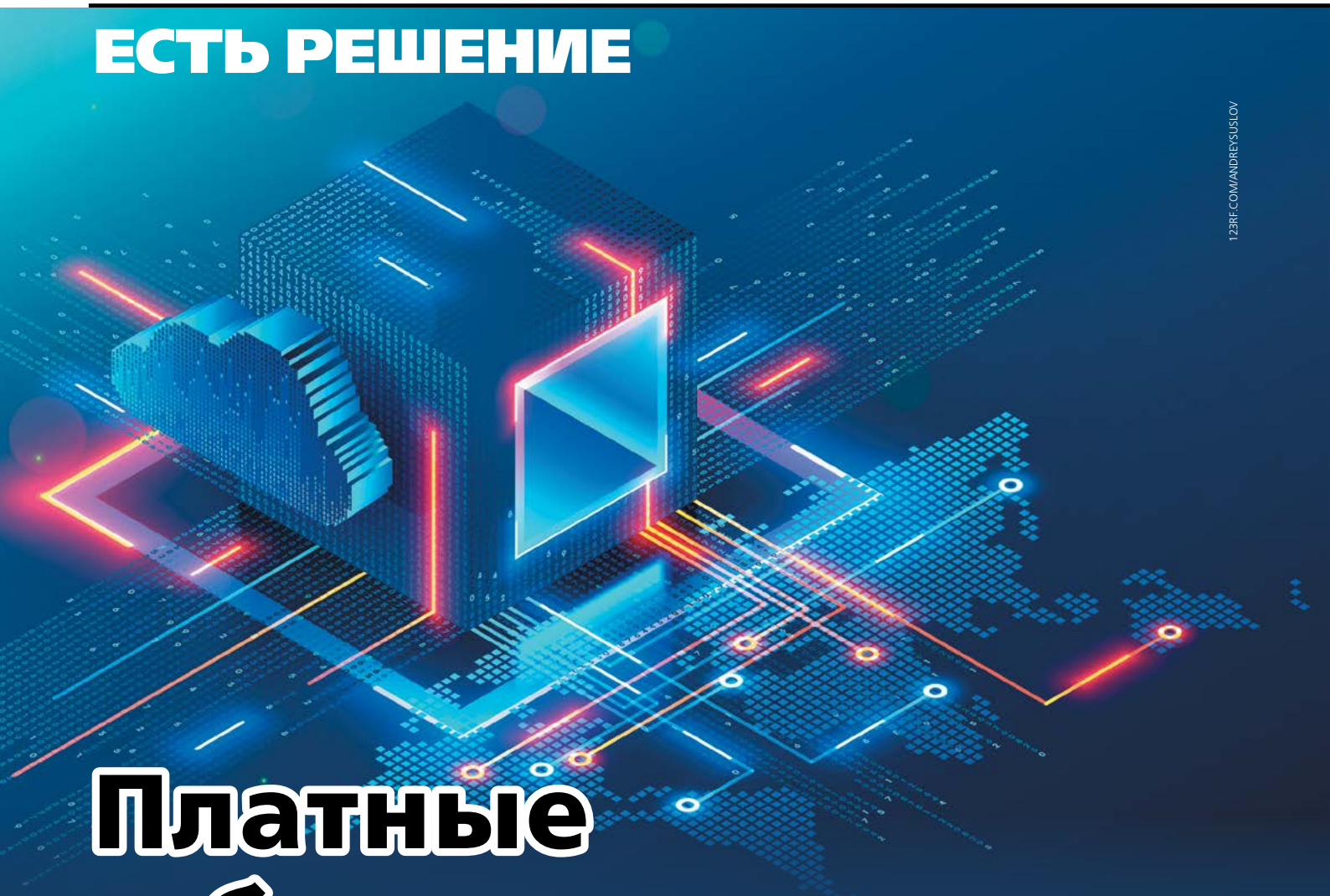
ЕСТЬ РЕШЕНИЕ



123RF.COM/ANDREYSUSLOV

Платные и бесплатные межсетевые экраны и средства обнаружения атак

В начале апреля текущего года Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации направило письмо (от 01.04.2022 года № МШ-П8-1-070-14732), в котором напомнило о необходимости активного импортозамещения цифровых решений и продуктов в связи с текущей геополитической обстановкой.

ДМИТРИЙ ВЕКШИН,
преподаватель кафедры сетевой безопасности Учебного центра «Информзащита»

В письме указывается единый реестр российских программ (reestr.digital.gov.ru) и перечень (catalog.arppsoft.ru/replacement) отечественных программных продуктов, который ведется ассоциацией разработчиков программных продуктов «Отечественный софт».

Еще к письму прилагается перечень некоторых цифровых решений иностранных компаний, деятельность которых полностью или частично ограничена в России, и рекомендованные решения для их замены.

В такой ситуации производители программного обеспечения получили гарантированный рынок сбыта и в несколько раз подняли цены.

В своей я статье предлагаю обратить внимание на платные и бесплатные решения в области сетевой безопасности на базе курсов, которые читаю сам в учебном центре «Информзащита». В частности, на межсетевые экраны и средства выявления уязвимостей.

Межсетевой экран блокирует или разрешает прохождение информации по сети, исходя из правил, которые ему определяет системный администратор. Чаще всего современные межсетевые экраны располагаются на границе двух сегментов сети: внутренней и внешней. С учетом последних тенденций в сторону удаленной работы эта граница становится все более и более размытой, и сейчас на межсетевой экран возлагаются функции создания виртуальных частных сетей, в которых информация зашифрована и аутентифицирована.

Аппаратно-программный комплекс шифрования «Континент», например, позволяет реализовать функции по ограничению нежелательных соединений и обеспечить конфиденциальность данных, передаваемых по открытым каналам связи. Он создает виртуальную частную сеть с помощью собственной разработки, сертифицированной ФСТЭК и ФСБ России.

Межсетевые экраны UserGate разработаны на базе специально созданной операционной системы, а также на специально спроектированных аппаратных устройствах, позволяющих обеспечить высокую эффективность и скорость обработки данных. Кроме того, UserGate NGFW можно использовать в качестве виртуального межсетевого экрана на облачной платформе, где вычислительные ресурсы предоставляются в аренду, например на «Яндекс.Облаке».

АПКШ «Континент» использует ядро FreeBSD, а UserGate – предположительно, ядро Linux. В Linux для управления передаваемыми по сети данными почти 25 лет используется iptables, а во FreeBSD – ipfw. И то, и другое распространяется бесплатно и имеет очень богатый функционал. Автоматизировать настройку виртуальной частной сети можно с помощью, например, Algo VPN. Это набор сценариев, который поддерживает все последние протоколы, включая OpenVPN и WireGuard. Платные решения, конечно, более дружественны к пользователю и к тому же предлагают комплексное решение. Но, на мой взгляд, опытный системный администратор вполне способен, используя бесплатные решения, настроить защиту сети в определенной степени.

Для выявления уязвимостей разумно использовать «XSpider», который много лет успешно разрабатывает «Positive Technologies». В обозримом будущем планируется заменить «XSpider» на «MaxPatrol VM». Это весьма комплексные решения и противопоставить им придется несколько наборов бесплатного программного обеспечения: OpenVAS, Metasploit Framework, OpenSCAP, w3af и другие. Дополнительная сложность заключается в адресном применении этих наборов: в одной области, например, для анализа кода сайта эффективны одни инструменты, но они же бесполезны при анализе защищенности внутренней сети. Здесь от системного администратора потребуется квалификация и опыт. ●

В текущей ситуации производители программного обеспечения получили гарантированный рынок сбыта и в несколько раз подняли цены