12. *Sentsova A.Yu., Mashkina I.V., Chayka V.Yu.* Sredstvo provedeniya ekspertnogo audita informatsionnoy bezopasnosti [Tool expert information security audit], *Svidetel'stvo o gosudarstvennoy registratsii programmy dlya EVM № 2014616279. 2014* [The certificate of state registration of the computer program No. 2014616279. 2014].

Статью рекомендовал к опубликованию д.т.н., профессор О.Б. Макаревич.

Машкина Ирина Владимировна – Уфимский государственный авиационный технический университет; e-mail: mashkina_vtzi@gmail.com; 450000, Республика Башкортостан, г. Уфа, ул. К. Маркса, 12; тел.: +79279277089; кафедра вычислительной техники и защиты информации; д.т.н.; профессор.

Сенцова Алина Юрьевна – e-mail: sentsova.alina@yandex.ru; тел.: +79174568307; аспирантка.

Mashkina Irina Vladimirovna – The Ufa State Aviation Technical University; e-mail: mashkina_vtzi@gmail.com; 12, K. Marx's street, Ufa, 450000, Russia; phone: +79279277089; chair of computer facilities and information protection; dr. of eng. sc.; professor.

Sentsova Alina Uryevna – e-mail: sentsova.alina@yandex.ru; phone: +79174568307; postgraduate student.

УДК 004.9

К.В. Курносов, В.В. Селифанов

ТРЕБОВАНИЯ К СИСТЕМЕ ЗАЩИТЫ ИНФОРМАЦИИ ДЛЯ ВИРТУАЛЬНОЙ ИНФРАСТРУКТУРЫ

Ввиду отсутствия требований для оценки систем защиты информации для технологий, реализующих виртуальные инфраструктуры, была поставлена цель по их разработке. В соответствии с руководящими и методическими документами в области технической защиты информации была разработана модель инфраструктуры, построенной с применением технологии виртуализации, в которой содержится информация ограниченного доступа, не содержащая сведений составляющих государственную тайну. Были определены виды потенциальных нарушителей безопасности, выделены актуальные угрозы, и выработан набор требований для оценки безопасности таких инфраструктур. При решении этих задач проводился анализ отечественной литературы по данному вопросу, нормативной и методической документации в области защиты информации, моделирование информационной инфраструктуры, угроз и нарушителя безопасности с учетом специфики технологий виртуализации. Объектом исследования в данной статье выступает виртуальная инфраструктура, включая ее компоненты. Предметом исследования являются требования и методика для оценки безопасности системы защиты информации для виртуальных инфраструктур.

Виртуализация; виртуальная инфраструктура; виртуальная машина; гипервизор; информационная безопасность; требования информационной безопасности.

K.V. Kurnosov, V.V. Selifanov

INFORMATION PROTECTION SYSTEM REQUIREMENTS FOR VIRTUAL INFRASTRUCTURE

Due to the lack of requirements for the evaluation of information security systems technology for implementing virtual infrastructure, the goal was set for their development. In accordance with the guiding and methodological documents in the field of technical protection of information, a model was developed infrastructure, built with the use of virtualization technologies, which contains information of restricted access, not containing information constituting state secrets. Were defined the types of potential offenders security, the urgent threats, and develop a set of requirements for safety assessment of such infrastructure. In solving these problems were analyzed na-

tional literature on the subject, normative and methodical documents in the field of information security, information infrastructure modeling, security threats and offender-specific virtualization technologies. The object of study in this paper advocates the virtual infrastructure, including its components. The subject of the study are the requirements and methodology for evaluation of safety information protection system for virtual infrastructures.

Virtualization; virtual infrastructure; virtual machine; hypervisor; information security; requirements for information security.

Обзор технологии виртуализации. Специфика современного рынка производства и услуг приводит к необходимости обработки огромных информационных потоков в реальном времени с повышенными требованиями к безопасности и надежности. Для продуктивной работы организаций требуется все больше и больше сервисов, предоставляемых как для клиентов, так и для собственных сотрудников. Запуск разнообразных служб и приложений на одном сервере ведет к увеличению рисков, связанных с выходом его из строя.

Для обеспечения минимизации таких рисков и изоляции приложений друг от друга очевидным представляется решение использовать для каждого сервиса отдельно выделенный сервер. Такой подход приводит к быстрому росту сетей и инженерных коммуникаций. Следствием чего непременно становится неконтролируемый рост расходов на содержание информационной инфраструктуры, а также сложности с ее управлением и масштабируемостью.

Виртуализация является одной из ключевых технологий, позволяющей решить большинство этих проблем и перейти от экстенсивного развития инфраструктуры к интенсивному.

В проекте ГОСТа «Защита информации. Защита информации при использовании технологий виртуализации. Общие положения» [1] под виртуальной инфраструктурой (ВИ) подразумевается сформированная совокупность физических серверов, виртуальных ресурсов и компонентов виртуальной платформы (ВП), развернутых на физических серверах, а также каналы связи.

Технология виртуализации несет такие преимущества, как оптимальное использование вычислительных и материальных ресурсов, масштабируемость инфраструктуры и увеличение уровня отказоустойчивости.

Конечно, данная технология несовершенна и обладает своими недостатками. Технологии виртуализации порождают новые специфические угрозы. Примерами таковых могут являться угрозы гипервизору, угрозы образам виртуальной машины (ВМ) и виртуальным сетевым инфраструктурам.

Согласно статистике «Лаборатории Касперского» [2], 59 % опрошенных российских компаний с локальными сетями от 100 компьютеров и выше, уже внедрили или планируют внедрить виртуализацию серверов.

По данным исследований Cisco Systems, Inc [3], в качестве основных препятствий для использования технологий виртуализации в информационных системах (ИС) чаще других упоминаются вопросы безопасности (23 % случаев). Таким образом, можно сделать вывод, что вопросы виртуализации и обеспечения ее безопасности на сегодняшний день довольно актуальны.

Анализ существующих информационных технологий, реализующих ВИ, показал, что для обеспечения их безопасности необходимо построение систем защиты информации, способных устранять специфичные угрозы, возникающие при использовании технологий виртуализации.

Модель виртуальной инфраструктуры. Когда виртуализация используется для построения ИС, в которых содержится информация ограниченного доступа, необходимо, чтобы средства защиты информации прошли процедуру оценку соответствия. Документы, в которых определены меры по защите среды виртуализации, – упомянутый выше проект ГОСТа [1] и Приказы ФСТЭК России №17 [6] и №21 [7].

На основе указанных выше документов, описания архитектуры и выделенных объектов защиты, при использовании технологии виртуализации, существующих в этих документах, была разработана модель ВИ, включающая ее основные компоненты (рис. 1).

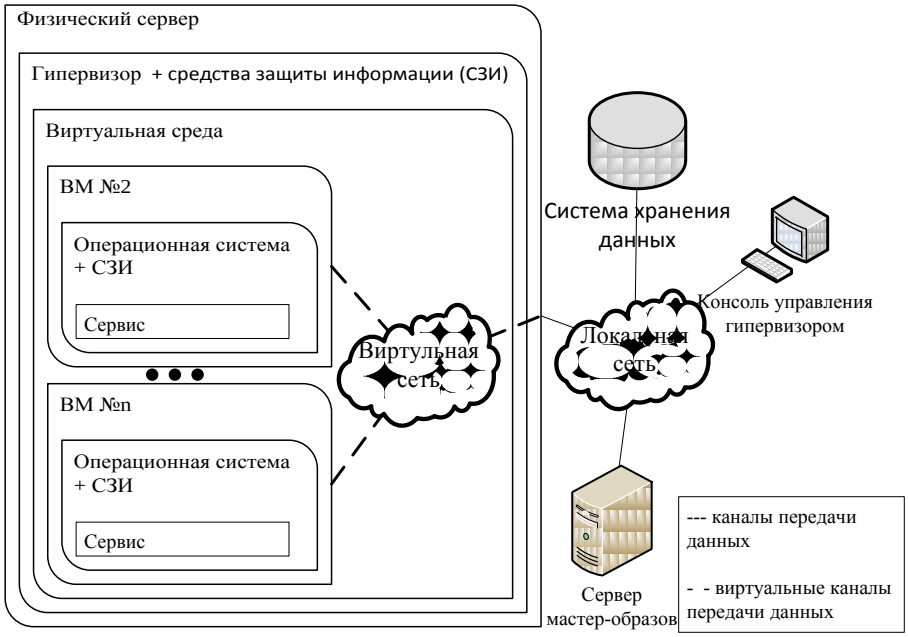

Рис. 1. Модель виртуальной инфраструктуры

Нарушитель и угрозы безопасности виртуальной инфраструктуры. Для определения угроз безопасности информации и разработки модели угроз, в рамках данной статьи, была разработана модель нарушителя безопасности ВИ.

В соответствии с методиками ФСТЭК России и ФСБ России [4], [5] все нарушители были поделены на внутренних и внешних. Внешние нарушители подразделяются на две категории: категория I (лица, не имеющие права доступа в контролируемую зону информационной системы) и категория II (лица, имеющие право постоянного или разового доступа в контролируемую зону информационной системы). К внешним нарушителям категории I относятся бывшие сотрудники предприятия и посторонние лица, действующие в инициативном порядке. К внешним нарушителям категории II относятся представители преступных организаций. К внутренним нарушителям относятся сотрудники организации с разными правами доступа к компонентам системы, персонал, не имеющий легитимного доступа к компонентам системы, и лица из сторонних организаций, имеющие прямой или косвенный доступ к компонентам инфраструктуры.

Для каждого нарушителя были выделены возможные объекты атаки, средства атаки и используемые ими уязвимости. Общий перечень угроз, характерных для ВИ, приведен в проекте ГОСТа «Защита информации. Защита информации при использовании технологий виртуализации. Общие положения» [1].

Требования к системе защиты информации для виртуальной инфраструктуры. Отталкиваясь от данных угроз и модели нарушителя, были разработаны требования к системе защиты информации для ВИ, являющихся частью ИС, в которых не ведется обработка сведений, составляющих государственную тайну.

В соответствии с Приказом ФСТЭК России №17 [6], устанавливаются четыре класса защищенности ИС. Ниже представлена табл. 1, в которой сведены воедино классы защищенности и требования, предъявляемые к ним.

Таблица 1

Требования безопасности для ВИ, являющихся частью ИС

№	Требования	Класс защищенности			
		4	3	2	1
Т1	Требования к идентификации и аутентификации субъектов доступа и объектов доступа в ВИ	+	+	++	++
Т2	Требования к управлению доступом субъектов доступа к объектам доступа в ВИ, в том числе внутри ВМ	+	++	++	++
Т3	Требования к регистрации событий безопасности в ВИ	-	+	+	+
Т4	Требования к управлению (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами ВИ, а также по периметру ВИ	-	-	+	++
Т5	Требования к доверенной загрузке серверов виртуализации (гипервизор), ВМ, серверов управления виртуализацией	-	-	-	-
Т6	Требования к управлению перемещением ВМ и обрабатываемых на них данных	-	-	+	++
Т7	Требования к контролю целостности ВИ и ее конфигураций	-	-	+	+
Т8	Требования к резервному копированию данных, резервированию технических средств, программного обеспечения ВИ, а также каналов связи внутри ВИ	-	-	+	++
Т9	Требования к реализации и управлению антивирусной защитой	-	+	++	++
Т10	Требования к разбиению ВИ на сегменты для обработки информации отдельным пользователем или группой	-	-	+	++
Т11	Минимальный требуемый класс СВТ при построении ИС	5	5	5	5
Т12	Минимальный требуемый класс СОВ при построении ИС (в случае взаимодействия с сетями международного обмена)	5	5(4)	4	4
Т13	Минимальный требуемый класс МЭ при построении ИС (в случае взаимодействия с сетями международного обмена)	4	4(3)	4(3)	4(3)
Т14	Минимальный требуемый класс антивирусной защиты при построении ИС (в случае взаимодействия с сетями международного обмена)	5	5(4)	4	4
Т15	Минимальный требуемый уровень уровню контроля отсутствия НДВ для используемого в ИС ПО	-	-	4	4

Примечания: *+ требование предъявляется; ++ предъявляются усиленные требования; (n) – значение в случае взаимодействия с сетями международного обмена.

В данной статье был сделан акцент на разборе требований, предъявляемых к системам защиты информации, разработанным для ВИ к построенным в соответствии с 1-м классом защищенности, как наиболее полном.

Т1. Требования к идентификации и аутентификации субъектов доступа и объектов доступа в ВИ, в том числе администраторов.

Идентификация и аутентификация субъектов и объектов доступа должна осуществляться в соответствии с требованиями ИАФ.1-ИАФ.7 из методического документа ФСТЭК России «Меры защиты информации в Государственных информационных системах» [5].

В качестве объектов доступа в ВИ необходимо рассматривать программное обеспечение управления ВИ, гипервизор, хостовую ОС, ВМ, виртуализированное ПО, СЗИ, используемые в рамках ВИ.

При реализации мер по идентификации и аутентификации субъектов доступа и объектов доступа в ВИ должны обеспечиваться:

- идентификация и аутентификация администраторов управления средствами виртуализации;
- идентификация и аутентификация субъектов доступа при их локальном и удалённом обращении к объектам доступа в ВИ;
- блокировка доступа к компонентам ВИ для субъектов доступа, не прошедших процедуру аутентификации;
- защита аутентификационной информации в процессе ее ввода для аутентификации в ВИ от возможного использования неуполномоченными лицами;
- идентификация и аутентификация субъектов доступа при осуществлении ими попыток доступа к средствам управления аппаратного обеспечения ВИ.

Внутри ВМ должна быть обеспечена реализация мер по идентификации и аутентификации субъектов и объектов доступа в соответствии с ИАФ.1–ИАФ.7[5].

Требования усиления.

В ИС должны обеспечиваться взаимная идентификация и аутентификация пользователя и ВМ при удалённом доступе.

Т2. Требования к управлению доступом субъектов доступа к объектам доступа в ВИ, в том числе внутри ВИ.

Эту функцию в части управления доступом к ВИ выполняет гипервизор или СЗИ. Но управление доступом внутри ВМ эти средства выполнить не могут, в этом случае используются классические СЗИ от НСД, устанавливаемые на ВМ.

В ВИ должно обеспечиваться управление доступом субъектов доступа к объектам доступа, в том числе внутри ВМ, в соответствии с УПД.1-УПД.13 из [5].

При реализации мер по управлению доступом субъектов доступа к объектам доступа в ВИ должны обеспечиваться:

- контроль доступа субъектов доступа к средствам управления компонентами ВИ;
- контроль доступа субъектов доступа к файлам-образам виртуализированного программного обеспечения, ВМ, файлам-образам ВМ;
- управление доступом к виртуальному аппаратному обеспечению информационной системы, являющимся объектом доступа;
- контроль запуска ВМ на основе заданных оператором правил;
- разграничение доступа субъектов доступа, зарегистрированных на ВМ, к объектам доступа, расположенным внутри ВМ, в соответствии с правилами разграничения доступа пользователей данных ВМ;
- разграничение доступа субъектов доступа, зарегистрированных на ВМ, к ресурсам ВИ, размещенным за пределами ВМ, в соответствии с правилами разграничения доступа.

Требования усиления.

В ВИ должен обеспечиваться доступ к операциям, выполняемым с помощью средств управления ВМ, в том числе к операциям создания, запуска, останова, создания копий, удаления ВМ, который должен быть разрешен только администраторам ВИ.

Т3. Требования к регистрации событий безопасности в ВИ.

Должна обеспечиваться регистрация событий безопасности в соответствии с РСБ.1-РСБ.5 [5].

При реализации мер по регистрации событий безопасности в ВИ дополнительно к событиям, установленным в РСБ.1 [5], должны подлежать регистрации: запуск и завершение работы компонентов ВИ, доступ субъектов доступа к компонентам ВИ, изменения в составе и конфигурации компонентов ВИ во время их запуска, функционирования и аппаратного отключения.

Для данных событий должны быть зафиксированы: дата и время события, результат события (успешный или не успешный), идентификатор пользователя, инициировавшего событие.

Т4. Требования к управлению потоками информации между компонентами ВИ, а также по периметру ВИ.

В ИС должно осуществляться управление потоками информации между компонентами ВИ и по периметру ВИ в соответствии с УПД.3, ЗИС.3 [5], при этом должны обеспечиваться:

- фильтрация сетевого трафика между компонентами ВИ, в том числе между внешними и внутренними по отношению к ВМ сетями;
- наличие доверенных маршрутов внутри ВИ между администратором, пользователем и СЗИ (функциями безопасности);
- контроль передачи служебных информационных сообщений;
- отключение неиспользуемых сетевых протоколов гипервизора, хостовой операционной системы (ОС), виртуальной вычислительной сети компонентами ВИ;
- обеспечение подлинности сетевых соединений (сеансов взаимодействия) внутри ВИ, в том числе для защиты от подмены сетевых устройств и сервисов;
- обеспечение изоляции потоков данных, передаваемых и обрабатываемых компонентами ВИ и сетевых потоков виртуальной вычислительной сети;
- семантический и статистический анализ сетевого трафика.

Требования усиления.

Должна быть обеспечена единая точка подключения к ВИ. В ИС должна обеспечиваться фильтрация сетевого трафика от (к) каждой гостевой ОС, в виртуальных сетях гипервизора и для каждой ВМ.

Т6. Требования к управлению перемещением ВМ и обрабатываемых данных.

Оператором должно обеспечиваться управление перемещением ВМ и обрабатываемых на них данных. При этом должны обеспечиваться:

- регламентирование порядка перемещения (определение ответственных за организацию процесса, объектов перемещения, ресурсов инфраструктуры, задействованных в перемещении, а также способов перемещения);
- управление размещением и перемещением данных, файлов-образов и исполняемых файлов ВМ.

Управление перемещением ВМ должно обеспечить:

- полный запрет перемещения ВМ;
- ограничение перемещения ВМ в пределах информационной системы;
- ограничение перемещения ВМ между сегментами ИС.

Требования усиления.

Оператором должна осуществляться обработка отказов перемещения ВМ (контейнеров) и обрабатываемых на них данных.

Т7. Требования к контролю целостности (КЦ) ВИ и ее конфигураций.

В ИС должен обеспечиваться КЦ компонентов ВИ в соответствии с ОЦЛ.1 [5]. При реализации этих мер должны обеспечиваться:

- КЦ компонентов, критически важных для функционирования хостовой ОС, гипервизора, гостевых ОС и (или) обеспечения безопасности обрабатываемой в них информации;

- КЦ состава и конфигурации виртуального оборудования;
- КЦ файлов, содержащих параметры настройки виртуализированного программного обеспечения и ВМ;
- КЦ файлов-образов виртуализированного программного обеспечения и ВМ, файлов-образов, используемых для обеспечения работы виртуальных файловых систем;
- КЦ резервных копий ВМ.

Т8. Требования к резервному копированию данных, резервированию технических средств, ПО ВИ, а также каналов связи внутри ВИ.

В ИС должны обеспечиваться резервное копирование данных, резервирование технических средств, программного обеспечения ВИ и каналов связи внутри ВИ в соответствии с ОДТ.2, ОДТ.4, ОДТ.5 [5]. При реализации этих требований должны обеспечиваться:

- определение мест хранения резервных копий ВМ и данных;
- резервное копирование ВМ;
- резервное копирование данных, обрабатываемых в ВИ;
- резервирование программного обеспечения ВИ;
- резервирование каналов связи, используемых в ВИ;
- периодическая проверка резервных копий и возможности восстановления ВМ и данных, обрабатываемых в ВИ с использованием резервных копий.

Требования усиления.

В ИС должно выполняться резервное копирование конфигурации ВИ, программного обеспечения серверов управления виртуализацией, автоматизированного рабочего места администратора управления средствами виртуализации, а также дистрибутивов средств построения ВИ.

Т9. Требования к реализации и управлению антивирусной защитой в ВИ.

В ИС должны обеспечиваться реализация и управление антивирусной защитой в ВИ в соответствии с АВЗ.1, АВЗ.2 [5]. При реализации соответствующих мер должны обеспечиваться:

- проверка наличия вредоносных программ (вирусов) в хостовой ОС, включая контроль файловой системы, памяти, запущенных процессов;
- проверка наличия вирусов в гостевой ОС, включая контроль файловой системы, памяти, запущенных приложений и процессов.

Требования усиления.

В информационной системе должно обеспечиваться разграничение доступа к управлению средствами антивирусной защиты.

Т10. Требования к разбиению ВИ на сегменты (сегментирование ВИ) для обработки информации отдельным пользователем и (или) группой пользователей.

В ИС должно обеспечиваться разбиение ВИ на сегменты для обработки информации пользователем и группой пользователей в соответствии с ЗИС.17 [5].

Требования усиления.

В ИС должно обеспечиваться выделение в отдельный сегмент (отдельные сегменты) серверов управления виртуализацией.

Заключение. Результатом данной работы стали разработанные модель типовой ВИ, которая может быть использована при создании различных ИС, модель нарушителя и модель угроз, а также непосредственный перечень требований к системам защиты информации для таких ИС.

Таким образом, на основании проанализированных документов, проектов документов и приведенных в данной статье наработок можно построить информационную систему с использованием технологий виртуализации, отвечающую требованиям основных регуляторов в сфере информационной безопасности на территории Российской Федерации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Защита информации. Защита информации при использовании технологий виртуализации. Общие положения [проект ГОСТ: разраб. ФСТЭК России]. – [окончательная редакция]. – М., 2014. – С. 39.
2. *Ледовской В.П.* Виртуальным инфраструктурам – прогрессивная защита // Anti-Malware.ru – независимый информационно-аналитический центр. 2012. URL: http://www.anti-malware.ru/analytics/Progressive_Defense_for_Virtual_Infrastructures (дата обращения: 28.04.2014).
3. Securing Virtual Applications and Servers // Cisco Systems, Inc. 2012. URL: http://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/unified-network-services-uns/white_paper_c11-652663.html (дата обращения: 28.04.2014).
4. Модель угроз и нарушителя безопасности персональных данных, обрабатываемых в специальных информационных системах персональных данных отрасли. Методический документ Министерства связи и массовых коммуникаций Российской Федерации: одобр. Решение секции №1 Научно-технического совета Минкомсвязи России «Научно-техническое и стратегическое развитие отрасли» 21.04.2010]. – 1-е изд. – М., 2010. – С. 50.
5. Меры защиты информации в государственных информационных системах. Методический документ ФСТЭК России: утв. ФСТЭК России 11.03.2014. – М., 2014. – С. 176.
6. Российская Федерация. Приказы. Об утверждении требований по защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах [приказ ФСТЭК России №17: издан ФСТЭК России 11.03.2013]. – 1-е изд. – М., 2013. – С. 37.
7. Российская Федерация. Приказы. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных [приказ ФСТЭК России №21: издан ФСТЭК России 18.03.2013]. – 1-е изд. – М., 2013. – С. 20.
8. *Бойцов И.В.* Как защитить виртуальную инфраструктуру по требованиям ФСТЭК // Информационная безопасность. – 2014. – № 1. – С. 30-32.
9. *Лапшин С.В., Конявская С.В.* Защита систем виртуализации // Информационная безопасность. – 2010. – № 6. – С. 34-35.

REFERENCES

1. Zashchita informatsii. Zashchita informatsii pri ispol'zovanii tekhnologiy virtualizatsii. Obshchie polozheniya [Protection of information. Information security when using virtualization technologies. General provisions] [proekt GOST: razrab. FSTEK Rossii]. [okonchatel'naya redaktsiya]. Moscow, 2014, pp. 39.
2. *Ledovskoy V.P.* Virtual'nym infrastrukturam – progressivnaya zashchita [Virtual infrastructures - progressive protection], Anti-Malware.ru – nezavisimyy informatsionno-analiticheskiy tsentr. 2012. Available at: http://www.anti-malware.ru/analytics/Progressive_Defense_for_Virtual_Infrastructures (accessed: 28 April 2014).
3. Securing Virtual Applications and Servers, *Cisco Systems, Inc. 2012*. Available at: http://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/unified-network-services-uns/white_paper_c11-652663.html (accessed: 28 April 2014).
4. Model' ugroz i narushitelya bezopasnosti personal'nykh dannykh, obrabatyvaemykh v spetsial'nykh informatsionnykh sistemakh personal'nykh dannykh otrasli [The threat model and intruder security of personal data processed in a special personal data information systems industry]. *Metodicheskiy dokument Ministerstva svyazi i massovykh kommunikatsiy Rossiyskoy Federatsii: odobr. Reshenie sektsii №1 Nauchno-tekhnicheskogo soveta Minkomsvyazi Rossii «Nauchno-tekhnicheskoe i strategicheskoe razvitie otrasli» 21.04.2010* [Methodological document of the Ministry of communications and mass communications of the Russian Federation: approved The solution of section No. 1 of the Scientific-technical Council of the Ministry of communications of Russia Scientific-technical and strategic development of the sector 21.04.2010]. 1st ed. Moscow, 2010, pp. 50.

5. Mery zashchity informatsii v gosudarstvennykh informatsionnykh sistemakh [Measures for protection of information in government information systems]. *Metodicheskiy dokument FSTEK Rossii: utv. FSTEK Rossii 11.03.2014* [Methodological document the FSTEC of Russia: appr. The FSTEC of Russia 11.03.2014]. Moscow, 2014, pp. 176.
6. Rossiyskaya Federatsiya. Prikazy. Ob utverzhdenii trebovaniy po zashchite informatsii, ne sostavlyayushchey gosudarstvennuyu taynu, soderzhashcheysya v gosudarstvennykh informatsionnykh sistemakh [of The Russian Federation. The orders. Approval requirements for protection of information, not state secrets contained in the state information systems] *[prikaz FSTEK Rossii №17: izdan FSTEK Rossii 11.03.2013]* [the order of the FSTEC of Russia No. 17: published by the Russian FSTEC 11.03.2013]. 1st ed. Moscow, 2013, pp. 37.
7. Rossiyskaya Federatsiya. Prikazy. Ob utverzhdenii sostava i soderzhaniya organizatsionnykh i tekhnicheskikh mer po obespecheniyu bezopasnosti personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh [of The Russian Federation. The orders. On approval of the composition and content of organizational and technical measures to ensure the security of personal data during their processing in information systems of personal data] *[prikaz FSTEK Rossii №21: izdan FSTEK Rossii 18.03.2013]* [the order of the FSTEC of Russia No. 21: published by the Russian FSTEC 18.03.2013]. 1st ed. Moscow, 2013, pp. 20.
8. *Boytsov I.V.* Kak zashchitit' virtual'nuyu infrastrukturu po trebovaniyam FSTEK [How to protect virtual infrastructure requirements FSTEC], *Informatsionnaya bezopasnost'* [Information Security], 2014, No. 1, pp. 30-32.
9. *Lapshin S.V., Konyavskaya S.V.* Zashchita sistem virtualizatsii [Protection systems virtualization], Informatsionnaya bezopasnost' [Information Security], 2010, No. 6, pp. 34-35.

Статью рекомендовал к опубликованию д.т.н., профессор О.Б. Макаревич.

Курносов Кирилл Викторович – НГУЭУ; e-mail: kursorkvk@mail.ru; 630099, г. Новосибирск, ул. Каменская, 52/1; тел.: 89137532181; кафедра информационной безопасности; студент.

Селифанов Валентин Валерьевич – e-mail: sfo1@mail.ru; тел.: 83832640484; кафедра информационной безопасности; старший преподаватель; начальник 6 отдела Управления ФСТЭК России по Сибирскому федеральному округу.

Kurnosov Kirill Viktorovich – Novosibirsk State University of Economics and Management; e-mail: kursorkvk@mail.ru; 52/1, Kamenskaya street, Novosibirsk, 630099, Russia; phone: +79137532181; the department of information security; student.

Selifanov Valentin Valer'evich – e-mail: sfo1@mail.ru; phone: +73832640484; the department of information security; senior lecturer; head of the 6th Department FSTEC of Russia in SFD.

УДК 004.057.4

А.М. Максимов, Е.Н. Тищенко, О.В. Серпенинов

РАССМОТРЕНИЕ HTTP-ЗАГОЛОВКА СТАНДАРТА ДЕ-ФАКТО X-FORWARDED-FOR КАК ЭЛЕМЕНТА, СПОСОБСТВУЮЩЕГО ОСУЩЕСТВЛЕНИЮ НСД К ВЕБ-РЕСУРСАМ

Рассмотрен один из аспектов функционирования современных компьютерных сетей – заголовки протоколов. Проведен краткий анализ документов, в которых представлены стандарты, регулирующие функционирование рассматриваемого протокола HTTP в сети Интернет. В частности, сделан анализ нестандартного заголовка для протокола HTTP – X-Forwarded-For. Данный заголовок является стандартом де-факто, что отражено и в документах, описывающих и регламентирующих его использование. Произведён краткий обзор распространённости платформ, которые поддерживают использование означенного заголовка. В результате анализа с точки зрения безопасности установлено наличие рис-