УДК 004.42

А. А. Стрелкина,
Д. Д. Узун, канд. техн. наук

Марковская модель процессов кибербезопасности информационных систем

Национальный аэрокосмический университет им. Н. Е. Жуковского "ХАИ"

Определены возможности применения марковских случайных процессов с точки зрения оценки безопасности информационных систем. Представлен граф состояний и переходов при воздействии на систему угроз и устранении уязвимостей, в котором также учтены периодические профилактики, патчеризации и обновления с устранением и внесением уязвимостей.

Ключевые слова: атака, вероятность, граф состояний, информационная безопасность, марковские случайные процессы, угроза, уязвимость.

Введение. В настоящее время информационная безопасность остается одной из наиболее динамически развивающихся областей информационных технологий. Главным образом это связано с растущим количеством атак на информационные ресурсы во всем мире. Исходя из этого для многих предприятий важно иметь защищенными свои информационные системы от атак извне.

Одной из самых актуальных задач в области информационной безопасности является оценка угроз. Качественная представляет собой основу для применения необходимых средств и методов защиты информации.

Существует несколько инструментариев оценки информационной безопасности, моделирования средств защиты и возможных атак, основные из которых приведены в [1]. К ним относятся: теория вероятностей, нечеткие множества, теория игр, графы, автоматы, сети Петри и случайные процессы.

Марковские случайные процессы нашли широкое применение в теории и практике. Согласно [2] данные процессы можно применять для оценки влияния на безопасность информации атак на систему в том случае, если атака является редким и независимым событием.

Исходя из этого для исследования влияния атак на информационную систему оправдано использование марковских случайных процессов.

Постановка задачи. Пусть на информационную систему воздействуют n независимых атак за конечное время t. При этом очередная атака воздействует на систему только после осуществления предыдущей. Переход системы из состояния в состояние происходит до тех пор, пока она не окажется в неработоспособном состоянии, соответствующем успешной реализации злоумышленником атаки на систему. Из данного состояния система может выйти после проведения патчеризации с устранением уязвимости или без ее устранения. Кроме того, в системе периодически проводятся профилактические мероприятия, в ходе которых устраняются существующие уязвимости и возможна разработка обновлений. В системе всегда существует уязвимость «нулевого дня» $n+1$.

В данной работе, под атакой понимается потенциально опасное событие, возникающее во время функционирования системы, которое создает особо опасную ситуацию для системы. Такая атака характеризуется следующими особенностями:

– может быть преднамеренной или непреднамеренной;

– является детерминированным событием;

– воздействия на информационную систему, как правило, являются стохастическими процессами, что дает возможность применять случайные процессы.

В отношении угрозы возникновения уязвимости и атаки (при устранении уязвимости исчезает и угроза атаки) информационную систему можно рассматривать как систему с отказами и восстановлениями характеристики информационной безопасности.

Результаты. Исходя из поставленной задачи примем следующие обозначения:

P_j и $\overline{P_j} = 1 - P_j$ – вероятности успешного и неуспешного парирования возникшей *j*-й атаки соответственно;

$\lambda_j, j = 1,n$ – интенсивность атак на информационную систему;

μ_j – интенсивность отражения последствий *j*-й атаки;

$\mu_j \cdot P_j$ – интенсивность отражения атак на информационную систему;

$\mu_j \cdot \overline{P_j}$ – интенсивность успешной реализации атаки на информационную систему;

λ_{prof} – интенсивность проведения профилактических мероприятий аудита безопасности;

μ_{prof} – интенсивность восстановления системы после профилактических мероприятий аудита безопасности;

P_{sv} – вероятность устранения одной уязвимости;

μ_{reb} – интенсивность перезапуска системы после атаки;

$\lambda_{patchup}$ – интенсивность разработки обновлений, в которых устраняются уязвимости;

λ_{patch} – интенсивность разработки патча после атаки на уязвимость;

μ_{patch} – интенсивность восстановления системы после установки патча (или обновлений);

λ_{fix} – интенсивность устранения уязвимости;

P_{fix} – вероятность перезапуска с устранением уязвимости;

$\Delta\lambda_a$ – изменение интенсивности проявления дефектов в системе, обусловленное появлением или устранением уязвимостей в системе.

Кроме того, примем следующие допущения:

– поток парирования и непарирования атак на систему является простейшим;

– возможности по парированию последствий воздействия на информационную систему j-й атаки не ограничены, т. е. $\mu_j \geq \lambda_j$.

При любом *j*-м воздействии с интенсивностью $\lambda_j^{i'}$ система может оказаться с вероятностью $P_j^{i'}$ и интенсивностью $\mu_j^{i'}$ в исходном состоянии $S_0^{i'}$ (рис. 1), что соответствует успешному парированию *j*-й атаки доступными методами и средствами.

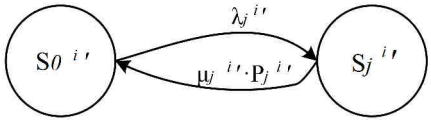

Рис. 1. Переход системы из одного состояния в другое при воздействии на нее атаки и успешном парировании

С некоторой периодичностью в системе проводятся профилактические мероприятия (состояния $S_{aud}{}^{i'}$), в результате которых может быть выявлено и устранено от 0 до n уязвимостей (рис. 2).

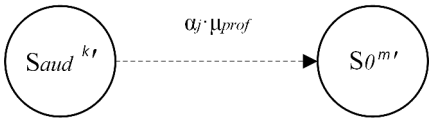

Рис. 2. Переход системы из одного состояния в другое при условии устранения уязвимостей после профилактических мероприятий

При профилактике возможно обнаружение и устранение нескольких уязвимостей из множества $[1,...,n]$. Для этого необходимо ввести параметр α_j вероятности обнаружения и устранения *j*-й уязвимости $\left(j \in [1,...,n]\right)$. Очевидно, что $\sum_{i=1}^{n} \alpha_i = 1$, а значения $\alpha_1, \alpha_2, ..., \alpha_j, ..., \alpha_n$ имеют дискретный закон распределения. Для соблюдения равенства $\sum_{i=1}^{n} \alpha_i = 1$ значения коэффициентов α_j необходимо рассчитывать по формулам из таблицы. При переходе в новое состояние после профилактики интенсивность атак на информационную систему перераспределяется на λ_a (так как сумма должна быть равна 1).

Определение вероятности обнаружения *j*-й уязвимости

j	1	2	3	…	$n-1$	n
α_j	p	$q \cdot p$	$q^2 \cdot p$	…	$q^{n-2} \cdot p$	$1-\sum_{i=1}^{n-1} \alpha_i$

После осуществления успешной атаки (переход в состояние $S_c{}^{i'}$ с интенсивностью $\mu_j{}^{i'} \cdot \overline{P_j{}^{i'}}$, что изображено на рис. 3) система теряет работоспособность.

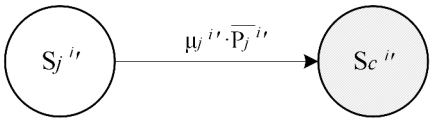

Рис. 3. Переход системы из одного состояния в другое после осуществления успешной атаки

После проявления уязвимости возможно два варианта развития событий: системная служба перезапускается (если уязвимость своевременно не обнаружена, то осуществляется переход из состояния $S_c^{i'}$ в состояние $S_o^{i'}$ с интенсивностью $\lambda_{fix} \cdot \overline{P_{fix}}$, что изображено на рис. 4); уязвимость выявляется и система остается в состоянии $S_c^{i'}$ и запускается разработка патча, а далее система переходит в состояние патчеризации $S_{pat}^{i'}$ с интенсивностью λ_{patch} (рис. 5).

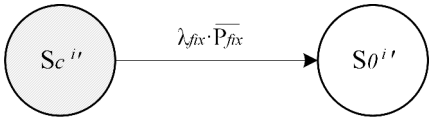

Рис. 4. Переход системы из одного состояния в другое при условии, что уязвимость своевременно не выявлена

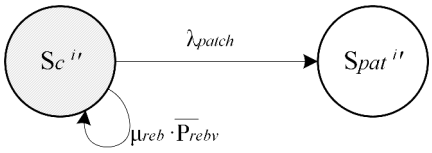

Рис. 5. Переход системы из одного состояния в другое при условии, что уязвимость выявлена

После установки патча также возможно несколько ситуаций: устраняется одна уязвимость (рис. 6), группа уязвимостей (рис. 7), уязвимость не устранена (рис.8), вносятся ранее устраненные уязвимости (рис. 9).

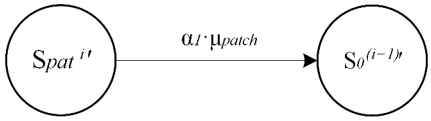

Рис. 6. Переход системы из одного состояния в другое после патчеризации при устранении одной уязвимости

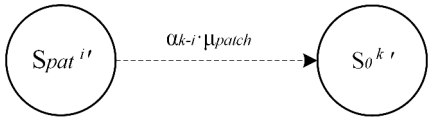

Рис. 7. Переход системы из одного состояния в другое после патчеризации при устранении группы уязвимостей

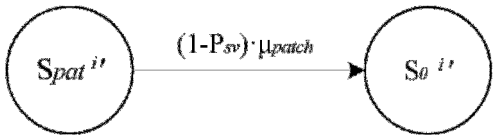

Рис. 8. Переход системы из одного состояния в другое после патчеризации, если уязвимость не устранена

Рис. 9. Переход системы из одного состояния в другое после патчеризации, если внесена одна или группа уязвимостей

В случае устранения *j*-й уязвимости $\left(j \in [1,...,n]\right)$ необходимо также использовать параметр α_j вероятности обнаружения и устранения уязвимости, как и в случае с профилактикой. Его также рассчитывают по формулам из таблицы.

Так как возможно внесение нескольких уязвимостей из множества $[1,...,n]$ после патчеризации, то необходимо ввести параметр β_j вероятности внесения уязвимости, который обладает такими же свойствами, как и α_j.

При переходе в новые состояния после установки патча интенсивность атак на информационную систему перераспределяется на $\Delta\lambda_a$ при устранении и внесении уязвимостей. Данный параметр может быть равен интенсивности устраненной атаки, разделенной на общее количество атак в следующем состоянии.

Возможна также разработка обновлений, в результате чего система из начального состояния переходит в состояние патчеризации с интенсивностью $\lambda_{patchup}$, что изображено на рис. 10.

Рис. 10. Переход системы из одного состояния в другое при разработке обновлений

После выявления и устранения всех уязвимостей (кроме уязвимости «нулевого дня») система продолжает функционировать в нормальном режиме.

Для рассматриваемого случая полный граф состояний и переходов показан на рис. 11.

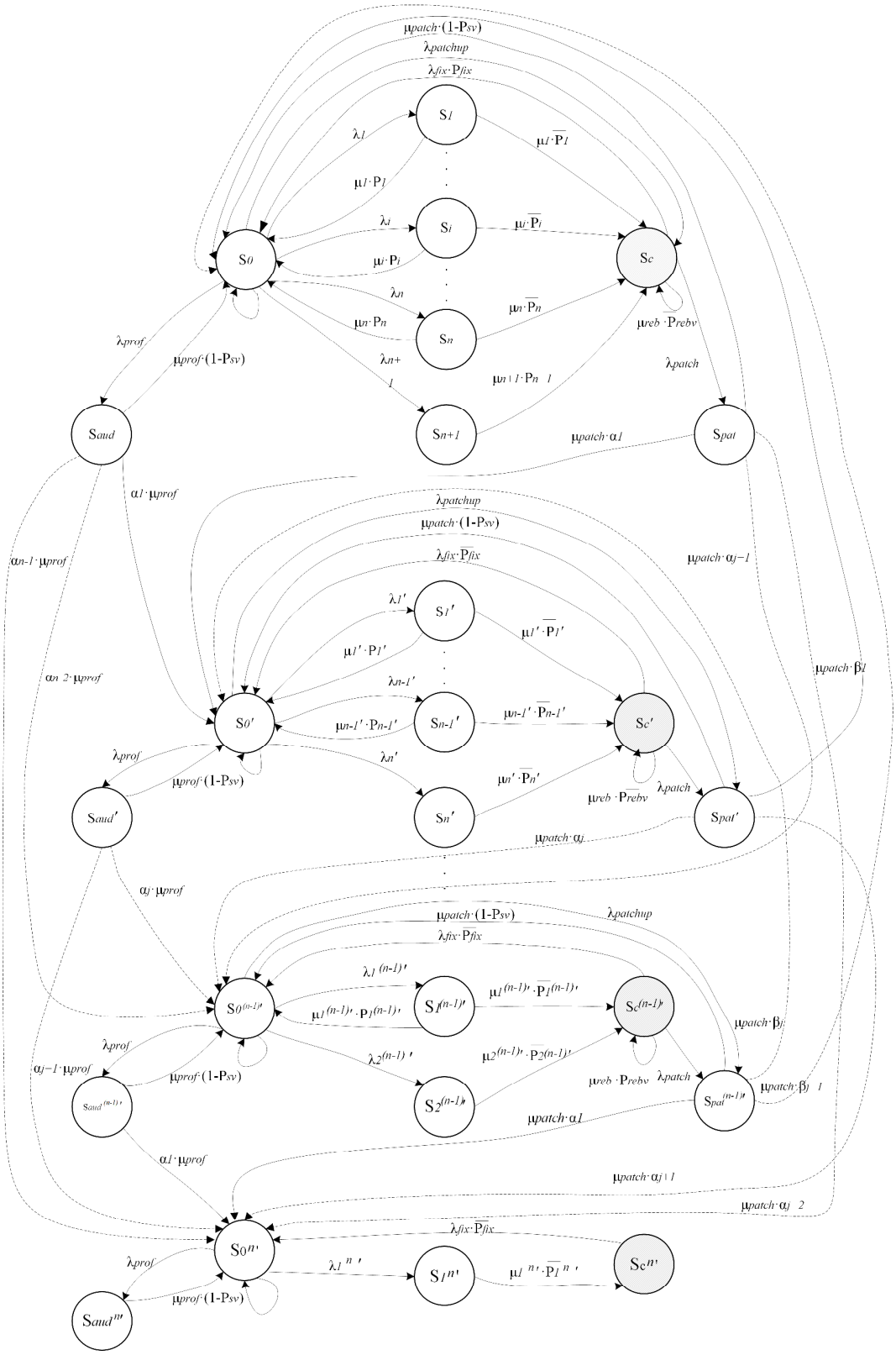

Рис. 11. Граф состояний и переходов системы при воздействии на нее n независимых угроз и устранении уязвимостей

Таким образом, марковские процессы можно применять для определения наиболее опасных угроз, а также разработки организационно-профилактических мероприятий по предупреждению воздействий атак на информационную систему.

Выводы

В работе определены возможности применения марковских случайных процессов для оценки угроз информационной безопасности систем. Представлен граф при воздействии на систему угроз и устранении уязвимостей, в котором также учтены периодические профилактики, патчеризации и обновления с устранением и внесениям уязвимостей.

Предложенный метод может быть использован для оценки и анализа уровня информационной безопасности на различных предприятиях.

В качестве направления дальнейших исследований можно считать изучение иных моделей, сбор статистических данных для проведения численных расчетов.

Список литературы

1. Майстренко, В. А. Безопасность информационных систем и технологий / В. А. Майстренко, В. Г. Шахов. – Омск: Изд-во ОмГТУ, 2006. – 232 с.

2. Росенко, А. П. Применение марковских случайных процессов с дискретным параметром для оценки уровня информационной безопасности / А. П. Росенко. // Известия Южного федерального университета. Технические науки. – 2009. – №11 – с. 169-179.

Поступила в редакцию 24.11.2015

Марковська модель процесів кібербезпеки інформаційних систем

Визначено можливості застосування марковських випадкових процесів з точки зору оцінювання безпеки інформаційних систем. Подано граф станів і переходів при впливі на систему загроз та усуненні вразливостей, в якому також враховано періодичні профілактики, патчеризації та оновлення з усуненням та внесенням вразливостей.

***Ключові слова*:** атака, ймовірність, граф станів, інформаційна безпека, марковські випадкові процеси, загроза, вразливість.

Markov Model of Information systEms' Cyber Security Processes

The possibilities of using Markov processes for cyber security assessment are defined. State machine for impacting on the system of threats and their elimination with periodic information security audit, patching and updating is shown.

Key words: attack, probability, state machine, cyber security, Markov process, threat, vulnerability.