Содержание

8 (952) 106-88-60 vk.com/a.projectit a.projectit

Введение

Актуальность исследования

На протяжении последних пятидесяти лет информационные технологии постоянно претерпевали кардинальные изменения. Все началось с огромных ламповых ЭВМ, впоследствии эволюционировавшие в компактные современные персональные компьютеры, которые превышают мощность первых в десятки миллионов раз. Инженерная мысль постоянно развивалась, ЭВМ становились все более технологичными, компактными и соответственно более массовыми, ими стало проще управлять. Их стали устанавливать везде в офисах, предприятиях, заводах, медицинских учреждениях и наступил тот момент, когда стало просто необходимо обмениваться информацией между двумя компьютерными системами. Решением стало создание распределенных компьютерных систем. Причем необязательно, что РКС должна ограничиваться только зданием, районом города или даже городом. Достаточно подключить РКС к сети Интернет и появляется возможность обмена информацией между разными частями мира. Внедрение РКС в деятельность организаций резко повысило эффективность информационной составляющей и экономическую отдачу, но в то же время становится и уязвимым местом, которое привлекает злоумышленника [93].

Распределенная компьютерная система – это набор независимых компьютеров, представляющийся их пользователям единой объединенной системой. У распределенных систем есть несколько особенностей: пользователи не замечают различий в архитектурах их компьютеров и в способах их связи, в том числе это относится и к внешней организации РКС; РКС должна быть легко масштабируема, что вытекает из определения – компьютеры независимы и не важно, каким способом они взаимодействуют [86].

Вследствие особенностей РКС и того, что они эффективны в плане обмена информацией на них осуществляется множество атак. Например, в отчете компании QratorLabs за 2013 год был отмечен рост на РКС примерно на 34%, причем чтобы

организовать атаку типа DNSAmplification (дословно DNS усиление) пропускной способностью около 160 Гбит/с достаточно всего около 7-10 серверов средней мощности. Именно данный способ атаки стал наиболее популярным в 2013 году. Суть этой атаки заключается в том, что злоумышленник посылает короткий запрос уязвимымDNS-серверам, а те в свою очередь отвечают пакетами, которые гораздо больше по размеру. Если при отправке коротких запросов использовать IP-адрес компьютера жертвы, например с помощью IP-спуфинга, то DNS-серверы будут слать ненужные ему пакеты, пока полностью не парализуют его работу. Если в случае жертвы будет сервер некоторой РКС предприятия, то это парализует нормальную его работу [1, 46].

Из отчета компании «Лаборатория Касперского» за август 2014 года можно понять, что уязвимым местом РКС может стать не сервер, а рядовая клиентская машина. В отчете рассказан случай, когда сотрудник европейского банка зашел на зараженный сайт. Ничего неподозревающему сотруднику злоумышленниками на компьютер было установлено вредоносное ПО посредством «drive-by» загрузки. Вредоносное приложение работало в фоновом режиме одновременно с легитимной сессией онлайн-банкинга. Вредоносное ПО искало в системе онлайн-банкинга учетные данные клиентов, которые затем использовались для проверки баланса жертвы и проведения вредоносных транзакций. Краденые средства переводились на заранее подготовленные счета. Всего же от данных действий пострадали около 190 человек, всего было украдено около 500 000 евро, реальная сумма неизвестна [1, 46].

Росту количества атак РКС способствует огромное количество факторов: ошибки в проектировании РКС, т.е. в архитектуре, в использовании оборудования, уПО которого нет цифровой подписи разработчика, не квалифицированные сотрудники, экономия руководства компании на отдел ИБ. Чтобы эффективно противодействовать атакам, необходимо проанализировать особенности каждого типа атак. Как правило, эти особенности связаны с характеристиками самих злоумышленников (субъектов), которые осуществляют деструктивные

информационные воздействия, и распределенных компьютерных систем (объектов), на которые направлены эти действия [83].

Всплеск многообразия компьютерных платформ и программного обеспечения приводит только к увеличению уязвимостей РКС и повышает требования к средствам защиты. Установка на компоненты РКС стандартных средств защиты, таких как антивирусов, межсетевых экранов, средств защиты от НСД, виртуальных частных сетей и т.д. является необходимым, но уже не достаточным условием для поддержания необходимого уровня безопасности [57].

Наиболее распространенной операционной системой для ЭВМ является Windows. Именно поэтому злоумышленники выбирают «жертвами» компьютеры, на которых установлена данная операционная система. В организациях и гос. учреждениях в компонентах (терминалы, клиентские компьютеры и серверы) своих сетей используют именно Windows. С одной стороны простота в использовании для рядовых сотрудников, с другой стороны качественная техническая поддержка. Нопо данным компании McAfee каждый день появляются около 10000 нового вредоносного ПО. Чтобы обезопасить себя от него, недостаточно просто установить средство защиты, так же необходимо постоянно проводить его грамотную настройку. Но существуют атаки, вероятность реализации которых нельзя приблизить к нулю.

В связи с этим необходимо снижать уровень риска РКС от реализации различных атак и в итоге минимизировать ущерб от деструктивных действий на ресурсы системы. В данной ситуации основополагающей процедурой является управление рисками и живучестью РКС, которые включают в себя и риск-анализ, при помощи которых становится возможным всесторонне исследовать РКС организации, выявить уязвимые места в системе защиты, оценить текущее состояние ИБ, проверить правильность подбора оборудования, средств защиты и их защиты.

Исходя из всего вышесказанного, можно сделать вывод, что выбранная тема дипломной работы на сегодняшний день является весьма актуальной.

Объектом исследования являются РКС, в отношении которых реализуются УАОС Windows, оказывающие деструктивное воздействие на субъекты защищаемой РКС.

Предметом исследования являются способы реализации УАОС Windows, имитационные модели, риск моделирование и оценка рисков РКС, а также параметры влияющие на живучесть РКС, при рассматриваемых атаках.

Цель исследования состоит в определении основных способов реализации УАОС Windows РКС, а так же создание имитационных моделей и разработка методики по управлению живучести РКС, в условиях данных атак.

Для реализации цели необходимо решить следующие **задачи**:

1. Проверка, уточнение и унификация ранее разработанных риск-моделей УАОС Windows;
2. Разработка программного обеспечения и осуществление численного моделирования по выше уточнѐнным моделям атак на РКС;
3. Выработка рекомендаций практического управления рисками при УАОС Windows РКС и их реализация на примерах.

Степень обоснованности научных положений, выводов и рекомендаций, сформулированных в дипломной работе, обеспечивается корректным использованием математических методов в приложении обозначенному предмету исследования.

В исследовании используются методы численные методы расчета и анализа, методы теории рисков, методы математического моделирования, теории графов, теории вероятности, элементы теории сложных систем, математической статистики и системного анализа.

Научная новизна результатов исследования заключается в следующем:

1. В отличие от аналогичных работ, при исследовании атак на распределенные компьютерные системы учитывался уровень автоматизации реализации атаки и способ распространения вредоносного программного обеспечения, с помощью которого производится атака, а так же была введена расширенная классификация нарушителя;
2. Впервые разработаны имитационные модели выбранных УАОС Windows.

Практическая ценность работы заключается в том, что:

1. Анализ механизмов реализации атак в организациях, использующих в своей работе распределенные компьютерные системы, позволяет обнаружить наиболее уязвимые и опасные места для атаки в конкретно взятой системе и на основании этих результатов построить более совершенную риск-модель.
2. Полученные имитационные модели могут быть использованы в организациях для создания систем, устойчивых к атакам и выявлению наиболее уязвимых элементов РКС.
3. Предложенные рекомендации по управлению рисками и живучестью позволяют снизить риски для наиболее уязвимых компонентов РКС, что повышает уровень защищенности системы в целом.

8 (952) 106-88-60 vk.com/a.projectit a.projectit

ЗАКЛЮЧЕНИЕ

1. Построены аналитические модели процессовУАОС семейства Windows версииXPи вышераспределенных компьютерных систем. Данные модели позволяют определить вероятности успешного осуществления атаки.

2. Получены вероятности успешного совершения УАОС семействаWindows версииXPи вышераспределенных компьютерных систем в зависимости от описанных классов нарушителя и для каждой описанной конфигурации системы.

3. Построены риск-модель для УАОС семейства Windows версииXPи выше распределенных компьютерных систем.

4. Предложены меры по управлению живучестью распределенных компьютерных систем, находящихся в условиях УАОС семейства Windows версииXPи выше.

5. Проведена оценка экономических показателей эффективности работы риск-моделирования и управления живучестью распределенной компьютерной системы, находящейся в условии УАОС семейства Windows версииXPи выше. Проведен расчет экономического ущерба от реализации атакУАОС семейства Windows версииXPи выше. Расчеты показали, что данная работа является экономически эффективной.