ГУАП

ОТЧЕТ   
ЗАЩИЩЕН С ОЦЕНКОЙ

ПРЕПОДАВАТЕЛЬ

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  | Фаткиева Р. Р. |
| должность, уч. степень, звание |  | подпись, дата |  | инициалы, фамилия |

|  |
| --- |
| ОТЧЕТ О ЛАБОРАТОРНОЙ РАБОТЕ |
| **Оценка нарушения информационной безопасности с использованием Марковской цепи** по дисциплине: Информатика. Основы информационной безопасности |

РАБОТУ ВЫПОЛНИЛИ

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| СТУДЕНТЫ ГР. |  |  |  |  |  |
|  |  |  | подпись, дата |  | инициалы, фамилия |

Санкт-Петербург 2018

1. **Постановка задачи**

Рассмотрим постановку задачи обеспечения безопасности в облачной среде на практическом примере доступа к облачному ресурсу. Ключевым вопросом при использовании облачной среды является безопасность виртуальной среды клиента, начиная с момента установления соединения и заканчивая получением результатов при использовании сервиса. В обобщенном виде процесс доступа к вычислительному ресурсу, представлен в виде графа состояний (рис. 2):



Рис. 1. Штатный процесс установления соединения

В частности, он соответствует процессу установления соединения по протоколу TCP/IP, согласно графу (рис 1), выделены следующие состояния: 1 клиент запускает исполняемый файл; 2 осуществляется открытие сессии; 3 передача данных по каналам связи; 4 установление соединения.

Требуется разработать подход, позволяющий оценить риски нарушения безопасности в облачной среде, а также выработать мероприятия по противодействию представленным атакам.

Поскольку события описываемого операционного процесса дискретны, а время выполнения непрерывно, то сам процесс может быть представлен как процесс с отсутствием последействия, т.е. он обладает марковским свойством. В этом случае процесс перехода из состояния в состояние возможно описать системой дифференциальных уравнений, позволяющей учитывать не только вероятности наступления того или иного события, но влияние мероприятий по защите на процессы, происходящие в облачной среде.

1. **Модель облачной среды в условиях информационных угроз**

Определим показатель периметра защищённости облачных вычислений, как вероятность того, что нарушение безопасности не произойдет. В этом случае защищённость облачных вычислений можно определить через математическое ожидание ущерба от нарушения защищаемых хостов , где  вероятность нарушения безопасности каждого хоста, при -м методе защиты, - количество представленных в системе виртуальных хостов; - значение ущерба от нарушения -го хоста. Выполнение оценки возможно при условии, что атаки являются независимыми, а работа виртуальных хостов не коррелируется.

Для нахождения на каждом виртуальном хосте определим методику, состоящую из следующих шагов:

Шаг. 1: Определение процессов , происходящих в системе, в штатном режиме функционирования.

Шаг. 2: Формирование перечня атак  и построение модели угроз в облачной среде.

Шаг. 3: Определение интенсивностей  перехода процесса  из состояния в состояние и нахождение начальных состояний на момент .

Шаг. 4: Решение системы дифференциальных уравнений относительно полученных интенсивностей перехода и начальных состояний.

Шаг. 5: Получение значений вероятностей  перехода из состояния в состояние на основе рассмотренной ранее системы дифференциальных уравнений для различных наборов значений интенсивностей, характерных альтернативным мероприятиям защиты.

Шаг 6. Влияние на процесс функционирования системы. Определение наилучшего варианта мероприятий по обеспечению информационной безопасности защиты  согласно .

Для построения простейшей модели расширим процесс доступа к вычислительному ресурсу, (рис. 3) с учетом возможных угроз. Этому процессу можно поставить в соответствие следующие состояния: 1-запуск программы; 2-открытие сессии; 3-передача данных по каналам связи; 4-установление соединение с сервером; 5- процесс аутентификации; 6- процесс авторизации; 7 -атака подбора пароля; 8-процесс получение доступа к управляемому ресурсу; 9- атака анализ приложения; 10- атака Ddos; 11- атака сканирование порта; 12-процесс получения данных о порте; 13- процесс получения доступа к ОС; 14-SQL инъекция; 15- процесс перехвата трафика; 16- атака подмена маршрутизатора; \* подделка (компрометация) криптоключа.

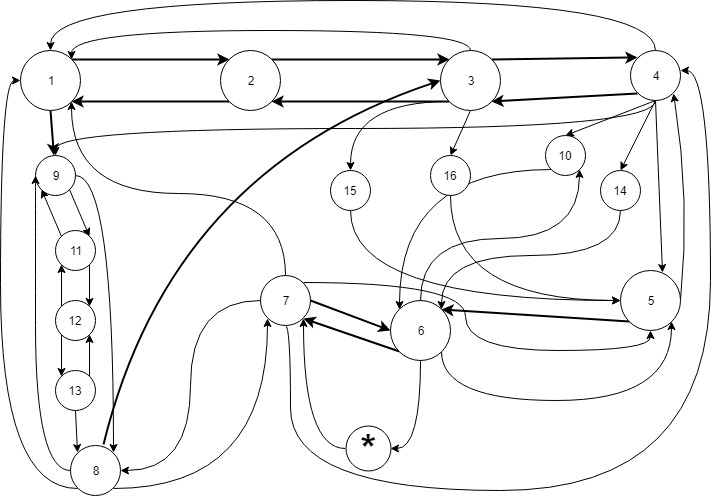


Рис. 3. Процесс доступа к вычислительному ресурсу при нарушениях ИБ

Оценка процессов, происходящих при доступе к сервису, позволяет выделить четыре основных этапа, которые необходимо осуществить для получения доступа к ресурсу: установление соединения, аутентификация, авторизация, доступ к ресурсу. Каждый из этапов представляет собой последовательный набор действий, приводящий к результату, но затрудняющий работу пользователя при осуществлении атаки. В связи с этим целесообразно рассмотреть частные модели возможных угроз на каждом из этапов.

1. **Результаты моделирования**

*Моделирование нарушения установления соединения.* В отличие от стандартного исполняемого файла, содержащего программу в виде, в котором она может быть исполнена компьютером, среда исполнения, а следовательно, и периметр исполняемого приложения, располагается не только на локальном вычислительном устройстве, но и в облаке. Перед исполнением программа загружается в память, и выполняются некоторые подготовительные операции (настройка окружения, загрузка библиотек), необходимые для связи с распределёнными вычислительными ресурсами. Далее осуществляется открытие сессии и установление соединения. Для построения модели угроз и оценки состояния нарушения осуществим моделирование процесса получения доступа с возможными нарушениями:

*-подбор пароля*- атака в основе, которой метод перебора по словарю. С точки зрения теории вероятностей, выбор пароля детерминирован и закономерен. В качестве пароля могут выступать: дата рождения, имя, предмет, набор цифр, последовательность близко расположенных на клавиатуре букв. В общем случае происходит конкатенация вышеперечисленного, поэтому предопределенность в выборе пароля играет ключевую роль в выборе алгоритмов, на которых основан метод перебора по словарю. Алфавитный пароль, сгенерированный человеком, неравномерно распределен в пространстве алфавитных последовательностей. Данное условие может быть учтено с большой точностью в «Марковских фильтрах» нулевого и первого порядка (*нулевой порядок модели Маркова*: каждый символ генерируется в соответствии со своим вероятностным распределением и независимо от предыдущих символов; *первый порядок модели Маркова*: каждой диаграмме (упорядоченной паре) символов присваивается вероятность и каждый символ порождается в условной зависимости от предыдущего);

*-перехват сетевых пакетов:* поскольку при передаче данных создаётся непрерывный динамический канал, проходящий через отдельные сегменты сети, создаётся возможность прослушивания и перехвата сетевых пакетов;

*-навязывание ложного маршрутизатора:* атака канального или сетевого уровня приводящая к перенаправлению сетевых пакетов жертвы или всего трафика сегмента на ненадлежащий адрес или к отказу в обслуживании (no route to host). Для защиты от ложного маршрута и подмены сервера, применим технологию DNS поверх TLS. Целью данного метода является повышение конфиденциальности и безопасности пользователей путем предотвращения перехвата и манипулирования данными DNS.

Для представленных атак граф перехода из состояния в состояние и соответствующая система дифференциальных уравнений представлены на рис 4а и 4б.

|  |  |
| --- | --- |
|  |  |
| Рис. 4а. Штатный процесс установления соединения | Рис. 4б. Система дифференциальных уравнений |

С момента запуска программы (рис. 5, кривая 1) вероятность приближается к единице и с течением времени снижается (согласно проблеме останова) до состояния, когда можно утверждать, что программа зависла. Критическая точка процесса определена 20-ой секундой. На рисунке 5 представлен график кривой 2, полученный с использованием моделирования мероприятий по повышению вероятности успешного запуска (использование «песочницы», т.е. изолированной среды исполнения, антивирусной защиты, контроля целостности приложений и разделение прав доступа пользователей). Это позволяет оценить влияние введения тех или иных мер по защите на протекание процесса.

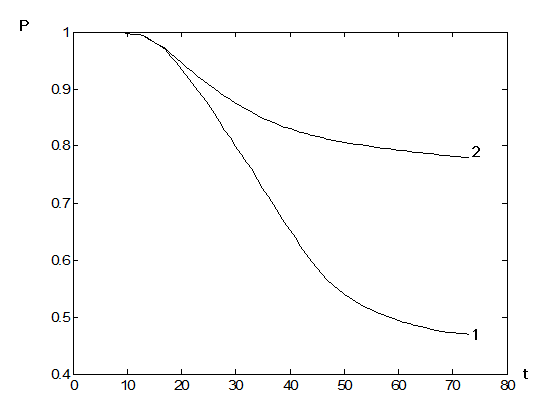


Рис.5. Вероятность запуска программы

*Зависимость процесса открытия сессии от процесса запуска программы*. Вероятность открытия сессии обеспечивается запуском программы (рис. 6, кривая 2), созданием нового соединения, инициируемого исполняемым файлом, с передачей пакета. Будем считать, что одновременно с созданием сессии открывается порт TCP/IP для последующей передачи данных и установления соединения с распределёнными вычислительными ресурсами. Такая последовательность действий обеспечивает рост вероятности до определённого момента, на которую могут повлиять атаки: MITM, DDOS. Для обеспечения успешного открытия сессии, а также в целях противодействия нарушениям безопасности и в качестве мер повышения вероятности было предложено применение аппаратного VPN точка-точка с криптографическим модулем. Анализ результатов моделирования показал эффективность проведенных мероприятий по защите (рис. 6 кривая 2).

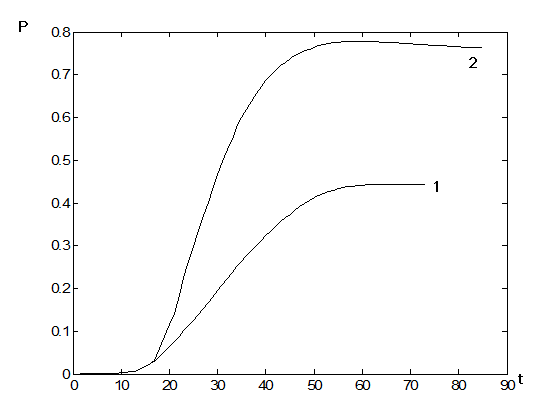


Рис.6. Вероятность открытия сессии

*Вероятность передачи данных по каналам связи*. Как и на предыдущем графике прослеживается зависимость от процессов его образующих (рис. 7, кривая 1). Критической точкой жизнеспособности процесса является тот же момент, при котором в процессе запуска приложения появляются те или иные проблемы с загрузкой. На рисунке 7 представлен график кривой 2, полученный после моделирования мер по повышению вероятности успешной передачи данных с использованием туннелирования в каналах передачи данных (VPN канал). Моделирование не показало, что существенное влияние на процесс передачи не оказывается, однако вероятность передачи повышается.

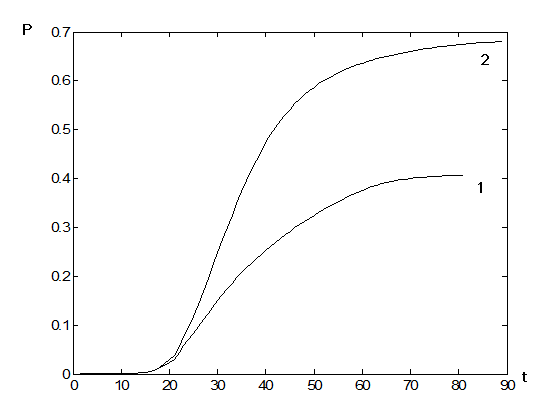


Рис.7. Вероятность передачи данных по каналам связи

Результаты показывают вероятность того, что в данный момент происходит установление соединения с сервером, аналогичны предыдущему процессу (рис. 8, кривая 1). На рисунке 8 (кривая 2) изображена вероятность успешного установления соединения с сервером при противодействии нарушению безопасности. Были предприняты следующие меры: ограничение доступа по геолокации (GeoIP Block), динамическая блокировка IP-адресов «разрешённых стран» согласно правилам фильтрации пакета, установлен VPN канал.

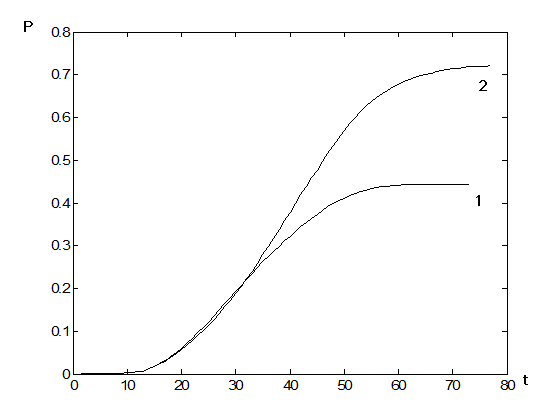


Рис.8 Вероятность установления соединения с сервером

Вероятность атаки подбора пароля рассматривается в момент соединения программы с сервером (рис 9, кривая 1). С точки зрения теории вероятностей, выбор пароля детерминирован и закономерен, поэтому применение генераторов паролей с аппаратным датчиком случайных чисел снижает вероятность успешной атаки (рис 9, кривая 2).

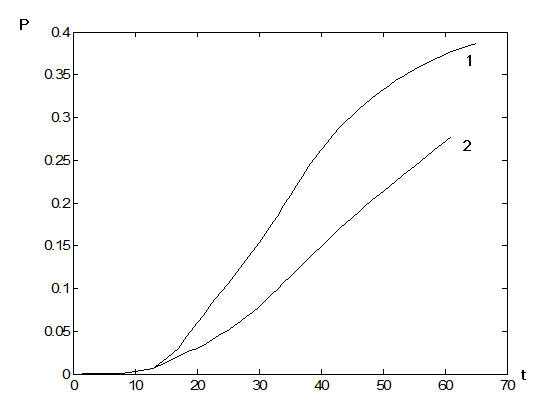


Рис.9 Вероятность успешной атаки подбора пароля

Вероятность успешного перехвата сетевых пакетов с целью их дальнейшего анализа растет на временном интервале (рис 10, кривая 1) и связана с установлением соединения между приложением и сервером. Рисунок 10 (кривая 2) демонстрирует, что процесс обнаружения атак (процесс оценки подозрительных действий узлов сети) понижает вероятность перехвата.

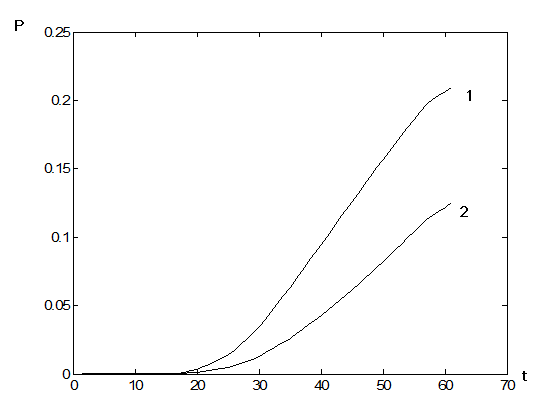


Рис.10. Вероятность успешного перехвата сетевых пакетов

Атака канального или сетевого уровня приводит (рис. 11, кривая 1) к перенаправлению сетевых пакетов жертвы или всего трафика сегмента на ненадлежащий адрес или к отказу в обслуживании (no route to host). Вероятность атаки зависит от успешности соединения с сервером, повышается по мере его установления. Результаты моделирования противодействия навязывания ложной маршрутизации пакетов с применением фильтрации проходящих ICMP-сообщений Redirect понижает вероятность атаки почти вдвое (рис. 11, кривая 2).

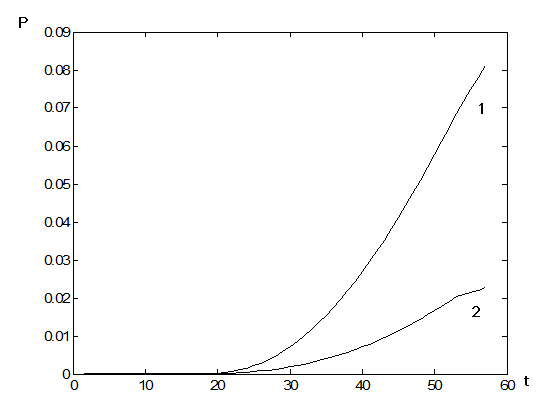


Рис. 11. Вероятность успешного навязывания ложной маршрутизации пакетов

Полученные результаты моделирования с учетом всей совокупности введенных мероприятий по защите (в табл. 1 и на рис. 12) позволяют определить влияние мер по обеспечению безопасности на уязвимые элементы в анализируемых процессах. Полученные решения применимы при планировании мероприятий по защите критически важных объектов от рассматриваемых угроз с учетом количественной оценки вероятности нарушения. Использование данной методики позволяет получить обоснование целесообразности мероприятий обеспечения безопасности в анализируемом объекте.

Таблица 1. Оценка вероятности нарушения безопасности

|  |  |  |
| --- | --- | --- |
| **Процесс** | **Вероятность без мероприятий по обеспечению безопасности** | **Вероятность при мероприятиях по обеспечению безопасности** |
| Запуск программы | 0.47 | 0.77 |
| Открытие сессии | 0.3 | 0.7 |
| Передача данных | 0.07 | 0.5 |
| Соединение с сервером | 0.07 | 0.6 |
| Атака подбора пароля | 0.03 | 0.18 |
| Атака перехвата сетевых пакетов | 0.03 | 0.09 |
| Атака ложная маршрутизация | 0.03 | 0.04 |

|  |  |
| --- | --- |
|  |  |
| Рис. 12а. Оценка вероятности нарушения безопасности | Рис. 12б. Оценка вероятности нарушения безопасности при мерах защиты |

Такое обоснование осуществляется за счет достижения максимального результата защиты при минимальных затратах и определяется следующими факторами: масштабностью и ресурсоемкостью сети, необходимостью применения однотипных технологий и средств защиты информации при проведении мероприятий по обеспечению системы защиты информации.

**Вывод**

Анализ полученных в ходе исследования результаты моделирования процессов безопасности виртуальной среды клиента и применения комплексного подхода к обеспечению информационной безопасности, показали следующее. Современные стереотипы по защите процессов клиентов виртуальной среды не в полной мере готовы противостоять текущим угрозам и новым вызовам безопасности. В связи с этим возникает необходимость совершенствования научно-методического аппарата. На примере конкретной задачи с типовыми процессами использована марковская модель для выявления наиболее значимых угроз, целесообразных мероприятий защиты и прогнозирования состояния системы. Аналогичная методика может быть использована для других моделей безопасности, для нахождения целесообразных мероприятий защиты и прогнозирования состояния системы. Применение полученных результатов в процессе построения, эксплуатации и модернизации системы информационной безопасности, предоставляющей облачные услуги ведет к повышению эффективности и качества обслуживания и позволяет эффективно управлять процессом информационной безопасности.

**Приложение 1. Код программы**

Main2.m

%Main

global l14 l29 l26 l211 l213 l312 l37 l45 l48 l410 l51 l63 l73 l85 l93 l105 l112 l123 l132;%определяем глобальные переменные

% глобальным переменным присваиваем значение лямбда

l14 = 0.2;

l29 = 0.1;

l26 = 0.95;

l211 = 0.3;

l213 = 0.5;

l312 = 0.2;

l37 = 0.95;

l45 = 0.95;

l48 = 0.3;

l410 = 0.5;

l51 = 0.1;

l63 = 0.3;

l73 = 0.95;

l85 = 0.15;

l93 = 0.05;

l105 = 0.6;

l112 = 0.7;

l123 = 0.2;

l132 = 0.5;

initial = [1; 0; 0; 0; 0; 0; 0; 0; 0; 0; 0; 0; 0];% определяем интервал

time = [0, 25];% временной интервал

[T, Y] = ode45('LotVol', time, initial); %строим функцию

for i = 1:13 %для диффуров

plot(Y(:,i)); hold on

end

LotVolCoefSource

function result = LotVolCoefSource()

%LOTVOLCOEFSOURCE Summary of this function goes here

% Detailed explanation goes here

global l14 l29 l26 l211 l213 l312 l37 l45 l48 l410 l51 l63 l73 l85 l93 l105 l112 l123 l132;% обозначаем данные

% матрица уравнений

lambda = [

% --1 --2 --3 --4 --5 --6 --7 --8 --9 --10 --11 --12 --13

0 0 0 l14 0 0 0 0 0 0 0 0 0;

0 0 0 0 0 l26 0 0 l29 0 l211 0 l213;

0 0 0 0 0 0 l37 0 0 0 0 l312 0;

0 0 0 0 l45 0 0 l48 0 l410 0 0 0;

l51 0 0 0 0 0 0 0 0 0 0 0 0;

0 0 l63 0 0 0 0 0 0 0 0 0 0;

0 0 l73 0 0 0 0 0 0 0 0 0 0;

0 0 0 0 l85 0 0 0 0 0 0 0 0;

0 0 l93 0 0 0 0 0 0 0 0 0 0;

0 0 0 0 l105 0 0 0 0 0 0 0 0;

0 l112 0 0 0 0 0 0 0 0 0 0 0;

0 0 l123 0 0 0 0 0 0 0 0 0 0;

0 l132 0 0 0 0 0 0 0 0 0 0 0

% --1 --2 --3 --4 --5 --6 --7 --8 --9 --10 --11 --12 --13

];

result = LotVolCoef(lambda);

end