4. Изоляция пользователей. Использование индивидуальной виртуальной машины и виртуальную сеть. Виртуальные сети должны быть развернуты с применением таких технологий, как VPN, VLAN и VPLS. Часто провайдеры изолируют данные пользователей друг от друга за счет изменения данных кода в единой программной среде. Данный подход имеет риски, связанные с опасностью найти дыру в нестандартном коде, позволяющему получить доступ к данным. В случаи возможной ошибки в коде пользователь может получить данные другого.

Фундаментальный и многосторонний анализ рисков для информационной безопасности является неотъемлемой предпосылкой разработки и сопровождения успешных и эффективных мер по защите информации в условиях облачных вычислений.

Несмотря на все достоинства облачных вычислений, на сегодняшний день потребителям необходимо взвешенно подходить к их внедрению, органично сочетать традиционные (локальные) и облачные инфраструктуры в организации вычислительного процесса.

ЛИТЕРАТУРА

1. Checkpoint [Электронный ресурс] – 2021. – Режим доступа: https://www.check-point.com/cyberhub/cloudsecurity/whatiscloudsecurity/topcloudsecurityissuesthreatsandconcerns/. – Дата доступа: 29.03.2021.

2. Phoenixnap [Электронный ресурс] – 2021. – Режим доступа: https://phoe-nixnap.com/blog/whatiscloudsecurity. – Дата доступа: 29.03.2021.

3. Habr [Электронный ресурс] – 2021. – Режим доступа:https://habr.com/ru-/company/cloud4y/blog/500866/. – Дата доступа: 29.03.2021.

УДК 004.056.53

Студ. Д.И. Леонов
Науч. рук. преп.-стаж. А.Д. Томко
(кафедра информационных систем и технологий, БГТУ)

О РАССТАНОВКЕ СИЛ В SECURITY-СООБЩЕСТВЕ И О КАРТЕ СРЕДСТВ САМОЗАЩИТЫ ЯДРА LINUX

Чего мы ждем от современной операционной системы. Без сомнений – это удобность в использовании, быстродействие и, конечно же, одним из главных критериев является безопасность. Безопасность – это то, что обеспечивает нам защиту от вирусов, комфортное пребы-

вание в интернете и позволяет меньше думать о том, как защитить свои файлы.

Одна из главных проблем всех ОС – это обеспечение безопасности пользователей. И вот как разработчики Linux справились с этим:

Проект Kernel Self-Protection Project (KSPP). Идея проекта состоит в том, что безопасность операционной системы – это больше, чем просто исправление ошибок в коде и разделение доступа к ресурсам. Операционная система должна отрабатывать безопасно в случае ошибки или попытки атаки. Поэтому KSPP ставит своей задачей устранение в ванильном ядре Linux целых классов уязвимостей и методов их эксплуатации.

Безопасность и расстановка сил security-сообщества ОС Linux осуществляется с помощью различных механизмов: MAC, DAC и т. д.

DAC (Discretionary Access Control) – избирательная модель, предоставляющая доступ на чтение, запись, выполнение.

SE Linux или Security Enhanced Linux – это улучшенный механизм управления доступом для предотвращения злонамеренных вторжений.

LSM – Linux Security Model, это фреймворк, который позволяет ядру Linux поддерживать различные модели компьютерной безопасности. LSM в первую очередь ориентирована на поддержку модулей контроля доступа. LSM впервые была включена в версию Linux2.6 в декабре 2003 года и стала дополнением к существующей системе безопасности Security Enhanced Linux.

Осталось узнать, как собственно работает вся эта система безопасности. Например, пользователь выполняет над объектом какое-либо разрешенное действие после DAC проверки. Этот запрос на выполнение операции попадает к перехватчику событий LSM. Оттуда он поступает на SE Linux. Далее на SE Linux поступают данные о том, возможно ли вообще данному пользователю выполнять операцию над данным файлом.

Для того, чтобы узнать о возможности доступа SE Linux обращается к AVC (Access Vector Cache). Если никаких ошибок не возникает, то пользователю предоставляется доступ к файлу.

Именно с помощью таких действий была решена проблема с безопасностью ОС Linux. Операционная система Linux, предоставляет безопасное пользование и пребывание в сети.

ЛИТЕРАТУРА

1. ПроектKernelSelf-ProtectionProject (KSPP) [Электронный ресурс]– 2021. – Режим доступа: https://kernsec.org/wiki/index.php/Kernel_Self_Protection_Proje-ct. – Дата доступа: 29.03.2021