МЕТОДИКА ОПЕРАТИВНОГО КОНТРОЛЯ ФУНКЦИОНАЛЬНОСТИ ИСПОЛЬЗОВАНИЯ РЕСУРСОВ И СЕРВИСОВ АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННО-УПРАВЛЯЮЩЕЙ СИСТЕМЫ ЕДИНОЙ ГОСУДАРСТВЕННОЙ СИСТЕМЫ ПРЕДУПРЕЖДЕНИЯ И ЛИКВИДАЦИИ ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЙ

В.С. Артамонов, доктор технических наук, доктор военных наук, профессор, заслуженный работник высшей школы Российской Федерации.
Министерство Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий.
С.В. Шарапов; М.Ю. Синещук.
Северо-Западный региональный центр МЧС России.
Д.В. Козьмовский, кандидат технических наук.
Институт проблем транспорта им. Н.С. Соломенко
Российской академии наук

Анализируются объективные противоречия, присущие системам и средствам автоматизации управления, связанные с функциональностью использования предоставляемых ресурсов и сервисов и с безопасностью информации. Обосновываются основные категории нарушителей безопасности и возможные угрозы, рассматривается методика снижения рисков, связанных с несанкционированной деятельностью в распределенных вычислительных сетях МЧС России, на основе анализа видов деятельности пользователей и классификации сетевого трафика.

Ключевые слова: автоматизированная система управления МЧС России, распределенные вычислительные сети, сетевой трафик

METHODS OF OPERATIONAL CONTROL OF FUNCTIONALITY USING RESOURCES AND SERVICES OF AUTOMATIC INFORMATION MANAGEMANT SYSTEM OF UNIFORM STATE SYSTEM OF PREVENTION AND LIQUIDATION OF EMERGENCY SITUATIONS OF EMERCOM OF RUSSIA

V.S. Artamonov. EMERCOM of Russia.
S.V. Sharapov; M.Yu. Sineshchuk. North-West regional centre of EMERCOM of Russia.
D.V. Kozmovsky.
Institute of transportation problems of N.S. Solomenko of Russian academy of sciences

Analyzed the objective contradictions inherent in systems and means of automation of management, associated with the use of resources and services, and information security. Defined categories of offenders security and potential threats, the methodology to reduce the risks of unauthorized activities in distributed computing networks of EMERCOM of Russia, based on the analysis of user activities and classification of network traffic.

Keywords: automatic management system of EMERCOM of Russia, distributed computing network, classification of network traffic

На сегодняшний день одним из основных способов информационного взаимодействия в МЧС России выбрана видеоконференцсвязь, которая позволяет в режиме реального времени передавать видео, графическую и голосовую информацию с места чрезвычайной ситуации. Подключение органов повседневного управления подсистем Единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций (РСЧС) к ведомственной цифровой сети связи с интеграцией услуг (ВЦССИУ) МЧС России позволит помимо взаимодействия в случае чрезвычайной ситуации также получать различные прогнозы и информационные материалы в режиме повседневного функционирования [1]. Наличие в арсенале средств автоматизированной информационной управляющей системы (АИУС) серверов аудио- и видеоконференцсвязи, FTP серверов, IP телефонных станций и других современных технических средств предполагает экспоненциальный рост трафика в ведомственной сети МЧС России.

Кроме того, использование интернет-технологий, электронной почты, корпоративных сервисов интрасети создает дополнительные возможности при управлении силами и средствами МЧС России. Формирование сети органов и объектов управления различного иерархического уровня МЧС России, автоматизация процессов управления привели к возникновению распределенных вычислительных сетей (РВС), обеспечивающих реализацию процессов управления и обеспечение поддержки принятия решений в АИУС МЧС России [2].

Вместе с тем современная практика организации функционирования РВС в рамках АИУС позволяет говорить о наличии противоречия, обусловленного, с одной стороны, опережающим развитием информационных технологий и автоматизированных средств управления, а с другой, их использование влечет за собою, помимо расширения предоставляемых сервисов, издержки безопасности.

Анализ задач и состава элементов РВС МЧС России выявил проблемы обеспечения безопасности, связанные с угрозами, исходящими от внутренних нарушителей – пользователей сети. На сегодняшний день количество возможных внутренних угроз значительно превышает количество внешних. Защита от внутреннего нарушителя является одним из наиболее приоритетных направлений обеспечения безопасности информационной системы.

Современные методы контроля деятельности пользователей и защиты информации не в полной мере способны обеспечить защиту информации от внутренних угроз. Сложность решения данного вопроса усиливается большим и непостоянным количеством пользователей РВС с разными уровнями доступа, большими объемами информации, циркулирующей внутри сети для обеспечения деятельности различных потребителей информационных ресурсов. Возникает еще одно противоречие между необходимостью поддержать достаточный уровень безопасности ресурсов РВС АИУС МЧС России и при этом обеспечить информационно-аналитическую поддержку основных видов деятельности объектов управления МЧС России, не снижая их функциональные возможности [3].

Предлагаемая методика выявления внутренних угроз безопасности подразумевает реализацию процедур мониторинга и анализа сетевого обмена данными внутри РВС АИУС РСЧС.

Формально РВС можно представить в виде множества:

$$S = \left(U,\ W,\ R\right),$$

где $U = \left\{u_i\right\}$ – множество пользователей РВС; $W = \left\{w_j\right\}$ – множество видов сетевой деятельности; $R = \left\{r_i\right\}$ – множество отношений U и W.

Под отношениями между пользователями и видами сетевой деятельности понимаются заданные соответствия каждому пользователю множества видов сетевой деятельности.

В процессе функционирования внутри РВС происходит непрерывный обмен данными в сети – сетевыми пакетами. В сетевом обмене участвует множество узлов как принадлежащих самой РВС, так и удаленных узлов.

Понятие сеанса появляется в результате временного анализа сетевого обмена. Под сеансом понимается непрерывный обмен сетевыми пакетами между одним узлом внутренней сети и одним удаленным узлом. Промежуток сетевого обмена, предназначенный для анализа, разделяется на сеансы, каждый из которых в результате классификации будет отнесен к тому или иному виду деятельности (рис. 1).

Рис. 1. **Пример временного анализа сетевого обмена**

Таким образом, N – бесконечное множество сеансов можно представить в следующем виде: $N = \{n_i\}$, а каждый сеанс:

$$n_i = \{ u_i, x_1, x_2, \ldots, x_n \},$$

где u_i – i пользователь системы; x_n – параметры сеанса.

Задача классификации – формализованная задача, в которой имеется множество объектов (сеансов), разделённых некоторым образом на классы. Необходим алгоритм, способный классифицировать произвольный сеанс из исходного множества. Классифицировать сеанс – значит указать вид деятельности, к которому он относится [4].

Существует целевая зависимость $N = \{(n_1, w_1), \ldots, (n_m, w_s)\}$. Требуется построить алгоритм: $a: N \to W$, способный классифицировать произвольный сеанс $n \in N$.

Методика классификации трафика предусматривает:

– каждый сеанс рассматривается как объект, характеризуемый набором статистических параметров;

– статистические параметры объекта являются независимыми между собой;

– статистическое распределение значений параметров сеансов различается в зависимости от вида деятельности;

– для каждого сеанса собираются и анализируются значения всех параметров;

– классификация сеанса производится на основе обучающей выборки, которая содержит распределения значений параметров эталонных сеансов для каждого вида деятельности.

Структура методики представлена на рис. 2.

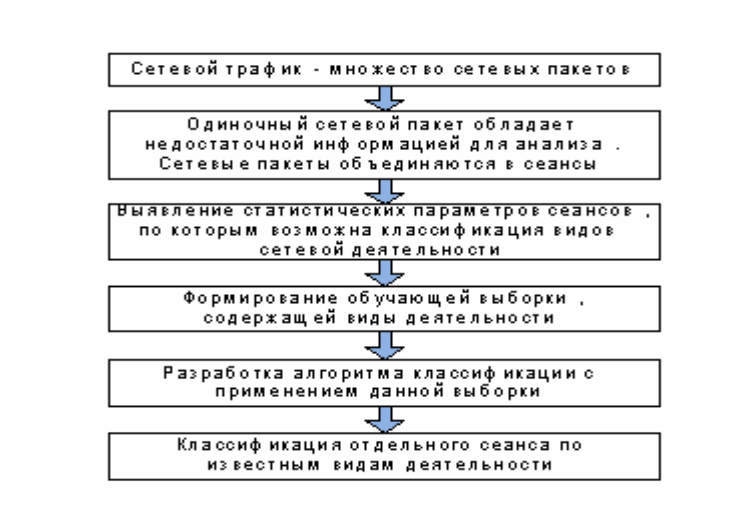


Рис. 2

Разработанная методика включает в себя подготовку трафика в виде данных, пригодных для анализа, то есть формирование сеансов, определение статистических характеристик трафика, выбор параметров, которые буду использоваться для классификации видов деятельности и построения диаграммы распределений параметров классификации для видов штатной деятельности РВС АИУС МЧС России.

Первым этапом анализа сетевой деятельности является подготовка входных данных – статистических параметров сеанса.

Существуют различные инструменты мониторинга вычислительных сетей. Они перехватывают пакеты или кадры, передаваемые между компьютерами или сетевыми устройствами. Затем анализаторы декодируют (интерпретируют) перехваченные пакеты, то есть преобразуют их из двоичного формата к виду, пригодному для анализа человеком. Многие анализаторы протоколов предоставляют статистическую информацию о перехваченных пакетах в текстовом или графическом виде.

Результатом захвата трафика является файл с расширением *.txt, в котором содержится информация, взятая из заголовков сетевых пакетов. Размер захваченного файла зависит от временного интервала, в течение которого производился захват трафика и интенсивности сетевой активности, количества узлов, подверженных мониторингу в этот период.

В целом статистические параметры сетевых сеансов, которые можно получить из заголовков сетевых пакетов и использовать в целях анализа и классификации трафика по видам деятельности содержат:

– общий объем анализируемого трафика;
– объем исходящего трафика;
– объем входящего трафика;
– долю исходящего трафика;
– количество пакетов в сеансе;
– средний размер пакета в сеансе;
– количество внутренних портов;
– количество внешних портов.

Временной анализ сетевого обмена узлов вычислительной сети и последующее формирование сеансов производится по алгоритму (рис. 3).

Определение параметров, пригодных для классификации, производится, применяя проверку наличия связи статистических параметров и видов деятельности и наличия связи между статистическими параметрами. В результате анализа статистических характеристик были отобраны следующие параметры классификации:

– количество внешних портов;

– количество внутренних портов;
– доля исходящего трафика;
– средний размер пакета.

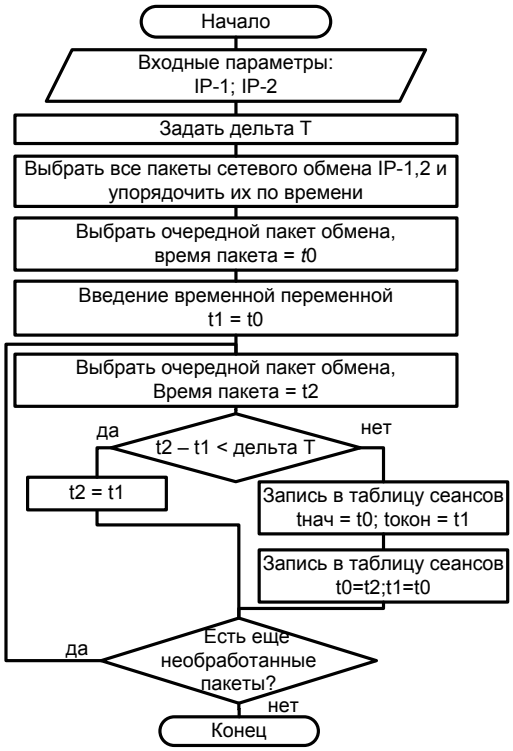


Рис. 3. **Алгоритм формирования сеансов**

Этапы методики анализа видов деятельности, выполнение которых обеспечивают эксперты, включают в себя:

Этап «Формирование нового класса сеансов», который состоит из:

– определения вида деятельности, которому соответствует данный класс сеансов;

– определения действий пользователя в рамках данного вида деятельности;

– накопления статистических данных по данному виду деятельности.

Этап «Анализ статистических данных параметров классификации нового вида деятельности», который состоит из:

– подсчета статистических характеристик сеансов;

– построения диаграмм распределения параметров классификации;

– формирования интервалов значений параметров классификации.

Этап «Формирование обучающей выборки нового класса сеансов», который состоит из:

– накопления сеансов, соответствующих новому виду деятельности;

– анализа накопленной статистики методом кросс-проверки;

– формирования обучающей выборки нового класса сеансов для классификации.

Таким образом, формируется накопленная статистика значений параметров классификации сеансов по различным видам сетевой деятельности – обучающая выборка, которая содержит эталонные сеансы. Каждый параметр имеет определенное распределение на интервале значений. Однако этот набор данных трудно поддается анализу, и делать по ним какие-то выводы невозможно. Поэтому производится их группировка.

Группировка представляет собой процесс систематизации или упорядочения первичных данных с целью извлечения содержащейся в них информации. Группировка заключается в распределении параметров классификации по интервалам, каждый из которых содержит некоторый диапазон значений изучаемого признака.

Сформированные интервалы для различных видов деятельности показаны на рис. 4.

Рис. 4. **Распределение значений статистических параметров разных видов деятельности**

В результате выполнения методики анализа видов деятельности были получены диаграммы распределений параметров классификации видов деятельности, свойственных РВС АИУС РСЧС (рис. 5).

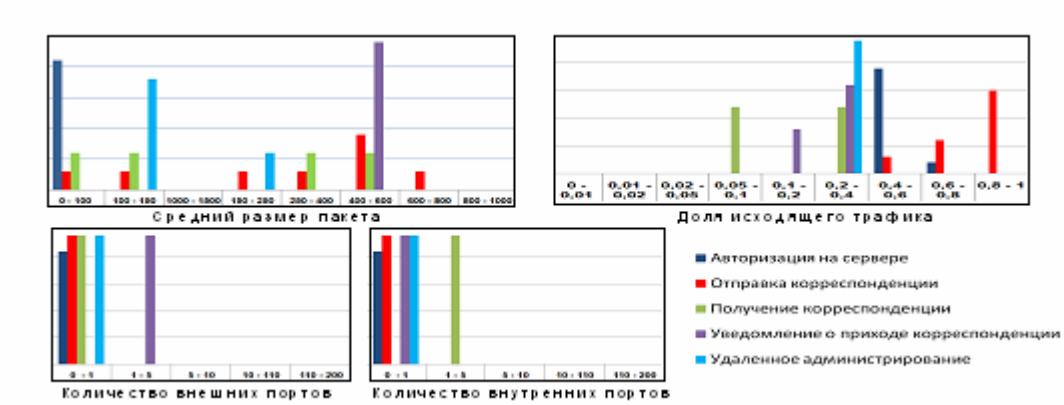


Рис. 5. **Распределение параметров классификации по интервалам видов деятельности**

Обработка трафика позволяет выявить параметры, которые характеризуют сеанс в зависимости от вида деятельности, которому он принадлежал.

Учитывая, что параметры классификации сеанса независимы, условную вероятность соответствия параметров классификации X данному виду деятельности H_i определяем как произведение по *j=от 1 до s* вероятностей соответствия каждого параметра классификации x_j виду деятельности H_i, где s – количество параметров классификации одного сеанса:

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

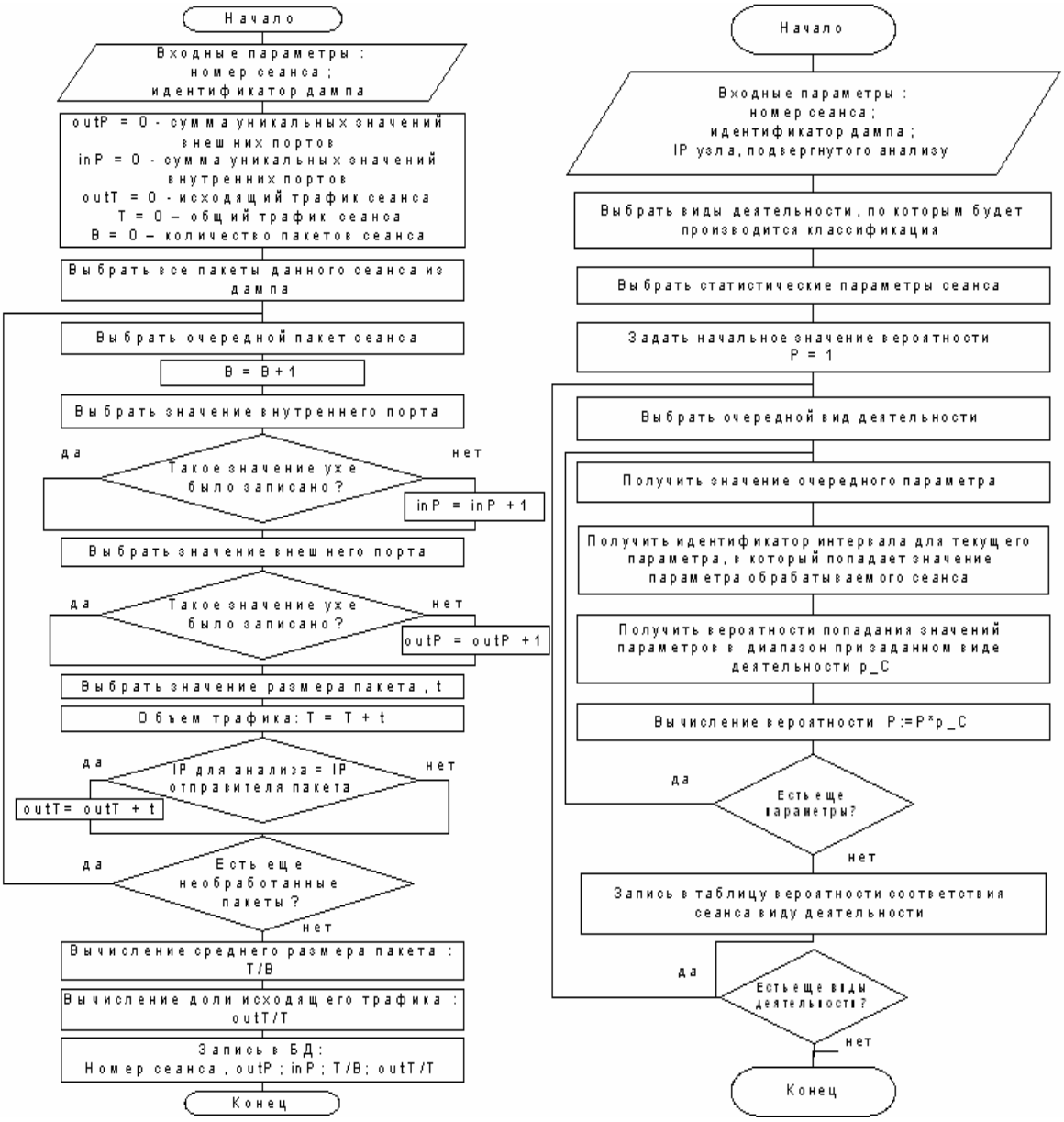
Для каждого нового сеанса, который подвергается классификации, вычислялись значения параметров классификации и определялись интервалы, в которые попали рассчитанные значения. Вероятность соответствия каждого вычисленного параметра x виду деятельности H_i вычислялась как относительная частота интервала – отношение числа

параметров, значения которых попали в данный интервал, к общему числу параметров вида деятельности H_i:

$$P(x \mid H_i) = \frac{m}{M},$$

где M – общее количество значений данного параметра x в обучающей выборке, накопленное эталонными сеансами вида деятельности H_i; m – количество значений данного параметра x, накопленное эталонными сеансами вида деятельности H_i в интервале, в который попадает вычисленное значение параметра классифицируемого сеанса.

Комплексный алгоритм автоматизированной классификации трафика по видам деятельности представлен на рис. 6. Он состоит из двух частей: алгоритма вычисления статистических характеристик сеанса (рис. 6а) и алгоритма выявления соответствия параметров сеанса определенному виду деятельности (рис. 6б).



а) б)

Рис. 6. **Классификация параметров трафика по видам деятельности пользователей в РВС АИУС РСЧС**

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

При сформированной статистике известных классов сеансов, соответствующих видам сетевой деятельности, определение данных классов при помощи описанных правил производится практически в автономном от человека режиме. На вход подается дамп памяти, а на выходе получаются статистические показатели анализируемой сетевой деятельности и вероятностная оценка соответствия данной деятельности ее шаблону.

Для проверки работоспособности методики сформулированы риски, связанные с этими видами деятельности:

– утечки информации через пользователей, ведущих электронную переписку;

– нестабильность работы сети из-за увеличения трафика;

– невыполнение штатных обязанностей;

– заражение вирусами через электронную почту и сайты Интернета;

– сетевые атаки;

– утечки информации через ftp-трафик.

В совокупности эти риски могут привести к серьезным последствиям для РВС, а именно, к срыву выполнения задач объекта управления.

В ходе тестовых испытаний выполнялись действия, связанные с несанкционированной деятельностью пользователей, то есть связанные с рисками для РВС. Для этого производилась следующая деятельность:

– запросы на WEB-сервер для эмуляции web-серфинга в интернете;

– обмен данными с FTP-сервером;

– отправка и получение электронной корреспонденции с почтового сервера.

В ходе тестирования имитировались действия пользователя, связанные с рисками утечки информации.

Тестирование проводилось в двух режимах:

– режим только со штатной системой защиты информации (СЗИ);

– режим со штатной СЗИ и программной реализацией автоматизированной классификации трафика по видам деятельности.

Оценка результатов производилась следующим образом:

– ставился один балл, в случае любого обнаружения подозрительного действия с последующей сигнализацией и записью в журнал отчетов специалисту по безопасности информации;

– ставилось ноль баллов, в случае отсутствия реакции на несанкционированную деятельность.

Результаты сравнительного тестирования представлены на рис. 7.

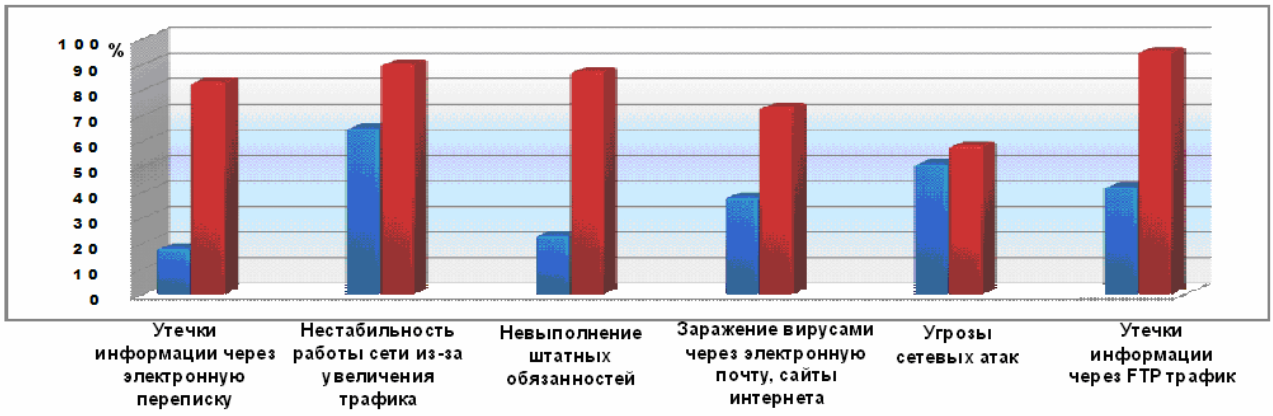


Рис. 7. **Результаты сравнительного тестирования**

Детальная информация представлена в табл. 1, 2.

Таблица 1. **Результаты проведения оценки эффективности**

Риски нарушения информационной безопасности	Применение штатных СЗИ		Применение штатных СЗИ и метода анализа видов деятельности		Всего использованных угроз
	количество выявленных угроз	% выявленных угроз	количество выявленных угроз	% выявленных угроз	
Утечки через электронную почту	5	18,5	22	81,5	27
Нестабильность работы сети из-за увеличения трафика	18	66,6	25	92,5	27
Невыполнение штатных обязанностей	6	22	24	89	27
Заражение вирусами через электронную почту, сайты	10	37	20	74	27
Сетевые атаки	14	54	16	61,5	26
Утечки информации через FTP-трафик	11	42	24	92,3	26

Таблица 2. **Совокупная оценка эффективности**

Совокупная эффективность средств защиты		
режим функционирования	кол-во выявленных несанкционированных действий	% от максимума (160)
только штатные СЗИ	64	39,5
штатные СЗИ и метод анализа трафика	131	81,7

Таким образом, применение предложенной методики совместно со штатными средствами защиты позволяет повысить эффективность выявления несанкционированной деятельности более чем в два раза, с 39,5 % до 81,7 % (на 42,2 %).

Литература

1. Об утверждении Положения о системе и порядке информационного обмена в рамках Единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций: Приказ Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий от 26 авг. 2009 г. № 496 // Рос. газ. 2009. 23 окт.

2. Артамонов В.С., Кадулин В.Е., Козленко Р.Н. Информационное обеспечение государственной пожарно-спасательной службы в условиях чрезвычайных ситуаций // Вестник С.-Петерб. ин-та ГПС МЧС России. 2003. № 3.

3. Основные угрозы и направления обеспечения безопасности единого информационного пространства / Ю.И. Синещук [и др.] // Вестн. С.-Петерб. ун-та МВД России. 2013. № 2. С. 150–154.

4. Малыгин И.Г., Козьмовский Д.В. Методы обеспечения безопасности распределенных информационных систем МЧС России, основаннных на анализе трафика и контроле сетевой деятельности пользователей // Проблемы управления рисками в техносфере. 2013. № 2 (26). С. 78–82.