УДК 004.421: 339.5

ВОЗМОЖНОСТИ, ПЕРСПЕКТИВЫ И ПРОБЛЕМЫ ВИРТУАЛИЗАЦИИ В ФЕДЕРАЛЬНОЙ ТАМОЖЕННОЙ СЛУЖБЕ РОССИИ

Афонин Д.Н.
Санкт-Петербургский имени В.Б.Бобкова филиал Российской таможенной академии

OPPORTUNITIES, PROSPECTS AND PROBLEMS OF VIRTUALIZATION IN THE FEDERAL CUSTOMS SERVICE OF RUSSIA

Afonin D.N.
St. Petersburg named after V.B. Bobkov branch of the Russian Customs Academy

Аннотация
В статье рассмотрены основные вопросы применения виртуализации и облачных технологий, в таможенных органах России. Большое внимание уделено обеспечению безопасности информации таможенных органов, обрабатываемой с использованием технологий виртуализации.

Ключевые слова: виртуализация, облачные технологии, Федеральная таможенная служба России, информационная безопасность.

Abstract
The article discusses the main issues of the application of virtualization and cloud technologies in the customs authorities of Russia. Much attention is paid to ensuring the security of customs information processed using virtualization technologies.

Keywords: virtualization, cloud technologies, Federal Customs Service of Russia, information security.

Технологии виртуализации являются неотъемлемой частью современной IT-инфраструктуры, так как они позволяют значительно ускорить внедрение новых и оптимизировать затраты на поддержку существующих информационных систем и услуг. Федеральная таможенная служба России, являющаяся одним из крупнейших среди федеральных органов исполнительной власти пользователей серверных операционных систем, систем управления базами данных, активно внедряет средства управления «облачной» инфраструктурой и виртуализацией.

В феврале 2020 года Советом Федерации Федерального Собрания Российской было рекомендовано Федеральной таможенной службе России создание нового Главного центра обработки данных ФТС России, предназначенного для реализации современных информационных технологий, обеспечивающих применение технологии «облачных вычислений» и централизацию приложений и баз данных, используемых таможенными органами России [1].

Применение «облачных технологий» позволит существенно снизить затраты на техническое обслуживание, устранение неполадок, обеспечить бесперебойную работу ЕАИС таможенных органов России и тем самым существенно повысить эффективность ее работы.

Применение облачных хранилищ (как основных, так и для резервного копирования) в настоящее время становится повсеместным явлением, поскольку современные как проводные, так и беспроводные сети обеспечивают скорость передачи данных свыше 1 Гбит/с. Данная функция реализована в Ethernet, 802.11ac Wi-Fi и тестируемом во многих странах стандарте высокоскоростных сетей 5G. Концепция виртуализации сегодня активно внедряется в сетевых технологиях. Огромной популярностью в мире пользуется «сеть как услуга» (NaaS). Внедрение виртуализации сетевых функций (NFV) осуществляется всеми операторами и особенно в области мобильной связи, позволяя им не только увеличить пропускную способность каналов связи, но и существенно расширить спектр предоставляемых услуг. Всё большее количество государственных и частных организаций ис-

пользуют NFV самостоятельно и в гибридных сетях, а широко применяемые VLAN (802.1Q) и виртуальные частные сети (VPN) практически повсеместно используют современные технологии виртуализации.

Масштабное внедрение технологий виртуализации в деятельность Федеральной таможенной службы приведет к существенному перераспределению и сокращению расходов на IT-технологии. Технологии современных микропроцессоров, увеличение производительности локальных сетей и сетей WAN (в т.ч. и беспроводных) обеспечивают возможность виртуализации практически каждого элемента IT-индустрии и при необходимости реализации его как масштабируемого облачного сервиса.

В России с 30.08.2019 по 30.12.2020 проводится эксперимент по переводу IT-систем и ресурсов федеральных органов исполнительной власти и государственных внебюджетных фондов в государственную единую облачную платформу. В рамках эксперимента осуществляется обеспечение указанных структур автоматизированными рабочими местами и программным обеспечением [2]. Одним из участников данного эксперимента является Федеральная таможенная служба России. ФГБУ «Научно-исследовательский институт «Восход» определен Правительством Российской Федерации [3] единственным исполнителем осуществляемых Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации в 2019 и 2020 годах закупок – товаров, работ, услуг, связанных с переводом информационных систем и информационных ресурсов ФТС России в государственную единую облачную платформу, а также с арендой вычислительной инфраструктуры и организацией связи, которые необходимы для проведения эксперимента, созданием постоянно действующих стендов, используемых для тестирования отдельных технических решений и автоматизированных рабочих мест должностных лиц таможенных органов.

Актуальной проблемой внедрения систем виртуализации в таможенных органах России является обеспечение их безопасности. С 01.06.2017 введен в действие ГОСТ Р 56938-2016 [4], разработанный ФАУ «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю». Данный ГОСТ определяет виртуальную инфраструктуру, как композицию «иерархически взаимосвязанных групп виртуальных устройств обработки, хранения и/или передачи данных, а также группы необходимых для их работы аппаратных и/или программных средств», акцентирует внимание на том, что использование технологий виртуализации создает предпосылки для появления угроз безопасности, не характерных для информационных систем, построенных без использования технологий виртуализации и выделяет основные объекты, требующие защиты при применении технологий виртуализации. К таким объектам относятся:

– средства создания и управления виртуальной инфраструктурой (гипервизор I типа, гипервизор II типа, гипервизор системы хранения данных, консоль управления виртуальной инфраструктурой и др.);

– виртуальные вычислительные системы (виртуальные машины, виртуальные сервера и др.);

– виртуальные системы хранения данных;

– виртуальные каналы передачи данных;

– отдельные виртуальные устройства обработки, хранения и передачи данных (виртуальные процессоры, виртуальные диски, виртуальную память, виртуальное активное и пассивное сетевое оборудование и др.);

– виртуальные средства защиты информации (ЗИ) и средства ЗИ, предназначенные для использования в среде виртуализации;

– периметр виртуальной инфраструктуры (задействованные при реализации технологий виртуализации центральные процессоры и их ядра, адресное пространство памяти, сетевые интерфейсы, порты подключения внешних устройств и др.).

Согласно ГОСТ Р 56938-2016 помимо существующих угроз информационной безопасности, ранее определенных в ГОСТ Р ИСО/МЭК 27001-2006 [5] внедрение технологий виртуализации дополнительно может привести к возникновению еще восемнадцати угроз:

– угрозы атаки на активное и/или пассивное виртуальное и/или физическое сетевое оборудование из физической и/или виртуальной сети;

– угрозы атаки на виртуальные каналы передачи;

– угрозы атаки на гипервизор из виртуальной машины и/или физической сети;

– угрозы атаки на защищаемые виртуальные устройства из виртуальной и/или физической сети;

– угрозы атаки на защищаемые виртуальные машины из виртуальной и/или физической сети;

– угрозы атаки на защищаемые виртуальные машины из виртуальной и/или физической сети;(здесь в найденных опубликованных экземплярах ГОСТа идёт задублированный пункт, возможно, допустили ошибку при наборе текста)

– угрозы атаки на систему хранения данных из виртуальной и/или физической сети;

– угрозы выхода процесса за пределы виртуальной машины;

– угрозы несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение;

– угрозы нарушения изоляции пользовательских данных внутри виртуальной машины;

– угрозы нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия;

– угрозы перехвата управления гипервизором;

– угрозы перехвата управления средой виртуализации;

– угрозы неконтролируемого роста числа виртуальных машин;

– угрозы неконтролируемого роста числа зарезервированных вычислительных ресурсов;

– угрозы нарушения технологии обработки информации путем несанкционированного внесения изменений в образы виртуальных машин;

– угрозы несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации;

– угрозы ошибок обновления гипервизора.

В зависимости от объекта защиты информации ГОСТ Р 56938-2016 предлагает шесть групп мер ее защиты:

– защита средств создания и управления виртуальной инфраструктурой;

– защита виртуальных вычислительных систем;

– защита виртуальных систем хранения данных;

– защита виртуальных каналов передачи данных;

– защита отдельных виртуальных устройств обработки, хранения и передачи данных;

– защита виртуальных средств защиты информации и средств защиты информации, предназначенных для использования в среде виртуализации.

Суммарная информация об угрозах и мерах защиты информации, обрабатываемой с использованием технологий виртуализации представлена в виде таблицы в приложении к ГОСТ Р 56938-2016.

Обращает на себя внимание появление новых мер защиты информации, таких, как шифрование передаваемых файлов-образов виртуальных машин, которые в настоящее время еще только разрабатываются. С другой стороны, в ГОСТ Р 56938-2016 не рассматриваются угрозы, относящиеся к снимкам виртуальных машин (snapshots), которые выделены в отдельный объект защиты National Institute of Standards and Technology США [6].

Таким образом, можно выделить следующие этапы выбора мер защиты информации таможенных органов, обрабатываемой с использованием технологий виртуализации:

– определение базового набора мер защиты;

– адаптация базового набора мер защиты;

– уточнение адаптированного базового набора мер защиты;

– дополнение уточненного адаптированного базового набора мер защиты.

Список литературы

1. Постановление СФ ФС РФ от 12.02.2020 № 45-СФ «О стратегических направлениях совершенствования таможенного администрирования в Российской Федерации»

2. Постановление Правительства РФ от 28.08.2019 № 1114 «О проведении эксперимента по переводу информационных систем и информационных ресурсов федеральных органов исполнительной власти и государственных внебюджетных фондов в государственную единую облачную платформу, а также по обеспечению федеральных органов исполнительной власти и государственных внебюджетных фондов автоматизированными рабочими местами и программным обеспечением» (вместе с «Положением о проведении экспери-

мента по переводу информационных систем и информационных ресурсов федеральных органов исполнительной власти и государственных внебюджетных фондов в государственную единую облачную платформу, а также по обеспечению федеральных органов исполнительной власти и государственных внебюджетных фондов автоматизированными рабочими местами и программным обеспечением»).

3. Распоряжение Правительства РФ от 11.11.2019 № 2667-р «Об определении публичного акционерного общества «Ростелеком» и ФГБУ «Научно-исследовательский институт «Восход» единственными исполнителями осуществляемых Минкомсвязью России в 2019 и 2020 годах закупок товаров, работ, услуг, связанных с переводом информационных систем и информационных ресурсов»

4. ГОСТ Р 56938-2016 «Защита информации. Защита информации при использовании технологий виртуализации. Общие положения»

5. ГОСТ Р ИСО/МЭК 27001-2006. «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности требования»

6. Scarfone K., Souppaya M., Hoffman P. NIST Special Publication 800-125. Guide to Security for Full Virtualization Technologies. Recommendations of the National Institute of Standards and Technology. Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930. 2011. 31 p.

Поступила в редакцию 23.03.2020

Сведения об авторе:

Афонин Дмитрий Николаевич – профессор кафедры таможенного дела Санкт-Петербургского имени В.Б.Бобкова филиала Российской таможенной академии, доктор медицинских наук, доцент, e-mail: dnafonin@gmail.com

Электронный научно-практический журнал "**Бюллетень инновационных технологий**"
(**ISSN 2520-2839**) является сетевым средством массовой информации
регистрационный номер **Эл № ФС77-73203**
по вопросам публикации в Журнале обращайтесь по адресу bitjournal@yandex.ru