ПОСТРОЕНИЕ ЗАКРЫТОГО УЧАСТКА ИНФРАСТРУКТУРЫ С ЦЕЛЬЮ ОБЕСПЕЧЕНИЯ ПОЛЬЗОВАТЕЛЕЙ БЕЗОПАСНОЙ ТЕСТОВОЙ ВИРТУАЛЬНОЙ СРЕДОЙ

Институт информационных технологий БГУИР,
г. Минск, Республика Беларусь

Петрович А.С., Думиков А.А.

Бакунова О.М. – ст. преподаватель каф. ИСиТ, м.т.н.
Бакунов А.М., ст. преподаватель каф. ИСиТ, м.т.н.
Калитеня И.Л. – ассистент каф. ИСиТ, м.т.н.

Одной из самых сложных задач инженерии является создание такой системы, которая одновременно надежна и эффективна. В работе рассмотрены особенности решения инженерных задач, реализуемых в закрытых зонах, в так называемых песочницах, на примере средства автоматизации развертывания виртуальных машин.

В древности словом «инженер» называли создателя военных машин; в средние века — создателя мостов, иных сооружений; современное понимание термина «инженер» возникло после Первой мировой войны, когда словом «инженер» стали называть создателей комплексов и систем различного назначения.

Примерно в то же время возникло понятие «инфраструктура». Оно обозначало комплекс сооружений, созданный для поддержки военных сил, однако в скором времени понятие «инфраструктура» получило более широкое значение и стало обозначать комплекс взаимосвязанных структур и объектов обслуживающего назначения, обеспечивающих функционирование системы.

В области информационных технологий инфраструктурой называют комплекс вычислительных, телекоммуникационных и программных средств, которые предоставлены сотрудникам для выполнения различных рабочих задач.

Для администраторов компьютерных систем и сетей одной из самых сложных задач является создание надежной инфраструктуры.

Одним из способов решения данной задачи является разделение заданной сети на несколько подсетей различного функционального назначения, сообщение между которыми осуществляется по заданным правилам. Простейший пример — разделение сети предприятия на пользовательскую и серверную подсети.

К правилам сообщения между подсетями относят правила маршрутизации и фильтрации сетевого трафика. Разумный выбор этих правил может значительно повысить безопасность сети. Например, можно допустить к работе с серверной сетью лишь отдельные сетевые адреса, уменьшая таким образом риск несанкционированного доступа.

Однако данный способ не подходит в случаях, когда произвольному числу пользователей необходим доступ к произвольному числу серверов. Тогда наиболее эффективным способом обезопасить сеть является выделение в серверной подсети так называемой «демилитаризованной зоны».

Демилитаризованная зона — буфер между наиболее важными серверами и пользовательской подсетью. Получение злоумышленником доступа к серверам демилитаризованной зоны не может привести к серьезным последствиям для инфраструктуры в целом, т.к. не дает злоумышленнику никаких прав в серверной подсети. Согласно примерным подсчетам, выделение демилитаризованной зоны в сети позволяет уменьшить стоимость инфраструктуры в 4 раза за счет сокращения расходов на отдельные отказоустойчивые серверы для наиболее важных систем, расходов на проведение балансировки нагрузки, регулярного резервного копирования и т.п.

Однако существует и другой способ. Он предлагает выделение закрытой подсети, которая функционирует независимо от демилитаризованной зоны. Такую подсеть называют «песочницей».

Песочница не проверяется и не контролируется системным администратором. Размещение в песочнице важных данных и систем запрещается административно. Работа с песочницей организуется таким образом, что любые данные и системы, которые в ней размещены, могут быть уничтожены в любой момент без последствий для инфраструктуры в целом и демилитаризованной зоны в частности.

Поэтому тестируемые в песочнице программные средства должны разрабатываться с использованием методов непрерывной поставки и интеграции, которые позволяют хранить код на одном носителе, а выполнять на другом. В этом отношении эталоном является такое программное средство, тестирование которого в песочнице требует меньше времени, чем получение несанкционированного доступа к ней, или такое, что несанкционированный доступ не может оказать на него негативных последствий.

Дополнительной линией защиты может служить физическое выделение песочницы в отдельную сеть. Для этого необходимы отдельный сервер и интернет-канал, посредством которого будет осуществляться доступ к песочнице из основной сети.

Принцип работы песочницы на примере средства автоматизации развертывания виртуальных машин «SelfPortal» изображен на рисунке 1.

Получение доступа к ресурсам песочницы сопряжено с рядом затруднений. Чтобы разъяснить это, условно разделим виртуальные машины по признаку используемой операционной системы:

1. Виртульные машины с ОС семейства Windows.
2. Виртуальные машины с ОС семейства Unix.
3. Виртуальные машины с другими операционными системами.

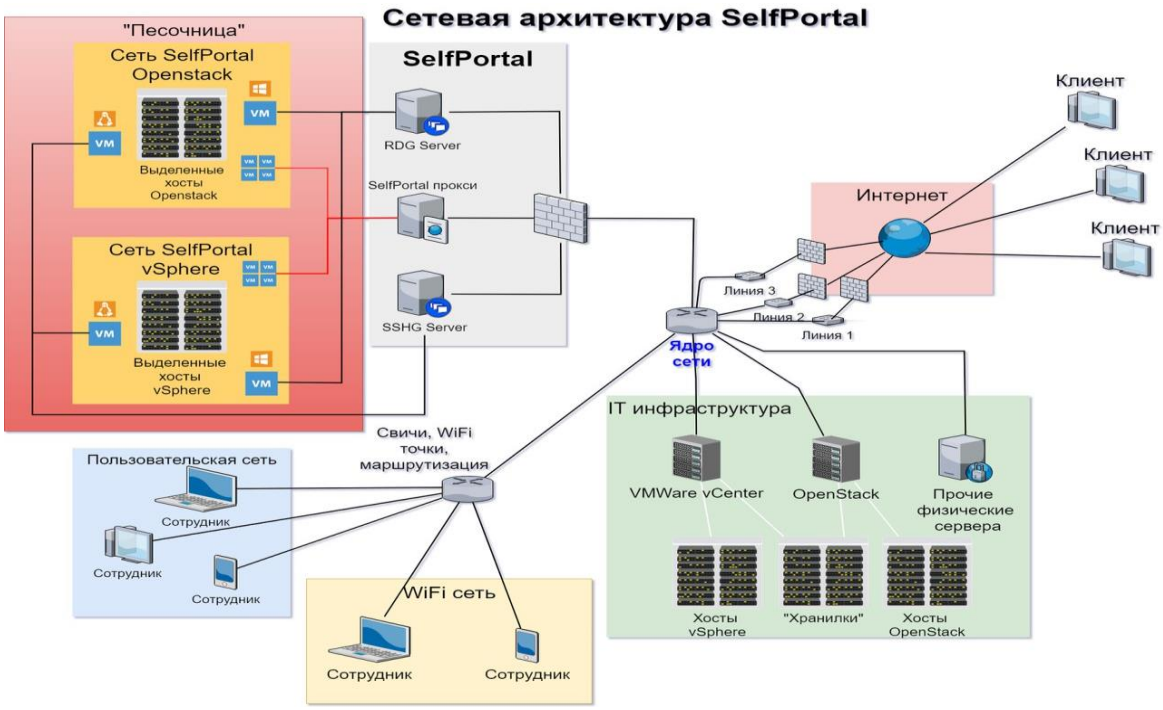

Рисунок 1 – Принцип работы песочницы на примере ПС «SelfPortal»

Это деление удобно в приложении к методам, которые позволяют получить доступ к системе. Например, основным способом доступа к виртуальным машинам категории 1 является Remote Desktop Protocol, тогда как для машин категории 2 — Secure Shell или Virtual Network Computing.

NoVNC Viewer является частью программного пакета, предоставляемого непосредственно системой виртуализации как инструмент контроля над виртуальной машиной. Его невозможно централизовать, так что общее число «входных точек» в песочницу будет равно числу используемых провайдеров виртуализации плюс два.

Поэтому необходимо строго настроить брандмауэр, чтобы запретить любой трафик, не прошедший через заданные системы. Кроме того, следует блокировать любой трафик, созданный данными системами, чтобы предотвратить доступ к основной сети предприятия злоумышленником, который получил возможность пользоваться ими. Такие меры обеспечивают сотрудникам предприятия качественно новый уровень сервиса.

Отметим в заключение, что описанная методика не принесет экономической выгоды предприятиям, которые не предоставляют сотрудникам непосредственным доступ к инфраструктуре, поскольку тогда любой виртуальный сервер будет проверяться системным администратором, так что сложные защитные меры по организации песочницы становятся лишними. Вместе с тем для предприятий, которые непосредственно выделяют сотрудникам вычислительные ресурсы, данная методика может стать инновационным решением.

МОДЕЛИ И АЛГОРИТМЫ ОБЕСПЕЧЕНИЯ НЕОБХОДИМЫМИ РЕСУРСАМИ ДЛЯ ЖИЗНЕДЕЯТЕЛЬНОСТИ ЧЕЛОВЕКА НА ОСНОВЕ ТЕОРИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Институт информационных технологий БГУИР,
г. Минск, Республика Беларусь

Поплёвка В.И.

Скудняков Ю.А.- доцент каф. ПЭ, к.т.н,, доцент

В работе рассматриваются возможности использования некоторых подходов и предложенных в ней моделей и алгоритмов обеспечения необходимыми ресурсами для жизнедеятельности человека на основе теории искусственного интеллекта [1,2].

Для формирования поведения человека наиболее подходящим является игровой искусственный интеллект, так как он позволяет задавать алгоритмы объекта в зависимости от текущего состояния системы.
При формировании игрового искусственного интеллекта используют следующие подходы [3]:

1.Машины конечных состояний

Машины конечных состояний являются наиболее распространенным алгоритмом поведенческого моделирования. Они концептуально просты и быстро кодируются, что приводит к созданию мощной и гибкой структуры искусственного интеллекта с небольшими расходами. Машины разбивают искусственный интеллект на