Анализ возможностей фильтрации трафика на межсетевом экране xFirewall

М.Ф. Андреев, А.С. Исмагилова

Уфимский Университет Науки и Технологий, Уфа

Аннотация: В данной статье анализируются возможности отечественного межсетевого экрана следующего поколения (NGFW) xFirewall с контролем состояния сессий. Рассматриваются его защитные функции и на реальных примерах иллюстрируются возможности по фильтрации сетевого трафика по различным признакам. Статья может быть полезна для специалистов занимающихся разработкой, внедрением или эксплуатацией современных межсетевых экранов.
Ключевые слова: межсетевой экран, ngfw, xfirewall, spi, импортозамещение, критическая информационная инфраструктура, защита информации, dpi, фильтрация трафика, контроль сессий, ViPNet, firewall

В условиях актуальной повестки, а именно - указа Президента Российской Федерации от 01.05.2022 № 250 "О дополнительных мерах по обеспечению информационной безопасности Российской Федерации" многим коммерческим компаниям и государственным предприятиям пришлось задуматься о поиске аналогов текущим решениям, обеспечивающим реализацию политик информационной безопасности на местах. В преобладающем числе случаев решения по защите информации, в том числе, сетевое оборудование, например, межсетевые экраны были от нероссийских компаний, как пример: CheckPoint (Israel, Tel-Aviv), FortiNet [1] (USA, Sunnyvale) Cisco (USA, Sun Jose), Huawei (China, Shenzhen), Palo Alto (USA, California). Справедливости ради, к моменту выхода указа у многих российских компаний, производящих решения по фильтрации трафика и защите информации, уже были готовые решения с большим охватом по опыту эксплуатации, но, как выяснилось уже позже, всё-таки существовал недостаток в наполнении функционала, в ряде случаев не хватало производительности. Эти недостатки производители средств защиты информации решали уже в ускоренном порядке.

В рамках данной статьи рассмотрим шлюз безопасности xFirewall, который производится компанией АО «ИнфоТеКС», описание с официального сайта гласит, что xFirewall это - «…межсетевой экран следующего поколения, сочетающий функции классического межсетевого экрана: анализ состояния сессии, проксирование, трансляция адресов; с расширенными функциями анализа и фильтрации трафика такими, как: глубокая инспекция протоколов, выявление и предотвращение компьютерных атак [2], инспекция SSL/TLS-трафика, взаимодействие с антивирусными решениями, DLP (Data Leak Prevention) и песочницами.»

Данный межсетевой экран поставляется в двух исполнениях – виртуальном и в виде программно-аппаратного комплекса (далее ПАК). Виртуальное исполнение может быть развёрнуто на разных гипервизорах 1-го и 2-го типов – Hyper-V от Microsoft, VMWare Workstation или ESXi, ProxMox, Xen (Citrix).

К анализу представлен ПАК xFirewall 100 и одна из его последних версий СПО (специального программного обеспечения) – 5.6.2.

ПАК обладает возможностями управления через Web-интерфейс, CLI (command line interface) посредством SSH, COM-консоли или VGA подключения. Во время первоначальной инициализации ПАК’а, в которую входит инициализация ключевого дистрибутива, воспользоваться можно только COM-консолью или VGA, а уже затем с помощью настроек управлять устройством с помощью SSH или WebUI. Файл, содержащий ключевую информацию (.dst), загрузить на ПАК возможно посредством CD-дисковода, USB-диска или с помощью протокола TFTP. Для загрузки ключей с помощью TFTP нужна предварительная настройка статического IP-адреса на клиентском устройстве, с которого будет передаваться файл на специальный технический. На самом ПАК необходимый адрес уже задан на интерфейсе eth1.

xFirewall предлагает ролевую модель доступа [3] к управлению ПАКом. Роли две (в самом ПАК они называются «режимами»), иллюстрация на Рис.1 ниже:

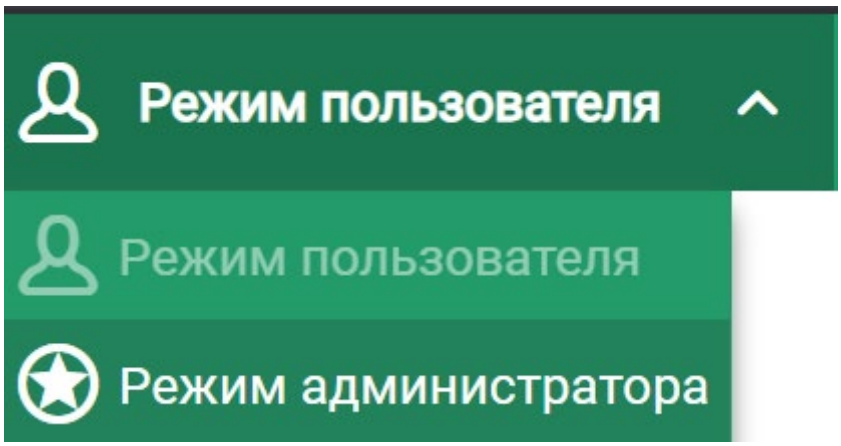

Рис. 1. – Две роли для работы с ПАК

Основное отличие режима администратора от режима пользователя заключается в возможности выполнения на ПАК действий, которые могут влиять на проходящий через него трафик, например, создание правил межсетевого экрана и правил трансляции адресов источника и/или назначения.

Рассмотрим основные возможности по фильтрации трафика и в целом структуру правил. На рис.2 представлен интерфейс создания правил межсетевого экрана (далее МЭ):

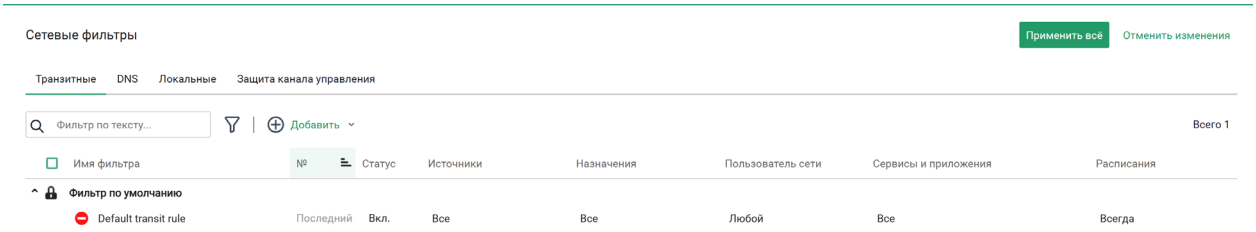

Рис. 2. – Две роли для работы с ПАКом

Следует обратить внимание, что xFirewall, являясь сертифицированным ФСТЭК МЭ, по умолчанию предполагает политику обработки трафика «запрещено всё, что не разрешено». Правила по умолчанию будут блокировать любой трафик, кроме служебного, куда входят порты, которые

обслуживают необходимые службы для инфраструктуры сети ViPNet, в рамках которой и функционирует ПАК xFirewall.

Типы фильтров подразделяются на транзитные, локальные и защищенные. В транзитных фильтрах задаются правила для обработки трафика, который не предназначен самому ПАК, а идёт через него, т.е. транзитом. В этих фильтрах возможно также указание необходимости проверки трафика в системе предотвращения вторжений, его антивирусной проверке, а также необходимости SSL-Inspection [4]. Также есть возможность задать проверку в трафике совпадения по базе пользователей из Active Directory или LDAP, возможность указать желаемые к пропуску или блокированию приложения или прикладные протоколы, а также их же, но в виде заранее приготовленных групп.

ПАК, с помощью технологии Deep Packet Inspection (далее DPI), позволяет сопоставлять в трафике принадлежность конкретного прикладного протокола, приложения или группы приложений к паттернам на прикладном уровне модели OSI. Когда трафик классифицирован, по нему можно принимать решения аналогично любым другим правила МЭ, а именно - запретить или разрешить. Ключевой особенностью классификации трафика с помощью DPI является тот факт, что приложение может работать на любом порту, но при этом с помощью DPI оно будет выявлено, т.к. классификация происходит на прикладном уровне. Как пример, в целях безопасности часто меняют порт у SSH-сервера, но сами признаки трафика SSH будут такими же, в журнале пакетов будет определён протокол и изменённый порт. Как пример, группа приложений «Messaging» ожидаемо позволит контролировать в транзитном трафике наиболее популярные приложения для обмена сообщениями, такие, как WhatsApp, Telegram, Viber, Threema, а также многие другие. Иллюстрация создания сетевого фильтра на рис.3. Следует отметить,

что возможность работы с трафиком на прикладном уровне существует только для транзитных пакетов.

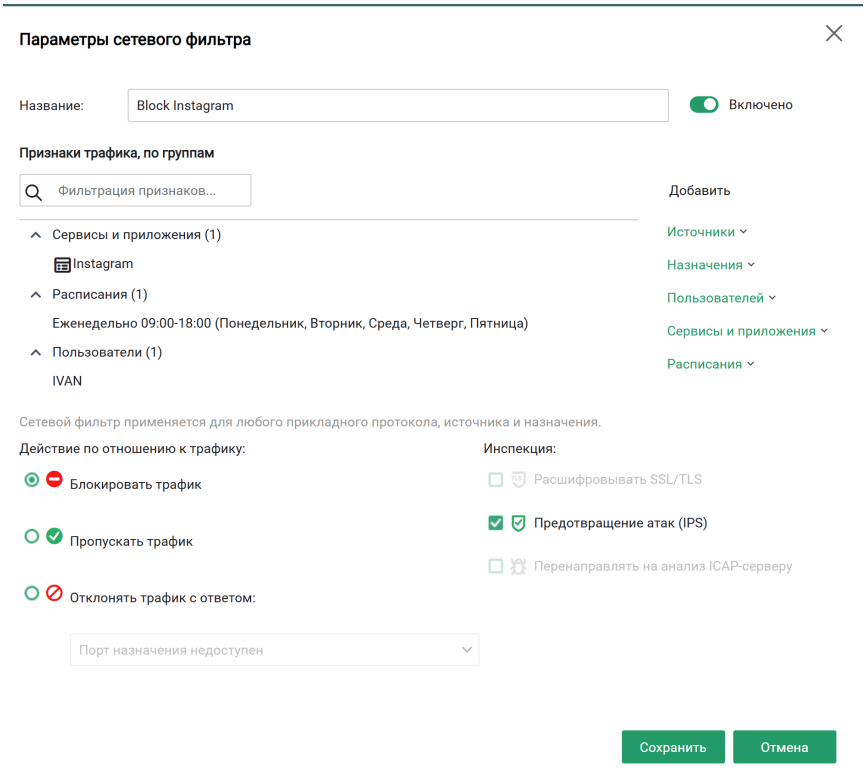

Рис. 3. – Создание транзитного фильтра на ViPNet xFirewall

Следует пояснить, какой эффект произведёт такой транзитный фильтр на сетевой трафик. В результате трафик приложения Instagram будет заблокирован с 09:00 утра до 18:00 вечера в будние дни, от времени, которое задано на ПАКе для пользователя IVAN, в дополнение трафик, который попал под условия данного правила, будет проверяться на предмет наличия признаков зловредной активности в системе предотвращения вторжений. Т.е., помимо логики МЭ, решение о блокировке трафика может принять система предотвращения вторжений. Для того, чтобы ПАК начал обрабатывать пакеты с локальным фильтром, нацеленным на блокирование ICMP [5] трафика, необходимо с помощью CLI создать соответствующий фильтр командой как на Рис 4. Команда приведена в полном виде, однако

может быть введена и в сокращённом, также возможно автодополнение ввода по клавише TAB.

```
xfva-4a43001f# firewall local add 1 src @any dst @any icmp drop
```

Рис. 4. – Создание локального фильтра на ViPNet xFirewall

Отправляем ICMP echo сообщения на xFirewall, на Рис 5:

```
root@debian:~# ping 10.52.57.252 -c 3
PING 10.52.57.252 (10.52.57.252) 56(84) bytes of data.

--- 10.52.57.252 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2052ms
```

Рис. 5. – Создание локального фильтра на ViPNet xFirewall

С помощью команды отображения журнала пакетов iplir view задаём условия для поиска искомого события, на Рис 6:

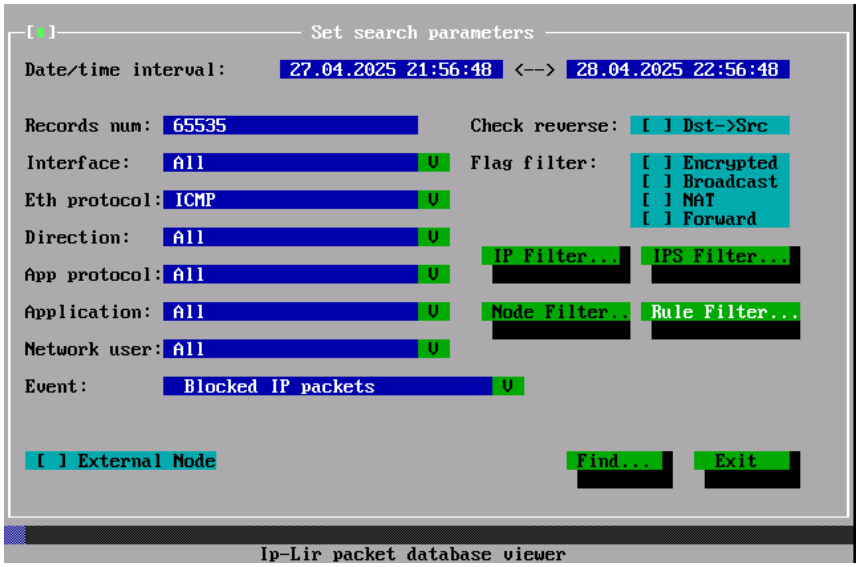

Рис. 6. – Меню журнала пакетов ViPNet xFirewall

Подтвердив условия поиска, наблюдаем в результатах поиска 3 заблокированных [6] ICMP пакета с событием 30 – Локальный IP-пакет заблокирован фильтром открытой сети (Рис. 7). Для уменьшения нагрузки на ПАК, устройство по умолчанию регистрирует только заблокированные пакеты любого типа трафика. Это опциональная настройка по усмотрению пользователя.

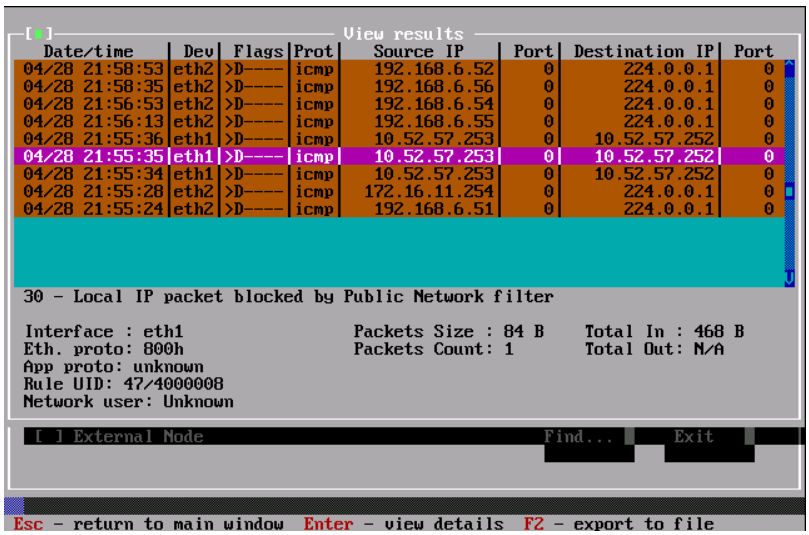

Рис. 7. – Результат поиска события в журнале пакетов ViPNet xFirewall

Для получения подробной информации по событию нужно выбрать событие. В предоставленных данных будет время начала и конца события, с какого сетевого интерфейса поступил пакет, IP-протокол [7] задействованный в событии, каким правилом был пропущен, заблокирован или же отброшен пакет, а также направление, IP-адреса источника и назначения и другая информация. Подробнее на Рис.8:

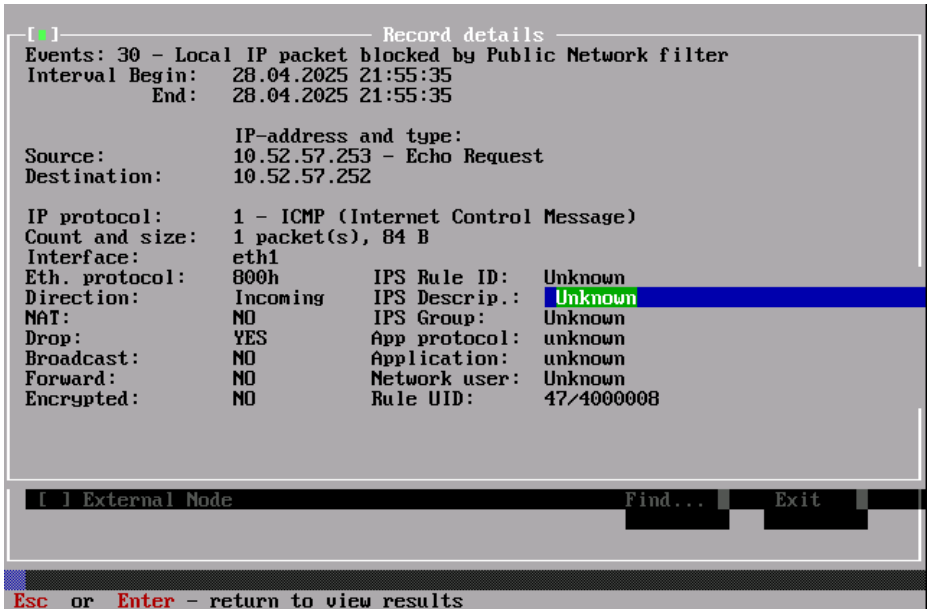

Рис. 8. – Вывод подробной информации по событию из журнала пакетов xFirewall

Следует отметить, что информация о событиях в журнале пакетов доступна как через CLI, так и через Web-интерфейс и по информационной наполненности эти два подхода не отличаются друг от друга. На Рис.9 заданы условия, аналогичные тем, что были заданы в CLI.

WebUI предоставляет более удобный для пользователя интерфейс, требующий наличия стороннего устройства для подключения, например, ноутбука. В то же время CLI требует наличия лишь консольного кабеля и монитора. В обоих случаях правилами пользования особенно отмечается, что управления допускается только из границ контролируемой зоны.

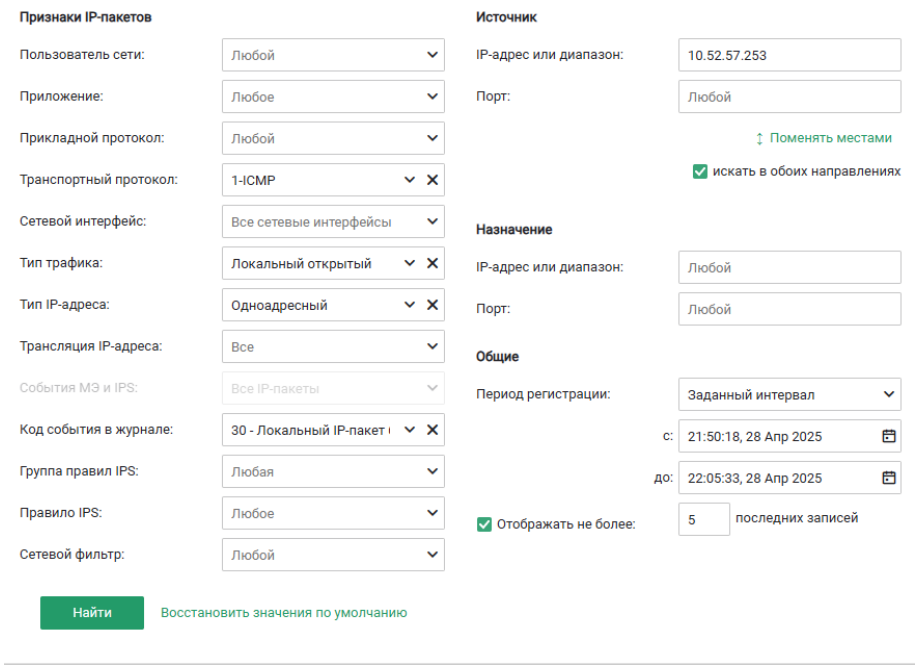

Рис. 9. – Задание условий для поиска в журнале пакетов ViPNet xFirewall через Web-интерфейс

Важно иметь возможность восстановить хронологию действий, совершаемых на устройстве. Данная возможность реализована через систему аудита [8] посредством ведения системного журнала. Сетевой фильтр, заданный выше для блокирования ICMP-трафика в системном журнале, записывается следующей строкой, как на Рис.10. Важной особенностью

ведения системного журнала является доказуемость записей в нём, что обеспечивается невозможностью их модификации или удаления таким образом, чтобы об этом не осталось записи. Иными словами, невозможно совершить такие действия на устройстве, чтобы об их сути не осталось никакой информации. Подобная мера является одним из требований для сертифицированных средств защиты информации в принципе.

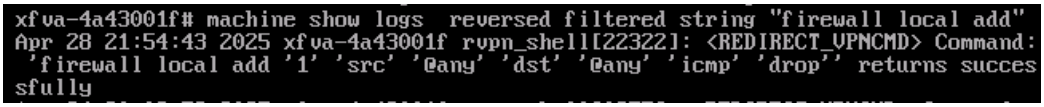

Рис. 10. – Событие аудита в системном журнале

В целях обеспечения отказоустойчивости в ПАК xFirewall реализована технология резервирования [9] по схеме «активный-пассивный». Для организации кластера потребуется два одинаковых ПАК и два одинаковых ключа. Между двумя узлами, которые имеют активную роль и пассивную роль, присутствует т.н. интерфейс синхронизации, по которому узел, имеющий активную роль, передаёт сделанные пользователем настройки на пассивный узел. Когда наступает момент, в который узел, исполняющий пассивную роль, понимает, что ему необходимо занять активную роль, он продолжает выполнять активную роль после переключения, обладая идентичными данными, которые он всё время перенимал от узла, находящегося в активной роли.

Логика, по которой узел, выполняющий пассивную роль, понимает, что необходимо переключение в активную роль, основана на принципе опроса по протоколу ARP каналов активного узла, и, если тот не отвечает некоторое количество раз, пассивный узел принимает решение о переключении. Также, со своей стороны, активный узел обладает механизмом определения собственной неработоспособности – он производит посылку ICMP echo сообщений на заранее заданный узел, и в том случае, если ответ от узла не приходит, инициирует собственную перезагрузку. Реализован и механизм

определения конфликтных ситуаций – если по какой-либо причине узел, выполняющий пассивную роль, перезагрузится и загрузится как активный узел, то механизм определения конфликта ролей [10] отправит в принудительную перезагрузку тот узел, который позже имел намерение стать активным. Таким образом обеспечивается и непрерывность в обслуживании.

В заключение отметим, что из вышеприведённых данных можно сделать вывод, что с помощью xFirewall можно осуществлять манипуляции с сетевым трафиком на уровнях модели OSI от сетевого до прикладного, а также осуществлять мониторинг корректности срабатывания правил путём задания условий поиска в журнале пакетов, искать причины поломок в сети с помощью этого же инструмента. Вышеприведённые факты также говорят о завершённости данного решения, возможности его применения на «боевых» сетях, где очень важна возможность поиска проблемы на ходу и предъявляются повышенные требования к инструментам диагностики.

Литература

1. Кацупаев А.А., Щербакова Е.А., Воробьёв С.П. Постановка и формализация задачи формирования информационной защиты распределённых систем // Инженерный вестник Дона, 2015, №1. URL: ivdon.ru/uploads/article/pdf/IVD_86_katsupeev.pdf_79178b4853.pdf

2. Шатурный М.В. Анализ актуальных угроз и разработка подходов к защите веб-приложений // Инженерный вестник Дона, 2024, №7. URL: ivdon.ru/uploads/article/pdf/IVD_58N7y24_Shaturniy.pdf_84babdb54b.pdf

3. Миняев А.А. Методика оценки эффективности системы защиты территориально-распределённых информационных систем: дис. … канд.техн.наук: 2.3.6. СпБ., 2021. 215 с.

4. Dormann Will Risks of SSL Inspection // Carnegie Mellon University, 2015

URL: insights.sei.cmu.edu/blog/the-risks-of-ssl-inspection/

5. Krystosek Paul, Shimeall Timothy J., Ott Nancy Network Traffic Analysis with SiLK: Profiling and Investigation Cyber Threats // Carnegie Mellon University, 2019. URL: insights.sei.cmu.edu/blog/the-risks-of-ssl-inspection/

6. Карташевский В.Г., Поздняк И.С. Фильтрация наблюдаемого трафика как способ обнаружения вторжений // Вестник УрФО №1(31), 2019, с.17-22.

7. Самаров В.В. Использование системы аудита операционных систем семейства linux при проведении сертификационных испытаний программных изделий // Надёжность и качество сложных систем, 2021 №1, с.144-149.

8. Майлыбаев Е.К., Жамангарин Д.С., Сапарходжаев Н.П. Реализация отказоустойчивой серверной инфраструктуры // Вестник КазАТК №2 (131), 2024, с.367-375.

9. Мещеряков А.И. Методы выполнения атаки “|ARP-Spoofing” и способы защиты от неё // Материалы Международной научно-практической конференции. В 2-х частях. Том Часть 1, 2021, с.80-85.

10. Михайлова В.Д. Описание инцидента при тестировании информационной безопасности киберфизических систем // Инженерный вестник Дона, 2025, №6. URL: ivdon.ru/uploads/article/pdf/IVD_74N5y25_Mihajlova.pdf_6274419cec.pdf

References

1. Kaczupaev A.A., Shherbakova E.A., Vorobyov S.P. Inzhenernyj vestnik Dona, 2015, №1. URL: ivdon.ru/uploads/article/pdf/IVD_86_katsupeev.pdf_79178b4853.pdf

2. Shaturny M.V. Inzhenernyj vestnik Dona, 2024, №7. URL: ivdon.ru/uploads/article/pdf/IVD_58N7y24_Shaturniy.pdf_84babdb54b.pdf

3. Minyaev A.A. Metodika ocenki e`ffektivnosti sistemy` zashhity` territorial`no-raspredelyonny`x informacionny`x sistem [Methodology of an

estimation of efficiency of protection system of territorially distributed information systems] : kand.texn.nauk: 2.3.6. SpB., 2021. 215 p.

4. Dormann Will Risks of SSL Inspection. Carnegie Mellon University, 2015. URL: insights.sei.cmu.edu/blog/the-risks-of-ssl-inspection/

5. Krystosek Paul, Shimeall Timothy J., Ott Nancy Network Traffic Analysis with SiLK: Profiling and Investigation Cyber Threats Carnegie Mellon University, 2019. URL: insights.sei.cmu.edu/blog/the-risks-of-ssl-inspection/

6. Kartashevskiy V.G., Pozdnyak I.S. Vestnik UrFO №1(31), 2019, pp.17-22.

7. Samarov V.V. Reliability and Quality of Complex Systems, 2021 No. 1, pp.144-149.

8. Mailybaev E.K., Zhamangarin D.S., Saparkhodjaev N.P. Vestnik KazATK №2 (131), 2024, pp.367-375.

9. Meshcheryakov A.I. Materialy` Mezhdunarodnoj nauchno-prakticheskoj konferencii. V 2-x chastyax. Tom Chast` 1, 2021, pp.80-85.

10. Mixajlova V.D. Inzhenernyj vestnik Dona, 2025, №6. URL: ivdon.ru/uploads/article/pdf/IVD_74N5y25_Mihajlova.pdf_6274419cec.pdf

Дата поступления: 5.05.2025

Дата публикации: 27.06.2025