DOI 10.37882/2223-2966.2026.02-2.11

РАЗРАБОТКА МЕР ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ВИРТУАЛЬНЫХ МАШИН

DEVELOPMENT OF INFORMATION SECURITY MEASURES FOR VIRTUAL MACHINES

V. Egorov
K. Lazunin

Summary. This article examines security issues in virtualization environments and models attacker actions against the hypervisor. Current threats and countermeasures are analyzed. A security analysis of the correct operation of the hypervisor is provided. Proposals for improving hypervisor security were formulated. An analysis of hypervisor components was conducted. Concepts of interaction between entities were introduced to formulate an approach to hypervisor security. The need for a rigorous mathematical model has been identified. Information security measures for virtual machines have been defined.

Keywords: information security, hypervisor, information security in virtualization environments.

Егоров Валерий Юрьевич
кандидат технических наук, доцент, ФГБОУ ВО «Пензенский государственный университет»
vec@mail.ru.
Лазунин Константин Александрович
старший преподаватель, ФГБОУ ВО «МИРЭА — Российский технологический университет»
07121917@mail.ru

Аннотация. Рассмотрены проблемы безопасности среды виртуализации, смоделированы действия нарушителя в отношении гипервизора. Рассмотрены действия нарушителя в отношении гипервизора. Проведен анализ актуальных угроз и методов противодействия. Проведен анализ безопасности применения корректной работы гипервизора. Сформированы предложения по необходимости совершенствования безопасности гипервизора. Проведен анализ компонентов гипервизора. Введены понятия взаимодействия между субъектами для формирования подхода по безопасности гипервизора. Сформулирована необходимость формирования строгой математической модели. Определены меры информационной безопасности для виртуальных машин.

Ключевые слова: информационная безопасность, гипервизор, защита информации среды виртуализации.

Применение среды виртуализации в современных условиях является неотъемлемой частью построения кластеров центров обработки данных, государство обеспечивает развитие облачных технологий и построение государственной единой облачной платформы в целях размещения информационных систем и информационных ресурсов [1].

Стоит отметить, что к средствам виртуализации регуляторами в области информационной безопасности уделяется большое внимание, разрабатываются соответствующие гипервизоры, однако вопрос построения комплексной безопасности на системном уровне до конца не изучен.

По настоящее время остаются актуальными угрозы в отношении гипервизора [2, 3]. Злоумышленник, получив административный доступ к гостевой виртуальной машине, может воздействовать на виртуальные аппаратные устройства гипервизора с целью внесения ошибок в его работу.

В случае успеха злоумышленник может повлиять на работоспособность виртуальной аппаратуры, обслуживающей не только виртуальную машину, на которой расположился злоумышленник, но и другие ВМ в составе хостового компьютера.

Рассмотрим, в качестве образца, виртуальную клавиатуру PS/2, которая имеется в наличии любого стандартного гипервизора. На этапе загрузки ОС с этой аппаратурой взаимодействует Firmware (BIOS или EFI загрузчик операционной системы). С помощью виртуальной клавиатуры происходит выбор загрузочных опций.

Рассмотрим средства ввода данных с клавиатуры. Работой клавиатуры управляет контроллер клавиатуры, который при нажатии или отпускании любой клавиши выполняет две функции:

- помещает в свой выходной порт с номером 60h скан-код клавиши;]
- посылает процессору через контроллер прерываний сигнал, инициирующий запуск программы обработки аппаратного прерывания от клавиатуры (прерывание INT 09h в стандартном Legacy BIOS).

Скан-код является порядковым номером клавиши и однозначно ее идентифицирует. Каждая клавиша имеет два скан-кода, которые отличаются на величину 80h:

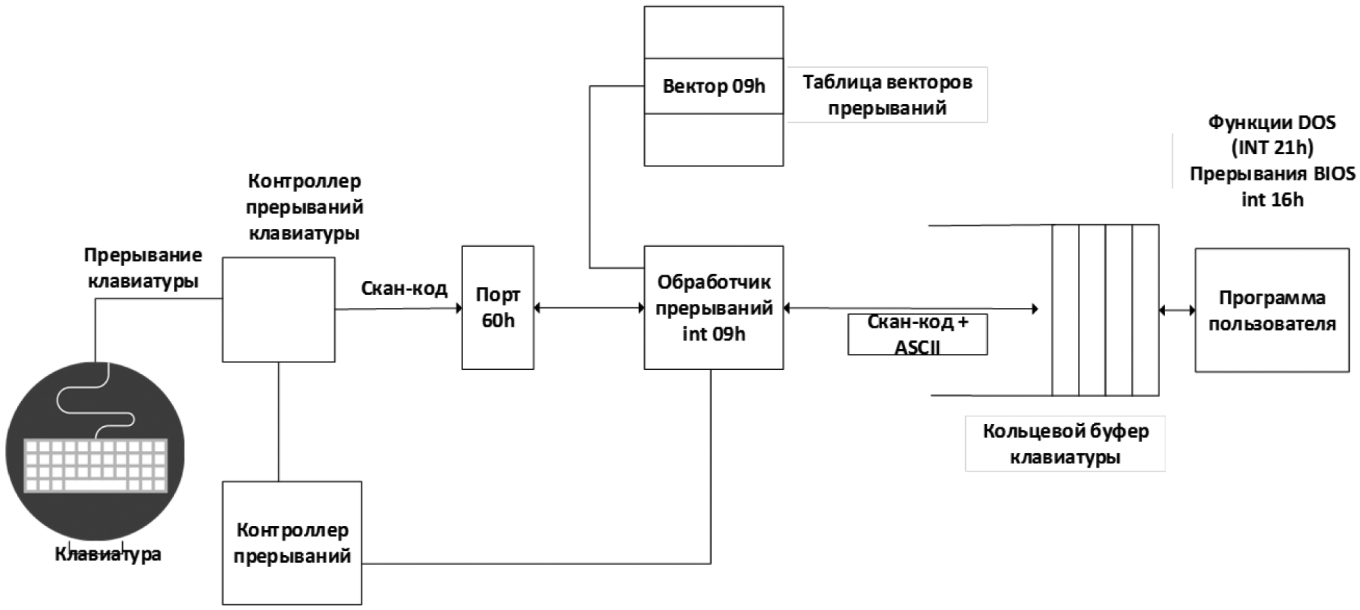

Рис. 1. Структурная схема клавиатуры

меньший — код нажатия

больший — код отпускания.

На рисунке №1 представим структурную схему клавиатуры.

Слова флагов клавиатуры:

1. Занимает байты памяти 40h:17, 40h:18h;
2. Показывает состояние служебных клавиш:

— если клавиша нажата, то соответствующий бит равен 1;
— если клавиша отпущена, то соответствующий бит равен 0.

Расположение битов клавиш в слове флагов клавиатуры:

Байт 40h:17h,
Биты
7 — insert;
6 — Caps Lock;
5 — Num Lock;
4 — Scroll Lock;
3 — Alt;
2 — Ctrl;
1 — Left Shift;
0 — Right Shift.
Байт 40h:18h,
Биты
7 — SysRq;
6 — Caps Lock;
5 — Num Lock;
4 — Scroll Lock;
3 — Right Alt;
2 — Right Ctrl;
1 — Left Alt;
0 — Left Ctrl.

Обработчик прерывания INT 09h считывает из порта 60h скан-код и анализирует его значение. Если скан-код принадлежит служебным клавишам, то в слове флагов клавиатуры при нажатии соответствующие биты, а при отпускании сбрасываются. Если нажать на любую другую клавишу, INT 09h формирует двухбайтовый код, который представляет собой скан-код, ASCII-код. Происходит запись двухбайтового кода в кольцевой буфер ввода клавиатуры. В свою очередь, кольцевой буфер имеет объем 15 слов, размещается в памяти, которая начинается с адреса 40h:1Eh и предназначена для синхронизации аппаратного ввода данных, а также приема их программной пользователя. Программа пользователя, использует прерывание BIOS int 16h, также могут быть использованы системные функции DOS. Программа пользователя, пытается считать символы из кольцевого буфера. Наличие символов подтверждает операцию ввода их и обрабатывает в последствии.

В таком виде всё работает, если используется стандартный загрузчик операционной системы. При наличии злоумышленника в составе виртуальной машины, стандартный загрузочный код подменяется вредоносным ПО, цель которого: нарушить работоспособность виртуальной клавиатуры. Так, например, злоумышленник начинает воздействовать на порты виртуальной клавиатуры (60h, 61h) иным способом, не предусмотренным стандартным алгоритмом взаимодействия между аппаратурой и драйвером.

Смоделируем действия нарушителя в отношении драйвера модуля аппаратной виртуализации на примере работы клавиатуры.

Действие нарушителя № 1 — развертывание подготовленного образа в гипервизоре, представляющий собой операционную систему с вредоносным программным обеспечением. Фактически создается новая виртуальная машина в гипервизоре.

Действие нарушителя № 2 — получение доступа к драйверу модуля аппаратной виртуализации.

Действие нарушителя № 3 — создание условий по воздействию на драйвер модуля аппаратной виртуализации по средству команд/запроса приводящего к нарушению доступности и целостности всего гипервизора.

Эти действия позволят негативно воздействовать на гипервизор, что нарушит работу системы в целом, такие последствия могут значительно негативно воздействовать на информационную инфраструктуру и в результате может привести к нарушению работы государственных систем.

Необходимо рассмотреть возможность совершенствования безопасности информационных систем, позволяющей противодействовать угрозам гипервизора, разработать методику позволяющую создавать систему в защищенном исполнении в условиях непреднамеренного воздействия на среду функционирования.

В современных информационных инфраструктурах применяются современные гипервизоры, которые позволяют создавать гипкую архитектуру для развертывания информационных систем на одном физическом ресурсе.

Однако отмечаются значительные угрозы информационной безопасности, которые могут повлечь нарушение целостности, конфиденциальности и доступности гипервизора, такие как: Угроза выхода за пределы виртуальной машины несет возможные последствия влекущие несанкционированный доступ к ресурсам средства виртуализации. Угроза несанкционированного доступа к ресурсам виртуальной машины пользователем другой виртуальной машины, влекущие возможные последствия распространение вредоносного программного обеспечения в гипервизоре, а также получение несанкционированного доступа к данным. Угроза несанкционированного доступа к гипервизору, влекущий несанкционированный доступ к данным [4].

Анализ современных атак и уязвимостей свидетельствует о необходимости усиления требований по безопасности [5, 6]. В таблице №1 представлены способы реализации угроз на гипервизор в соответствии с банком данных угроз безопасности информации ФСТЭК России [7].

В гипервизоре реализуется взаимодействие между субъектами, которые могут требовать выполнение опе-

Таблица 1.

Способы реализации угроз на гипервизор в соответствии с банком данных угроз безопасности информации ФСТЭК России

	Способы реализации угроз в отношении гипервизора
1.	Эксплуатация известных уязвимостей
2.	Эксплуатация уязвимостей «нулевого дня»
3.	Использование недостатков, связанных с неполнотой проверки вводимых (входных) данных
4.	Использование недостатков, связанных с управлением учетными данными
5.	Использование недостатков, связанных с отсутствием проверки достоверности отправителя и/или получателя
6.	Использование недостатков, связанных с хранением ключевой информации в программном коде (в оперативной памяти)
7.	Использование недостатков, связанных с использованием нестойкой криптографии
8.	Использование недостатков, связанных с некорректной настройкой сетевого доступа
9.	Использование недостатков конфигурации, связанных с настройками по умолчанию (включая пароли по умолчанию)
10.	Использование недостатков, связанных с некорректной настройкой прав доступа
11.	Внедрение вредоносного программного обеспечения через скомпрометированные обновления программного обеспечения или операционной системы
12.	Внедрение закладок в системное программное обеспечение
13.	Идентификация пользователей
14.	Получение данных о пользователях и группах
15.	Получение данных о процессах
16.	Получение данных о настройках безопасности
17.	Блокировка пользователей
18.	Множественный запуск программного обеспечения
19.	Выход за пределы виртуальной инфраструктуры
20.	Перебор паролей к учетной записи
21.	Перебор пользователей к паролю (Password Spraying)
22.	Перебор утекших пар пользователь/пароль (Credential Stuffing)
23.	Восстановление аутентификационной информации из журналов приложений
24.	Доступ без авторизации
25.	Использование ошибок или отсутствия проверки прав доступа

раций посредством передачи команд, что позволяет атакующему воздействовать на его компоненты такие как адресное пространство памяти, адресное пространство ввода-вывода, адресное пространство шин PCI и другая виртуальная аппаратура, понуждая субъект назначения к реализации угрозы.

Введем понятие «последовательность операций» как набора действий, выполняемых субъектом на основе полученных команд от других субъектов.

Введем понятие «валидная последовательность операций», как последовательность операций, допустимая при работе виртуальной машины и не проводящая к ухудшению параметров работоспособности субъектов. Все операции, не являющимися валидными, объявляются невалидными, то есть запрещенными.

Определим, что виртуальные устройства могут требовать выполнения операций другими устройствами только посредством процессоров, а не напрямую. Все операции между виртуальными устройствами, осуществляются напрямую, являются невалидныими.

Для анализа безопасности и корректности работы гипервизора требуется строгая математическая модель, описывающая:

— множество субъектов (процессоров и виртуальных устройств);
— доступные им адреса пространства как каналы взаимодействия;
— операции, которые субъекты могут инициировать и принимать;
— последовательность операций, реализующие алгоритмы работы ВМ;
— критерии валидности и невалидности этих последовательностей.

Обмен командами между субъектами осуществляется через адресные пространства, представляемые аппаратной и программной конфигурацией компьютера. Необходимо ввести множество адресных пространств:

Состояние может включать:

— значения регистров процессора;
— конфигурацию виртуального устройства;
— содержимое внутренних буферов и очередей;
— параметры, связанные с производительностью и допустимостью.

Интерпретация: последовательность операций представляет собой алгоритм работы субъекта (или совокупности субъектов) в рамках функционирования виртуальной машины. Тем самым должно исключаться:

— состояния сбоя и зависания;
— некорректные конфигурации;
— состояния с недопустимой деградацией производительности.

То есть для любой валидной последовательности запрещено существование операции, у которой источником и назначением одновременно являются виртуальные устройства.

Предлагаемый подход позволит задать строгую математическую основу для анализа безопасности гипервизора. На его базе возможно решение следующих задач:

— контроль доступа.
— верификация гипервизора.
— защита виртуальных машин.
— противодействие атакам.
— отказоустойчивость.
— статический и динамический анализ.

Возможно предложить формальную модель взаимодействия субъектов гипервизора на основе теории множеств.

Необходимо особое внимание уделить ограничениям на взаимодействие виртуальных устройств и требованиям к корректности состояний субъектов. Это создаст основу для дальнейшей формальной верификации гипервизоров, построения моделей безопасности и нарушителя и разработки методов автоматизированного анализа безопасности гипервизора.

ЛИТЕРАТУРА

1. Правительство Российской Федерации Постановление от 10 июля 2024 г. № 929 «Об утверждении Положения о государственной единой облачной платформе» // Официальный сайт Правительства Российской Федерации [Электронный ресурс] URL http://static.government.ru/media/files/cA6wM8fMQGuFv294tfPEumfAVAVGKvTf.pdf/.
2. Darshan Tank, Akshai Aggarwal, Nirbhay Kumar Chaubey. — Virtualization vulnerabilities, security issues, and solutions: a critical study and comparison, International Journal of InformationTechnologyAn Official Journal of BharatiVidyapeeth's Institute of ComputerApplications and Management [Электронный ресурс] https://www.researchgate.net/, ISSN 2511-2104, 2019.
3. Francesco Gadaleta, Nick Nikiforakis, Yves Younan, and Wouter Joosen — Hello rootKitty: A lightweight invariance-enforcing framework // Information Security 14th International Conference, ISC 2011, Xi'an, China, October 26–29, 2011, Proceedings [Электронный ресурс] https://www.researchgate.net/, 2011.
4. Фомин Юрий Сергеевич, Алтынбаев Артур Фларитович, Тарануха Александр Васильевич Целостность, доступность, конфиденциальность виртуализации и контейнеризации // Парадигма. 2025. №5-5. URL: https://cyberleninka.ru/article/n/tselostnost-dostupnost-konfidentsialnost-virtualizatsii-i-konteynerizatsii (дата обращения: 25.12.2025).
5. Pan G. et al. Breaking Isolation: A New Perspective on Hypervisor Exploitation via Cross-Domain Attacks //arXiv preprint arXiv:2512.04260. — 2025.
6. Lee J. et al. {BOOTKITTY}: A Stealthy {Bootkit-Rootkit} Against Modern Operating Systems //19th USENIX WOOT Conference on Offensive Technologies (WOOT 25). — 2025. — С. 303–320.
7. Банк данных угроз безопасности информации // БДУ — Компоненты объектов воздействия. URL: https://bdu.fstec.ru/threat-section/components (дата обращения: 13.01.2025).