УДК 004.9

К.В. Курносков

Методика оценки безопасности информационных систем, построенных с использованием технологий виртуализации

Защита виртуальных сегментов информационных систем является актуальной проблемой для компаний, использующих технологии виртуализации. Обеспечение информационной безопасности виртуализации является одним из приоритетных направлений в развитии ИТ-рынка России. В данной работе проанализированы существующие методики оценки безопасности и кратко описана собственная методика оценки безопасности информационных систем, построенных с использованием технологий виртуализации, разработанная с учетом выявленных недостатков у существующих на данный момент. Модель, на которой основывается данная методика, может быть использована при оценке безопасности более широкого круга информационных систем.

Ключевые слова: виртуализация, виртуальная инфраструктура, виртуальная машина, гипервизор, информационная безопасность, уязвимости виртуализации, идентификация угроз, модель угроз.

doi: 10.21293/1818-0442-2019-22-1-37-44

По оценкам компании Veeam [1], IDC [2] и Cisco [3], мировой рынок виртуализации продолжает развиваться очень быстрыми темпами, а в России это одна из самых стремительно развивающихся областей ИТ-рынка. В утвержденной Постановлением Правительства Российской Федерации от 28 июля 2017 г. № 1632-р программе «Цифровая экономика Российской Федерации» [4], подписанной Председателем Правительства Д.А. Медведевым, отмечается, что рынок «облачных услуг», в основе которых лежит использование технологий виртуализации, растет на 40% ежегодно. Но в отличие от большинства стран Россия не имеет стандартов оценки безопасности в этой сфере. При этом количество преступлений в цифровой среде за последние три года возросло на 75%.

Информационную безопасность, согласно этой программе, относят к одному из пяти базовых направлений развития цифровой экономики, а для решения проблем роста киберпреступности предлагается совершенствовать систему информационной безопасности во всех секторах экономики. Одним из основных препятствий на данном пути развития называют нерешенные проблемы при обеспечении информационной безопасности в сложных иерархических информационно-телекоммуникационных системах, широко использующих виртуализацию.

К таким проблемам относятся: 1) недостаточная нормативная база обеспечения безопасности ИС, использующих технологии виртуализации; 2) дефицит методического обеспечения для построения систем защиты и оценки уровня защищенности систем, использующих технологии виртуализации; 3) оценка уровня доверия к платформам виртуализации и разработанным для них средствам защиты.

Для решения этих проблем в дорожной карте реализации работ по направлению «Информационная безопасность» выделяются такие вехи как: 1) разработка проектов стандартов информационной безопасности объектов информационной инфраструктуры; 2) определение методики оценки показателей информационной безопасности на сетях связи;

3) законодательное закрепление требований к устойчивости и безопасности сетей связи и оборудования; 4) разработка и внедрение национальных стандартов в области информационной безопасности в системах, реализующих облачные, туманные и прочие технологии, построенные с использованием систем виртуализации.

Таким образом, результаты данной работы могут внести некоторый вклад в реализацию программы «Цифровая экономика».

Анализ текущего состояния нормативно-методического обеспечения в сфере безопасности виртуальных инфраструктур позволяет выделить следующие проблемы, связанные с нормативно-методической базой и стандартизацией.

По результатам анализа существующих российских и международных методик по определению угроз и оценке безопасности в информационных системах разного назначения [5–14] были сделаны следующие выводы.

Во-первых, существующие методики позволяют получить статическую оценку системы в определенный момент времени и не учитывают изменения в инфраструктуре и (или) внешней среде. Данная оценка не может считаться актуальной после даже незначительных изменений, примерами которых являются установка обновлений, замена программного обеспечения, публикация информации о новых методах атак, изменение уровня важности защищаемой информации. Пересчет показателей при подобных изменениях выполняется вручную, являясь достаточно трудоёмким даже для высококвалифицированных специалистов.

Во-вторых, компоненты системы в данных методиках рассматриваются как отдельные элементы. Не учитывается специфическая связь между объектами, присущая виртуальным инфраструктурам, и влияние реализации одних угроз на возможность реализации других. Например, компрометация гипервизора практически всегда будет нести за собой компрометацию виртуальных машин, управляемых им.

В-третьих, основным критерием оценки угроз является субъективная оценка экспертов. Такой подход к оценке рассматривает угрозу как отдельную сущность, а не взаимосвязанный набор компонентов, из которых она сформирована, что ограничивает возможность формализации и математических обоснований [6].

В данной работе сформулированы требования, которым должна отвечать методика оценки безопасности информационных систем, функционирующих на базе технологий виртуализации.

Пространство понятий

Нередко встречается ситуация, когда методики оперируют понятиями, которые в разных документах интерпретируются по-разному. Примером может являться подход к понятию «угроза безопасности информации», которое имеет различные толкования. В методическом документе «Меры защиты информации в ГИС» [5] компонентами угрозы являются: возможности нарушителя, уязвимость информационной системы, способ реализации и последствия от реализации. В проекте методики определения угроз безопасности ФСТЭК [6], помимо вышеперечисленных компонентов, появляется еще один: объект воздействия. Несмотря на то, что определение этого понятия стало более полным и точным, это идет вразрез с классической терминологией, данной в ГОСТ Р 50922–2006 [15]. Существуют и другие подходы к определению понятия «угроза» [16].

Соответственно, для корректного применения данных методик, необходимо изначально определить границы соответствия терминологии некому подходу или стандарту.

Формализация

Методика должна оперировать понятиями, подающимися математической формализации и состоящими из простых элементов, допускающих количественные оценки или имеющих качественные характеристики, представленные конечными списками возможных состояний. Итоговые оценки должны присваиваться путем математических расчетов по представленным формулам и на основе конкретно определенных исходных данных. Количество исходных параметров, основанных на экспертных оценках, должно быть сведено к минимуму.

Спецификация

Методика оценки безопасности информационных систем, построенных на базе виртуальных инфраструктур, должна учитывать их специфику. Виртуализация имеет принципиальные отличия от технологий, работающих на физических объектах. Многие особенности, такие как наличие гипервизора, моментальных снимков (снапшотов) или эталонных образов, не имеют аналогов в обычных информационных системах, поэтому некорректно оценивать их безопасность по общим методикам.

Взаимосвязанность

При использовании технологий виртуализации многие компоненты взаимосвязаны гораздо теснее, чем компоненты обычных информационных систем.

Такие компоненты, как гипервизор, виртуальная машина, виртуальная сеть, невозможно рассматривать изолированно ввиду их технологической реализации. Любые угрозы, настройки и изменения в одном из компонентов имеют значительное влияние на смежные компоненты. Важной особенностью является то, что одни самостоятельные объекты являются просто данными для других, являющихся их носителями [17].

Динамичность

Информационная система и внешняя среда не являются статическими объектами. Регулярно обнаруживаются новые уязвимости программного обеспечения, появляются новые методы атак, выходят обновления и патчи, способные за несколько недель значительно изменить функционал платформ виртуализации. Важность информации и ее свойств тоже не является постоянной величиной. Если речь идет о реальном обеспечении безопасности, а не о разовом выполнении нормативных требований при аттестации, то методика должна иметь механизмы, позволяющие с минимальными затратами ресурсов актуализировать оценку уровня безопасности информационных систем «на лету». На практике это означает, что методика должна иметь возможность автоматизации процесса оценки при изменении объекта или внешней среды.

Соблюдение данных требований является необходимым условием для качественного улучшения методик оценки показателей информационной безопасности в информационных системах, построенных с применением технологий виртуализации.

Ниже приведена сравнительная характеристика некоторых из наиболее распространенных методик по предложенным критериям (табл. 1).

Полученные данные дают представление о сильных и слабых сторонах рассмотренных методик оценки безопасности виртуальной инфраструктуры и позволяют определить основные направления их совершенствования с целью создания удовлетворяющей данным требованиям методики и основанной на ней автоматизированной системы оценки безопасности информационных систем, построенных на технологиях виртуализации.

Разработанный алгоритм оценки защищенности ИС состоит из следующих этапов: 1) идентификация защищаемой информации; 2) ранжирование информации по уровням важности; 3) идентификация носителей защищаемой информации – объектов защиты; 4) определение необходимого состояния объекта, которое будет считаться безопасным; 5) определение множества состояний, в которые может перейти объект из состояния, считающегося безопасным; 6) идентификация угроз, реализация которых может привести к изменению безопасного состояния объекта; 7) определение требований безопасности для объектов защиты; 8) оценка соответствия системы защиты предъявляемым требованиям; 9) составление рекомендаций для повышения уровня защищенности ИС.

Таблица 1

Сравнение методик по представленным требованиям

Название методики или подхода	Пространство понятий	Формализация	Спецификация	Взаимосвязанность	Динамичность
Cloud Computing Risk Assessment [18]	Использует термины Европейского агентства сетевой и информационной безопасности	Конечные списки, количественные оценки, экспертные оценки	Учитывается	Отсутствует	Статична
Методика определения угроз безопасности информации в информационных системах [6]	Предлагаются собственные определения, выходящие за рамки ГОСТ Р 56938–2016 [19] и ГОСТ Р 50922–2006 [15]	Использован банк угроз безопасности, конечные списки	Универсальная	Отсутствует	Статична
ГОСТ Р ИСО/МЭК ТО 13335-3–2007. Методы и средства обеспечения безопасности [9]	Использует термины ИСО/МЭК	Конечные списки, количественные оценки, экспертные оценки	Универсальная	Присутствует	Статична
Попов А.М., Золотарев В.В., Бондарь И.В. Методика оценки защищенности информационной системы по требованиям стандартов информационной безопасности [10]	Использует термины ИСО/МЭК	Количествен. оценка, использование двоичной логики, экспертные оценки	Универсальная	Отсутствует	Статична

Идентификация защищаемой информации

Идентификация защищаемой информации – это первый шаг при построении системы защиты и оценки защищенности ИС. Первоначально определяется перечень конфиденциальной информации, подлежащей защите в соответствии с требованием текущего законодательства в области защиты информации. Далее включается информация, подлежащая защите на основе внутренних документов организации, коммерческая тайна и прочая информация, отнесенная организацией к защищаемой. На практике основным способом определения перечня защищаемой информации является организация работы экспертной комиссии в организации. Более подробно о различных методах идентификации информации написано в работах Н.В. Гришиной [20], Г.Г. Камаловой [21], А.А. Караваевой [22].

Ранжирование информации по уровням важности

На основе списка идентифицированной защищаемой информации экспертная комиссия определяет важность сохранения свойств каждого информационного ресурса для организации и непосредственную его ценность. В рамках предлагаемой методики можно использовать любую количественную оценку важности – как базовую с рангами: 1 – «неважная», 2 – «важная», 3 – «критически важная», так и более сложные градации. Способы оценки важности информации и ее свойств в своих работах предлагали В.Е. Ходаков, В.Н. Козел [23], А.Ф. Чипига [24]; И.Ю. Нежданов [25].

Идентификация носителей защищаемой информации

Идентификация носителей защищаемой информации является важным шагом при оценке защищенности.

Носитель может быть как физическим устройством (жесткий диск, сетевой кабель), так и логиче-

ским объектом (виртуальный жесткий диск, пакет данных, оперативная память виртуальной машины). В рамках данной работы носителем будет считаться как конечный объект (компонент виртуальной инфраструктуры), на котором происходит хранение информации, так и промежуточные объекты, через которые информация передается.

Нельзя не отметить, что носители обладают своей иерархией, например, физический носитель может содержать несколько логических носителей, которые, в свою очередь, могут содержать другие логические носители. Таким образом, выстраивается «пирамида», в основании которой находится физический носитель, а каждая последующая логическая сущность последовательно надстраивается на него и является просто информацией по сравнению с предыдущей ступенью. Следовательно, для полноты модели нельзя не учитывать такой вид информации (рис. 1).

Рис. 1. Иерархия носителей информации

На первом этапе определяется статическое место хранения всей идентифицированной защищаемой информации. Это позволяет определить конечные объекты защиты. На втором этапе на основе бизнес-процессов, связанных с обработкой защищаемой информации, определяются пути движения информации в границах информационной системы, построенной с использованием технологий виртуализации. На основе карт перемещения информации в процессе ее обработки определяются ресурсы, вы-

ступающие носителями информации при ее движении. На третьем шаге определяются носители, выступающие родительскими по отношению к ресурсам виртуализации в информационной системе. В качестве примера рассмотрим процесс доступа к

условному файлу, содержащему конфиденциальную информацию пользователем информационной системы посредством удаленного доступа к виртуальной машине, на которой этот файл расположен (рис. 2).

Рис. 2. Процесс доступа пользователя к файлу

Таким образом, видно, что при обработке файла с защищаемой информацией его носителем выступает не один объект – виртуальный жесткий диск, а некоторое множество. При этом изменение безопасного состояния любого из носителей приведет к изменению свойств информации в самом защищаемом файле. Следовательно, оценивать нужно не только безопасность конечного носителя, но и всех, участвующих в процессе обработки.

Определение безопасного состояния объекта

На основе результата сопоставления уровня важности свойств информации и носителей, на которых она располагается при хранении и обработке составляется таблица соответствия состояния информации и состояния носителя, при котором может быть достигнуто требуемое состояние информации. Каждому состоянию информации соответствует однозначно определенное состояние носителя этой информации (табл. 2).

Таблица 2

Соответствие состояния информации с состоянием ее носителя

Состояние информации	Состояние физической компоненты носителя	Состояние логической компоненты носителя
Конфиденциальность информации	Доступность чтения только разрешенными интерфейсами*	Доступность чтения носителя только для легитимных функций, запущенных легитимным пользователем
Целостность информации	Доступность записи только разрешенными интерфейсами	Доступность записи на носитель только для легитимных функций, запущенных легитимным пользователем
Доступность информации	Наличие функционирующего физического канала связи с пользователем информации**	Наличие функционирующего логического канала связи информации с легитимным пользователем

* Интерфейс системы, предназначенный для взаимодействия с этим носителем.

** Как конечный пользователь, так и любой элемент системы, использующий эту информацию.

Определение множества состояний, в которые может перейти объект из состояния, считающегося безопасным

Опираясь на табл. 2, можно заключить, что для обеспечения безопасности информации требуется

обеспечение поддержания определенного состояния носителей этой информации. Выход из этого состояния и переход в состояние, которое не является безопасным, возможен при реализации некоторых условий перехода. Для моделирования таких переходов был использован аппарат ингибиторных сетей Петри (рис. 3).

Рис. 3. Модель выхода объекта из безопасного состояния

Состояние p1 определяется как безопасное состояние объекта. Условия перехода в другие конечные состояния объекта при осуществлении перехода представлены ниже (табл. 3).

Идентификация угроз, реализация которых может привести к изменению безопасного состояния объекта

Для решения задач идентификации и построения модели угроз безопасности информационных систем в настоящий момент используются следующие подходы: 1) модели, построенные на основе сетей Петри; 2) геометрические модели; 3) нечеткие продукционные модели; 4) математический анализ устойчивости систем; 5) теоретико-множественный подход; 6) нечеткие когнитивные карты.

Любая реализация угрозы информационной безопасности предполагает следующую последовательность событий.

Таблица 3

Условия перехода объекта в небезопасные состояния

Состояние объекта	Переход	Условия перехода
p2 Доступность чтения носителя для нелегитимных функций или функций, запущенных нелегитимным пользователем	t1	Несанкционированный доступ на чтение – доступ, не предусмотренный политиками доступа
	t2	Переополнение буфера – обращение к участкам памяти, не предназначенным для чтения информации этим пользователем
	t3	Повышение прав доступа – запуск функций с правами, не предоставленными пользователю, инициирующему запуск
	t4	Получение доступа на чтение пользователем после нелегитимного изменения матрицы доступа
p3 Доступность записи на носитель только для нелегитимных функций или функций, запущенных нелегитимным пользователем	t5	Несанкционированный доступ на запись – доступ с возможностью внесения изменений, не предусмотренный политиками доступа
	t6	Переополнение буфера – обращение к участкам памяти, не предназначенным для записи информации этим пользователем
	t7	Повышение прав доступа – запуск функций с правами на запись, не предоставленными пользователю, инициирующему запуск
	t8	Получение доступа на запись пользователем после нелегитимного изменения матрицы доступа
p3 Нарушение функционирующего логического канала связи информации с пользователем информации	t9	Атака типа «отказ в обслуживании», вызывающая исчерпание вычислительных ресурсов носителя
	t10	Изменение конфигурации носителя, влекущее невозможность его взаимодействия с пользователем информации

Источник угрозы через канал взаимодействия с одним из компонентов виртуальной инфраструктуры (это может быть как физический, так и логический объект) совершает некоторое воздействие (отправляет пакет, изменяет параметры конфигурации). Эти действия реализуют процесс, при котором система или ее компоненты меняют свое текущее состояние (в данной работе этот процесс будет называться атакой). В случае наличия у системы уязвимости атака может реализовать некое деструктивное воздействие, способное изменить некоторые свойства компонента виртуальной инфраструктуры, а следовательно, и информации, которую он содержит. Схематически этот процесс можно изобразить в виде ментальной карты (рис. 4). Подробнее этот шаг описан в ранних статьях [16, 17].

Определение требований безопасности**для объектов защиты**

После идентификации всех угроз, влекущих переходы объектов из безопасного состояния в другие, необходимо определить требования, выполнение которых позволит нейтрализовать идентифицированные угрозы. Как видно из карты, представленной на рис. 4, все требования сводятся к двум видам. Для устранения угрозы можно или закрыть уязвимость объекта, или закрыть канал связи между источником угрозы и защищаемым объектом. В качестве примера разберем случай угрозы пользовательским данным, расположенным на виртуальном диске виртуальной машины, под управлением ОС Windows при использовании уязвимости MS17-010, ставшей широко известной после эпидемии вируса WannaCry. Угрозы можно устранить двумя путями. Во-первых, можно установить обновление «Security Update for Microsoft Windows SMB Server (4013389)» на виртуальной машине или заблокировать передачу трафика в виртуальную локальную сеть гипервизора по протоколу SMB.

Оценка соответствия системы защиты предъявляемым требованиям

Оценка соответствия проводится последовательной проверкой выполнения требований, представленных на предыдущем шаге. Сопоставление текущих и требуемых версий программного обеспечения, проверка наличия установленных обновлений или выполнение требуемых настроек могут быть автоматизированы для ускорения процесса и получения динамично изменяющейся итоговой оценки, которая может автоматически пересчитываться при изменении инфраструктуры или добавлении новых требований безопасности.

Составление рекомендаций для повышения уровня защищенности

Рекомендация составляются на основе результатов оценки соответствия системы защиты предъявленным требованиям. Данный процесс также может быть автоматизирован.

Таким образом, в данной работе в сжатом виде представлено упрощенное представление методики оценки безопасности информационных систем, построенных с использованием технологий виртуализации. Данная методика имеет высокий уровень формализации, позволяющий получить качественные оценки параметров угрозы и автоматизировать процесс оценки. Автоматизация позволит динамически пересчитывать полученные результаты при изменении внешней среды или компонентов системы. Объекты в модели тесно взаимосвязаны, и анализ производится с учетом этих связей, учитывающих особенности использования технологий виртуализации.

Заключение

Также учитывается рекурсивная последовательность, при которой для реализации угрозы необходим канал связи (объект виртуальной платформы), который, в свою очередь, может быть представлен как информация и ее носитель, а следовательно, для него тоже требуется определение перечня угроз.

Рис. 4. Ментальная карта понятия «угроза»

Литература

1. Ледовской В.П. Обзор средств защиты виртуальных сред VMware vSphere [Электронный ресурс]. – Режим доступа: http://www.anti-malware.ru/analytics/Virtualization_Security, свободный (дата обращения: 13.05.2018).
2. Гаврилов Д.А. Russian Cloud Services Market 2017–2021 Forecast and 2016 Vendor Shares [Электронный ресурс]. – Режим доступа: <http://idcrussia.com/ru/research/published-reports/65018-russian-cloud-services-market-2017-2021-forecast-and-2016-vendor-shares/2-abstract>, свободный (дата обращения: 13.05.2018).
3. Virtual Security In The Data Center [Электронный ресурс]. – Режим доступа: http://www.cisco.com/c/dam/en/us/solutions/collateral/data-center-virtualization/unified-fabric/tap_virtual_security_032012.pdf, свободный (дата обращения: 13.05.2018).
4. Программа «Цифровая экономика Российской Федерации», утв. распоряжением Председателя Правительства Российской Федерации от 28.07. 2017 г. № 1632-р. – М., 2017. – 88 с.
5. Меры защиты информации в государственных информационных системах: методический документ ФСТЭК России, утв. 2014-02-11. – М., 2017. – 176 с.
6. Методика определения угроз безопасности информации в информационных системах: проект методического документа ФСТЭК России [Электронный ресурс]. – Режим доступа: <https://fstec.ru/component/attachments/download/812> (дата обращения: 13.05.2018).
7. Определение актуальных угроз безопасности персональных данных при их обработке в информационных системах (ИС) персональных данных: методический документ ФСТЭК России, утв. 2008-02-14. – М., 2008. – 10 с.
8. Определение актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры: методический документ ФСТЭК России (ДСП), утв. 2008.11.18.
9. ГОСТ Р ИСО/МЭК ТО 13335-3–2007. Методы и средства обеспечения безопасности. – Ч. 3. – Введ. 2007-06-07. – М.: Изд-во стандартов, 2007. – 49 с.
10. Попов А.М. Методика оценки защищенности информационной системы по требованиям стандартов информационной безопасности / А.М. Попов, В.В. Золотарев, И.В. Бондарь // Информатика и системы управления. – 2010. – Т. 4, вып. 26. – С. 3–12.
11. Барабанов А.В. Методический аппарат оценки соответствия автоматизированных систем требованиям безопасности информации / А.В. Барабанов, А.С. Марков, В.Л. Цирлов // Спецтехника и связь. – 2011. – Вып. 3. – С. 48–53.
12. Еременко В.Т. Автоматизация процесса оценки состояния защищенности объекта информатизации с использованием ингибиторных, вероятностных и раскрашенных сетей Петри от утечки информации / В.Т. Еременко, М.Ю. Рытов, А.П. Горлов // Информация и безопасность. – 2015. – Т. 18, вып. 1. – С. 123–126.
13. Плетнев П.В. Методика оценки рисков информационной безопасности на предприятиях малого и среднего бизнеса / П.В. Плетнев, В.М. Белов // Доклады ТУСУР. – 2012. – Т. 1, вып. 25. – С. 83–86.
14. Баранова Е.К. Методика анализа рисков информационной безопасности с использованием нечеткой логики на базе инструментария Matlab / Е.К. Баранова, А.М. Гусев // Образовательные ресурсы и технологии. – 2016. – Т. 1, вып. 13. – С. 88–96.
15. ГОСТ Р 50922–2006. Защита информации. Основные термины и определения. – Введ. 2006-12-27. – М.: Изд-во стандартов, 2008. – 12 с.
16. Курносов К.В. Системный анализ угроз безопасности информации, обрабатываемой виртуальными инфраструктурами // Матер. 54-й Междунар. науч. студенческой конф. МНСК–2016. – Новосибирск: Новосиб. нац. исслед. гос. ун-т, 2016. – С. 32.

17. Курносов К.В. Модель идентификации угроз виртуальной инфраструктуры // Матер. VII Всерос. молодежной школы-семинара по проблемам информационной безопасности «Перспектива-2016». – Таганрог: ЮФУ, 2016. – С. 11–17.

18. Catteddu D. Cloud Computing Risk Assessment / D. Catteddu, G. Hogben et al. – Heraclion: Greece, 2009. – 125 p.

19. ГОСТ Р 56938–2016. Защита информации при использовании технологий виртуализации. – Введ. 2016-07-01. – М.: Изд-во стандартов, 2016. – 36 с.

20. Гришина Н.В. Организация комплексной системы защиты информации. – М.: Гелиос АРВ, 2007. – 256 с.

21. Камалова Г.Г. О способе отнесения сведений к информации ограниченного доступа // Вестник Удмурт. ун-та. – 2015. – Т. 25, вып. 2. – С. 107–111.

22. Караваев А.А. О «перечне сведений конфиденциального характера» в системе нормативно-правового регулирования конфиденциальной информации // Вестник Воронеж. гос. ун-та. – 2015. – Т. 3, вып. 16. – С. 155–160.

23. Ходаков В.Е. Оценка эффективности информационных систем по частным показателям / В.Е. Ходаков, В.Н. Козел // Научный журнал «Компьютерно-інтегровані технології: освіта, наука, виробництво». – 2017. – Т. 1, вып. 26. – С. 159–163.

24. Чипига А.Ф. Основы построения и системного анализа комплексных систем обеспечения информационной безопасности: учеб. пособие. – Ставрополь: СКФУ, 2014. – 198 с.

25. Нежданов И.Ю. Аналитическая разведка для бизнеса. – М.: Ось-89, 2008. – 336 с.

Курносов Кирилл Викторович

Аспирант каф. информационной безопасности (ИБ) Новосибирского государственного университета экономики и управления (НГУЭУ)
Каменская ул., 56, г. Новосибирск, Россия, 630099
Тел.: +7-913-753-21-81
Эл. почта: k.v.kurnosov@nsuem.ru

Kurnosov K.V.

Methodology for assessing the security of information systems built using virtualization technologies

Protecting virtual segments of information systems is an urgent problem for companies that use virtualization technologies. Ensuring information security of virtualization is one of the priority directions in the development of the IT market in Russia. In this paper, the existing methods for assessing security are analyzed and the new methodology for assessing the security of information systems built using virtualization technologies and developed taking into account the identified shortcomings in existing ones, is briefly described. The model the methodology is based on can be used to assess the security of a wider range of information systems.

Keywords: virtualization, virtual infrastructure, virtual machine, hypervisor, information security, virtualization vulnerabilities, threat identification, threat model.

doi: 10.21293/1818-0442-2019-22-1-37-44

References

1. Ledovskoj V.P. Overview of protection of virtual environments VMware vSphere. – Access mode: http://www.anti-malware.ru/analytics/Virtualization_Security_free (accessed: May 13, 2018) (in Russ.).

2. Gavrilov D. A. Russian Cloud Services Market 2017–2021 Forecast and 2016 Vendor Shares – Access mode: <http://idcrussia.com/ru/research/published-reports/65018-russian-cloud-services-market-2017-2021-forecast-and-2016-vendor-shares/2-abstract>, free (accessed: May 13, 2018) (in Russ.).

3. Virtual Security in The Data Center – Access mode: http://www.cisco.com/c/dam/en/us/solutions/collateral/data-center-virtualization/unified-fabric/tap_virtual_security_032012.pdf, free (accessed: May 13, 2018) (in Russ.).

4. The program «Digital economy of the Russian Federation»: approved by the order of the Chairman of the Government of the Russian Federation dated July 28. 2017, №1632-p, М., 2017, 88 p. (in Russ.).

5. Measures to protect information in state information systems: a methodological document of the FSTEC of Russia. М., 2017, 176 p. (in Russ.).

6. Methods for determining threats to the security of information in information systems: a draft methodological document of the FSTEC of Russia. Access mode: <https://fstec.ru/component/attachments/download/812> (accessed: May 13, 2018) (in Russ.).

7. Determination of actual threats to the security of personal data when they are processed in personal data information systems (IS): a methodological document of the FSTEC of Russia. Moscow, 2008, 10 p. (in Russ.).

8. Determination of actual threats to the security of information in key information infrastructure systems: a methodological document of the FSTEC of Russia (DSP). Approved. 2008-11-18 (in Russ.).

9. GOST R ISO / IEC 13335-3–2007. Methods and means of security. Part 3. Moscow, 2007, 49 p. (in Russ.).

10. Popov A.M., Zolotarev V.V., Bondar I.V. Methodology for assessing the security of an information system according to the requirements of standards of information security. *Computer Science and Control Systems*, 2010, vol. 4, no. 26, p. 3–12 (in Russ.).

11. Barabanov A.V., Markov A.S., Tsirlov V.L. Methodical apparatus for assessing the compliance of automated systems with information security requirements. *Special equipment and communication*, 2011, vol. 3, p. 48–53 (in Russ.).

12. Eremenko V.T., Rytov M.Yu., Gorlov A.P. Automating the process of assessing the state of protection of an informatization object using inhibitory, probabilistic and colored Petri nets from information leakage. *Information and Security*, 2015, vol. 18, no. 1, p. 123–126 (in Russ.).

13. Pletnev P.V., Belov V.M. Methodology for assessing information security risks in small and medium-sized enterprises. *Proceedings of TUSUR University*, 2012, vol. 1, no. 25, p. 83–86 (in Russ.).

14. Baranova E.K., Gusev A.M. Information security risk analysis technique using fuzzy logic based on Matlab tools. *Educational Resources and Technologies*, 2016, vol. 1, no. 13, p. 88–96 (in Russ.).

15. GOST R 50922–2006 «Information Security. Basic terms and definitions». М., 2008, 12 p. (in Russ.).

16. Kurnosov K.V. System analysis of threats to the security of information processed by virtual infrastructures // *Proceedings of the 54th International Scientific Student Conference ISSC–2016*, 2016, p. 32. (in Russ.).

17. Kurnosov K.V. Model of identifying threats to the virtual infrastructure. *Proceedings of the VII All-Russian Youth School-Seminar on Information Security Issues «Perspective 2016»*, Taganrog: SFU, 2016, p. 11–17 (in Russ.).

18. Catteddu D., Hogben G. et al. Cloud Computing Risk Assessment. – Heraclion: Greece, 2009, 125 p.

19. GOST R 56938–2016 «Information Security in the Use of Virtualization Technologies». M., 2016, 36 p. (in Russ.).

20. Grishina N. Organization of an Integrated Information Protection System. Moscow, Helios ARV, 2007, pp. 60–66 (in Russ.).

21. Kamalova G.G. On the method of attributing information to the information of limited access. *Bulletin of Udmurt University*, 2015, vol. 25, no. 2, pp. 107–111 (in Russ.).

22. Karavayev A.A. On the «list of confidential information» in the system of regulatory and legal regulation of confidential information. *Bulletin of Voronezh State University*, 2015, vol. 3, no. 16, p. 155–160 (in Russ.).

23. Khodakov V.E., Kozel V.N. Evaluation of the effectiveness of information systems on private indicators. *Scientific journal «Computer-integrated technologies: science and technology»*, 2017, vol. 1, no. 26, p. 159–163 (in Russ.).

24. Chipiga A.F. Basics of building and system analysis of integrated information security systems: studies. Manual. – Stavropol: SKFU, 2014, 198 p. (in Russ.).

25. Nezhdanov I.Yu. Analytical intelligence for business. Moscow, Os-89, 2008, 336 p. (in Russ.).

Kirill V. Kurnosov

Graduate student of Novosibirsk State University
of Economics and Management (NSUEM)
56, g, Kamenskaya st., Novosibirsk, Russia, 630099
Phone: +7-913-753-21-81
Email: k.v.kurnosov@nsuem.ru