Научная статья
УДК 004.716
ББК 32.971.35
К 38
DOI: 10.53598/2410-3225-2023-1-316-52-58

Отечественный Интернет-шлюз для небольшого офиса

(*Рецензирована*)

Асхад Асланчериевич Киздермишов[1], Сулиет Халидовна Киздермишова[2]

[1] *Адыгейский государственный университет*, *Майкоп*, *Россия*, *Askhad_75@rambler.ru*
[2] *Майкопский государственный технологический университет*, *Майкоп*, *Россия*, *Suliet@rambler.ru*

Аннотация. *Рассматриваются вопросы замены программных пакетов SQUID, SQUIDGUARD и SARG отечественным программным обеспечением для небольшого офиса. При этом под решением для небольшого офиса подразумевается применение встроенных в операционную систему средств и открытых программных пакетов* (*свободно распространяемого программного обеспечения*)*. Даны рекомендации по выбору отечественных операционных систем и применению Uncomplicated Firewall* (*UFW*)*.*

Ключевые слова: *SQUID, SQUIDGUARD, SARG, прокси-сервер, Интернет-шлюз, импортозамещение*, *Astra Linux*, *ALT Linux*, *Uncomplicated Firewall* (*UFW*)

Original Research Paper

Domestic Internet gateway for a small office

Askhad A. Kizdermishov[1], Suliet Kh. Kizdermishova[2]

[1] *Adyghe State University*, *Maikop*, *Russia*, *Askhad_75@rambler.ru*
[2] *Maikop State University of Technology*, *Maikop*, *Russia, Suliet@rambler.ru*

Abstract. *The issues of replacing the SQUID, SQUIDGUARD and SARG software packages with domestic software for a small office are considered, while the solution for a small office means the use of tools built into the operating system and open software packages* (*freely distributed software*)*. Recommendations on the choice of domestic operating systems and the use of Uncomplicated Firewall (UFW) are given.*

Keywords: *SQUID, SQUIDGUARD, SARG, proxy server, Internet gateway, Import substitution*, *Astra Linux*, *Alt Linux*, *Uncomplicated Firewall* (*UFW*)

Переход на отечественное программное обеспечение является актуальной задачей информационной безопасности. В условиях обострения геополитической обстановки Правительство Российской Федерации предпринимает меры по форсированию перехода на отечественное программное обеспечение на объектах критической информационной инфраструктуры. К первому января 2025 года планируется завершить первый масштабный переход к использованию отечественных программных продуктов. В частности, наиболее распространенные в государственном секторе операционные системы семейства Microsoft Windows должны быть заменены на отечественные операционные системы.

Очевидно, что в дальнейшем переход на применение отечественного программного обеспечения должен быть осуществлен во всем государственном секторе вне зависимости от масштаба автоматизированной информационной системы государствен-

ного учреждения. Если для больших корпоративных систем такой переход может быть осуществлен с помощью специализированных ИТ-компаний, например, в рамках реализации ведомственных концепций развития государственных информационных систем, то для небольших офисов – только силами штатных работников. При этом ситуация усложняется тем, что в небольших офисах, как правило, работают неопытные администраторы [1]. Кроме этого, для небольшого офиса целесообразно применять бюджетные решения, основанные на использовании встроенных в операционную систему средств и открытых программных пакетов (свободно распространяемого программного обеспечения).

Под Интернет-шлюзом для малого офиса будем понимать прокси-сервер, редиректор и генератор отчетов, совместно установленные на базе открытой операционной системы. Решение для Интернет-шлюза, основанное на свободно распространяемом иностранном программном обеспечении, было в работах [2–5]. В качестве операционной системы была предложена операционная система Ubuntu, а в качестве прокси-сервера, редиректора и генератора отчетов – программные пакеты SQUID, SQUIDGUARD и SARG, соответственно. Предложенное ранее решение может быть использовано только после оценки всех сопутствующих рисков, которые связаны с тем фактом, что Ubuntu не является отечественной операционной системой.

Кроме этого, риски связаны с тем, что исходные коды программных пакетов SQUID, SQUIDGUARD и SARG, необходимые для сборки такого Интернет-шлюза, опубликованы на зарубежных Интернет ресурсах и могут содержать вредоносный код. В этой статье мы предложим альтернативное решение для небольшого офиса, основанное на применении отечественного программного обеспечения, эквивалентного операционной системе Ubuntu и программным пакетам SQUID, SQUIDGUARD и SARG.

Следует отметить, что существуют относительно недорогие отечественные решения для Интернет-шлюза в небольшом офисе, полностью эквивалентные связке SQUID, SQUIDGUARD и SARG. Например, Kaspersky Web Traffic Security [6] и Solar webProxy [7], но в рамках поставленной в статье задачи мы не будем их рассматривать.

В первую очередь определимся с операционной системой. Для неопытных администраторов большое значение имеет наличие графических интерфейсов управления и универсальность, максимальная схожесть по функционалу с операционными системами Microsoft Windows. Под универсальностью понимается возможность установки на все средства вычислительной техники в офисе.

Для выбора отечественной операционной системы воспользуемся сервисом на Интернет-портале Минцифры России, предназначенным для поиска российских аналогов зарубежного программного обеспечения – «Реестр программного обеспечения» [8]. На запрос по поиску аналогов Microsoft Windows портал формирует список из десяти операционных систем, распределение количества которых по годам регистрации за период с 2016 по 2022 годы показано на рисунке 1. Из рисунка 1 следует, что активная разработка отечественных операционных систем началась после 2014 года и к 2016 году появились первые шесть программных продуктов.

Далее разработчики усовершенствовали и адаптировали отечественные операционные системы к профильным задачам: специального назначения, общего назначения, универсальные, мобильные и др. Относительно короткий срок, за который были созданы отечественные операционные системы, в первую очередь связан с тем, что их создавали на базе существующих операционных систем из семейства Linux. В частности, операционная система ALT Linux, изначально основанная на дистрибутиве Mandrake, была доработана ООО «Базальт СПО» до самостоятельной операционной системы со своим собственным репозиторием программ «Сизиф», который включает как популярные Linux приложения, так и программы, адаптированные специально для

ALT Linux. Другой пример – разработанная ООО «РусБИТех-Астра» операционная система Astra Linux, которая считается «официально признанным» дериватом дистрибутива Debian.

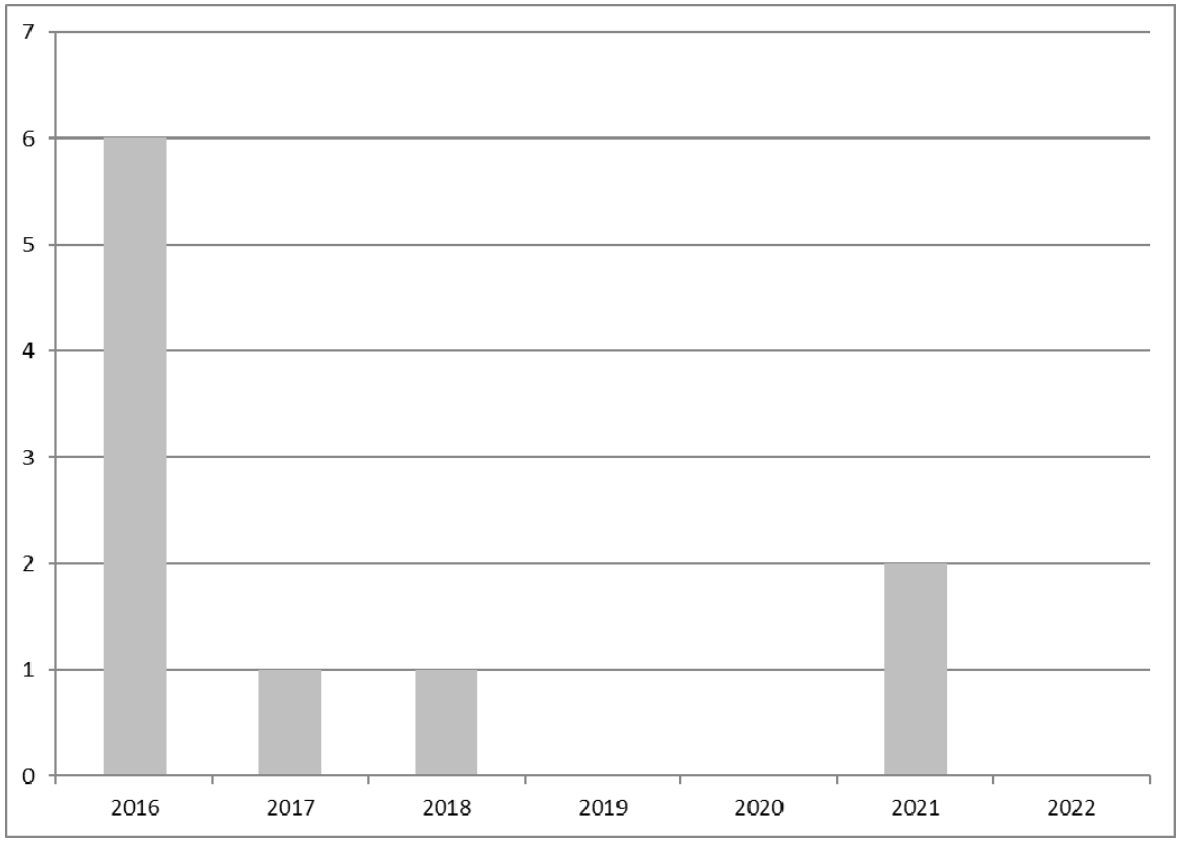

Рис. 1. Распределение количества отечественных операционных систем, являющихся аналогом Microsoft Windows, зарегистрированных в реестре в 2016–2022 годах

Fig. 1. Distribution of the number of domestic operating systems that are analogue of Microsoft Windows registered in the registry in 2016–2022

Лидерами в разработке отечественных операционных систем являются ООО «РусБИТех-Астра» и ООО «Базальт СПО» (рис. 2). В 2022 году ООО «РусБИТех-Астра», разработавшее 40% отечественных операционных систем, заняло около 70% рынка российских операционных систем – более полутора миллионов инсталляций.

Таким образом, операционную систему целесообразно выбрать из семейств Astra Linux или ALT Linux, разработанных РусБИТех-Астра» и ООО «Базальт СПО» соответственно. Не вдаваясь в рассмотрение организационно-правовых вопросов применения этих операционных систем в небольших офисах, следует отметить, что у семейств Astra Linux и ALT Linux есть версии, сертифицированные ФСТЭК России [9]. К сожалению, свободно распространяемых версий вышеуказанных операционных систем не существует. На наш взгляд, в целях популяризации отечественных операционных систем разработчикам стоит рассмотреть вопрос о создании свободно распространяемых дистрибутивов, возможно, с ограниченным функционалом.

Кроме этого, для форсирования перехода на отечественные операционные системы требуется организовать обучение (самообучение) системных администраторов. В этом направлении есть небольшие успехи, в частности, созданы информационные порталы для начинающих администраторов.

Далее рассмотрим, какими отечественными программными продуктами можно заменить программные пакеты SQUID, SQUIDGUARD и SARG:

1. Программный пакет, кеширующий прокси-сервер SQUID, входит в состав официальных дистрибутивов Astra Linux и ALT Linux и не требует импортозамещения. Тем не менее, следует отметить, что исходники SQUID находятся на зарубежных сайтах, что не позволяет делать его особые сборки с включением дополнительных библиотек. Например, невозможно собрать SQUID со специальным режимом sslbump, так как необходимо подключить криптографические библиотеки OpenSSL или LibreSSL. Без специального режима SSLBump невозможно осуществлять полноценное журналирование, контентную фильтрацию и др. в отношении HTTPS-трафика, а так же применять потоковые антивирусы. Таким образом, применение SQUID возможно, но существенно ограничено.

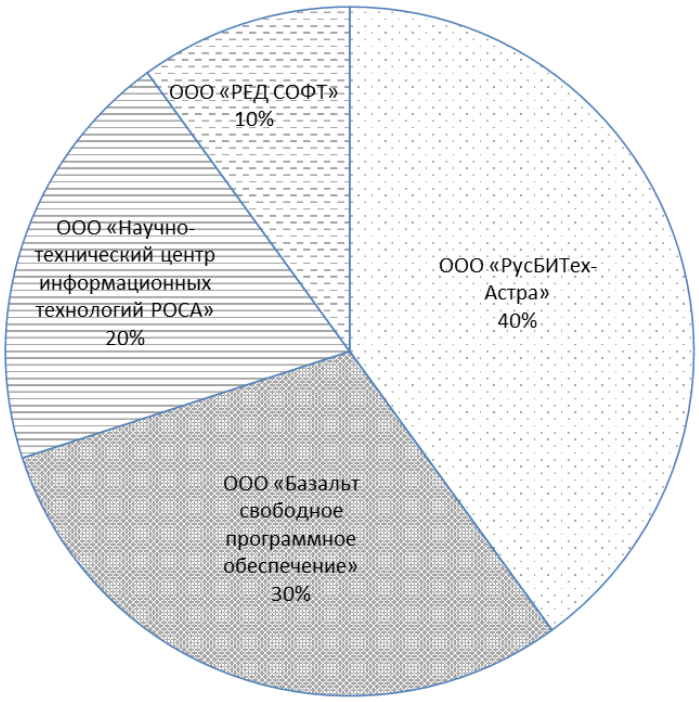

Рис. 2. Количество разработанных операционных систем

Fig. 2. Number of the developed operating systems

2. Следует пояснить, что SQUIDGUARD это внешний редиректор, который не является частью пакета SQUID. Пакет SQUIDGUARD позволяет обеспечить более эффективную фильтрацию Интернет-трафика, чем встроенный функционал SQUID. Эквивалент программного пакета SQUIDGUARD в реестре не представлен [8]. В Интернете можно найти примеры скриптов для написания собственного редиректора. Однако для начинающего администратора написание собственного редиректора – невыполнимая задача. Еще одной серьезной проблемой является получение базы нежелательных сайтов из доверенного источника. Например, для SQUIDGUARD такую базу можно скачать с официального сайта проекта.

3. Как и в случае SQUIDGUARD, эквивалент программного пакета SARG (Squid Analysis Report Generator) в реестре не представлен [8]. Существует несколько десятков зарубежных эквивалентов пакета SARG, при этом известен только один отечественный эквивалент – пакет free-sa [10]. Как ни странно, но в отличие от зарубежных разработчиков, ответственные разработчики не уделили должного внимания созданию анализаторов журналов для одного из самых популярных прокси-серверов в России – SQUID. Программное обеспечение free-sa не включено в реестр [8], так как последняя его версия вышла в ноябре 2013 года. Это программное обеспечение может быть использовано

только после оценки всех сопутствующих рисков.

Далее рассмотрим отдельные вопросы сетевой защиты.

В наших статьях [4, 5] не рассматривались вопросы защиты операционной системы, в которой установлен прокси-сервер. Предполагалось, что сервер расположен за межсетевым экраном или в демилитаризованной зоне. С учетом высокой стоимости межсетевых экранов целесообразно рассмотреть функционал по фильтрации трафика, предоставляемый самими операционными системами. Как и все линуксоподобные операционные системы, Astra Linux и ALT Linux имеют встроенную утилиту iptables, которая является стандартным интерфейсом управления работой межсетевого экрана (брандмауэра) Netfilte. Обычно, когда говорят Netfilter, то имеют в виду только элементы межсетевого экрана, являющиеся частью ядра. Все, что не относится к ядру, а именно: таблицы, цепочки, правила, – называют iptables. Поэтому правильно называть всю систему – netfilter/iptables. В версию Astra Linux Special Edition добавлен дополнительный модуль тестирования astralabel, средствами которого реализовано расширение функционала netfilter/iptables для работы с классификационными метками [11].

С учетом этого у начинающего администратора, привыкшего работать с графическим интерфейсом Microsoft Windows, администрирование в командной строке ожидаемо приведет к ошибкам, целесообразно использовать графический интерфейс GUFW для iptables – Uncomplicated Firewall (UFW). UFW входит в официальные дистрибутивы рассматриваемых операционных систем и имеет высокую надежность.

Согласно базе данных ФСТЭК России, уязвимость утилиты межсетевого экрана UFW операционной системы Astra Linux была выявлена и устранена всего однажды в 2019 году. UFW – удобный инструмент для неопытных администраторов, позволяющий контролировать свой сетевой трафик и защищать свою систему, реализуя правила или действия с простым синтаксисом.

Отдельного внимания заслуживают следующие опции и инструменты GUFW/UFW, важные для начинающих администраторов:

1. Опция – dry-run для тестирования правил без их фактического применения, что важно для начинающего администратора;

2. Графический интерфейс GUFW позволяет применить три предустановленных профиля безопасности. Указанные профили интуитивно понятны большинству администраторов и пользователей Microsoft Windows: «Дом», «Общественное место» и «Офис». Разумеется, профили безопасности имеют соответствующие наименованию предварительно настроенные правила фильтрации. Как и в Microsoft Windows, самый строгий профиль – «Общественное место», самый слабый – «Дом»;

3. Вкладка «Отчет», которая предоставляет информацию о программах и процессах, инициирующих сетевые соединения, что позволяет выявлять приложения и процессы, трафик которых следует блокировать. Подобный функционал есть у большинства персональных файерволов, входящих в состав антивирусных средств защиты.

В заключение можно сказать, что для полноценного импортозамещения в рамках рассматриваемой задачи Интернет-шлюзов в небольших офисах в России необходимо:

– создать отечественные проекты, эквивалентные проектам SQUIDGUARD и SARG;

– обеспечить публикацию общедоступных баз нежелательных сайтов, ключевых слов и IP адресов (включая GeoIP), необходимых для осуществления фильтрации Интернет-трафика (в том числе контентной фильтрации);

– создать свободно распространяемые дистрибутивы отечественных операционных систем Astra Linux и ALT Linux;

– обеспечить масштабное обучение (переобучение) работе с отечественными

операционными системами для системных администраторов и пользователей.

По состоянию на сегодняшний день рекомендуем применять в качестве Интернет-шлюза в небольшом офисе прокси-сервер SQUID, установленный на операционной системе Astra Linux или ALT Linux, дополнительно защищенный средствами netfilter/iptables под управлением интерфейса UFW.

Примечания

1. Киздермишов А.А. Снижение риска возникновения предпосылок угроз информационной безопасности, связанных с ошибочными действиями и неверно принятыми решениями специалистов ответственных за защиту информации // Вестник Майкопского государственного технологического университета. 2009. № 3. С. 111–115.

2. Киздермишов А.А., Киздермишова С.Х. Интернет-шлюз для небольшого офиса: SQUID, SQUIDGUARD и SARG // Цифровая экономика: новая реальность: сб. ст. по итогам Междунар. науч.-практ. видеоконф., посвященной 25-летию ВУЗа. 2018. С. 42–45.

3. Киздермишов А.А., Киздермишова С.Х. Установка и настройка специального режима Squid (ssl-bump) на Ubuntu 12.04 TLS // Вестник Адыгейского государственного университета. Сер.: Естественно-математические и технические науки. 2017. Вып. 4 (211). С. 154–159. URL: http://vestnik.adygnet.ru

4. Киздермишов А.А., Киздермишова С.Х. Установка и настройка редиректора для Squid (ssl-bump) // Вестник Адыгейского государственного университета. Сер. Естественно-математические и технические науки. 2018. Вып. 1 (216). С. 154–159. URL: http://vestnik.adygnet.ru

5. Киздермишов А.А., Киздермишова С.Х. Установка и настройка SQUID ANALYSIS REPORT GENERATOR // Вестник Адыгейского государственного университета. Сер. Естественно-математические и технические науки. 2018. Вып. 3 (226). С. 135–141. URL: http://vestnik.adygnet.ru

6. Kaspersky Web Traffic Security. URL: https://www.kaspersky.ru/small-to-medium-business-security/proxy-web-traffic

7. Solar webProxy. URL: https://rt-solar.ru/products/solar_webproxy/

8. Реестр программного обеспечения. URL: https://reestr.digital.gov.ru/import-substitution/?query=Windows

9. Государственный реестр сертифицированных средств защиты информации. URL: https://fstec.ru

10. SourceForge. URL: https://sourceforge.net/projects/free-sa/files

11. Справочный центр AstraLinux. URL: https://wiki.astralinux.ru

References

1. Kizdermishov A.A. Risk reduction of information security threats prerequisites associated with erroneous actions and wrong decisions of specialists responsible for information security // The Bulletin of the Maikop State University of Technology. 2009. No. 3. P. 111–115.

2. Kizdermishov A.A., Kizdermishova S.H. Internet gateway for a small office: SQUID, SQUIDGUARD and SARG // Digital Economy: New reality: a collection of articles based on the results of an international scientific and practical videoconference dedicated to the 25th anniversary of the University. 2018. P. 42–45.

3. Kizdermishov A.A., Kizdermishova S.H. Installing and configuring a special Squid mode (ssl-bump) on Ubuntu 12.04 TLS // The Bulletin of the Adyghe State University. Ser.: Natural-Mathematical and Technical Sciences. 2017. Iss. 4 (211). P. 154–159. URL: http://vestnik.adygnet.ru

4 Kizdermishov A.A., Kizdermishova S.H. Installation and configuration of a redirector for Squid (ssl-bump) // The Bulletin of the Adyghe State University. Ser.: Natural-Mathematical and Technical Sciences. 2018. Iss. 1 (216). P. 154–159. URL: http://vestnik.adygnet.ru

5. Kizdermishov A.A., Kizdermishova S.H. Installation and configuring the Squid Analysis Report Generator // The Bulletin of the Adyghe State University. Ser.: Natural-Mathematical and Technical Sciences. 2018. Iss. 3 (226). P. 135–141. URL: http://vestnik.adygnet.ru

6. Kaspersky Web Traffic Security. URL: https://www.kaspersky.ru/small-to-medium-business-security/proxy-web-traffic

7. Solar webProxy. URL: https://rt-solar.ru/ products/ solar_webproxy/

8. Software registry. URL: https://reestr.digital.gov.ru/ import-substitution/?query =Windows
9. The State Register of certified means of information protection. URL: https://fstec.ru
10. SourceForge. URL: https://sourceforge.net/projects/free-sa/files
11. Astra Linux Help Center. URL: https://wiki.astralinux.ru

Авторы заявляют об отсутствии конфликта интересов.

The authors declare no conflicts of interests.

Статья поступила в редакцию 13.01.2023; *одобрена после рецензирования 04.02.2023*; *принята к публикации 05.02.2023*.

The article was submitted 13.01.2023; *approved after reviewing 04.02.2023*; *accepted for publication 05.02.2023*.