., Osin A.V. Eksperimentalnye issledovaniia rechevykh potokov v setiakh VoIP [Voice Traffic Experimental Study in the VoIP Networks]. *Elektrotekhnicheskie i informatsionnye kompleksy i sistemy* [Electrical and Data Processing Facilities and Systems], 2006, no. 2, pp. 54–58.

8. Gorelik A.L. Skripkin V.A. *Metody raspoznavaniia. Ucheb. posobie* [Recognition Technique. Textbook]. Moscow, Vysshaia shkola Publ., 1977. 221 p.

9. Manita A.D. *Teoriia veroiatnostei i matematicheskaia statistika. Ucheb. posobie* [The Theory of Probability and Mahtematical Statistics]. Moscow, UNTs DO Publ., 2001. 256 p.

10. Smirnov A.S., Kozmovskii D.V., Pantikhovskii O.V. Problemy bezopasnosti informatsii raspredelennykh informatsionnykh sistem obektov upravleniia [The Problems of Information Safety. Distributed Information Systems of Management Objects]. *Problemy upravleniia riskami v tekhnosfere* [Risk Management Problems in Technosphere], 2011, vol. 18, no. 2, pp. 88–92.

11. Kozmovskii D.V., Kuvatov V.I., Pantikhovskii O.V. K voprosu o klassifikatsii deiatelnosti polzovatelei v raspredelennykh setiakh [On User Activity Classification in Distributed Networks]. *Regionalnaia informatika (RI-2010). Tr. XII Sankt-Peterburg. mezhdunar. konf. SPOISU* [Regional Informatics (RI-2010). Proc. of the 12th St. Petersburg Int. Conf. SPOISU]. St. Petersburg, 2011, pp. 157–160.