ПОДХОДЫ К АДАПТИВНОМУ ПРОГНОЗИРОВАНИЮ НАПРАВЛЕНИЙ РАЗВИТИЯ КОМПЬЮТЕРНЫХ АТАК В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Голицын Сергей Александрович

кандидат технических наук,
магистр Краснодарского высшего военного училища
имени генерала армии С.М. Штеменко,
специалист в области организации защиты информации

Шульженко Анастасия Дмитриевна

начальник лаборатории Военно-космической академии
имени А.Ф. Можайского, г. Санкт-Петербург,
специалист в области обработки информации

APPROACHES TO ADAPTIVE FORECASTING OF THE DIRECTIONS OF DEVELOPMENT OF COMPUTER ATTACKS IN INFORMATION SYSTEMS

Golitsyn Sergey Alexandrovich

candidate of technical sciences,
Master of the Krasnodar Higher Military School
named after General of the Army S.M. Shtemenko,
information security specialist

Shulzhenko Anastasia Dmitrievna

Head of the Laboratory of the Military Space Academy
named after A.F. Mozhaisky, St. Petersburg,
information processing specialist

Аннотация. В данной статье рассмотрены вопросы организации противодействия компьютерным атакам на основе прогнозирования направлений их развития и формирования альтернатив противодействия им. Предложены функционально-структурная схема и архитектура подсистемы прогнозирования компьютерных атак.

Abstract. This article discusses the issues of organizing countering computer attacks based on predicting the directions of their development and the formation of alternatives to counter them. The functional-structural diagram and architecture of the subsystem for predicting computer attacks are proposed.

Ключевые слова: компьютерные атаки, противодействие деструктивным воздействиям, прогноз развития деструктивных воздействий, система прогнозирования.

Key words: computer attacks, counteraction to destructive influences, forecast of the development of destructive influences, forecasting system.

В процессе развития методов и подходов к организации информационно-аналитического обеспечения в сложных аналитических системах, в том числе системах обнаружения, предупреждения и ликвидации последствий компьютерных атак (далее – СОПКА), специалисты информационной безопасности сталкиваются с необходимостью реализации алгоритмов принятия решений в условиях нечеткости и неопределенности исходной информации.

В связи с тем, что на сегодняшний день СОПКА еще не способна осуществлять свою деятельность в полностью автоматизированном режиме, то для эффективного ее функционирования необходима система экспертной поддержки (далее – СЭП).

В свою очередь СЭП в процессе подготовки решений по реагированию на компьютерные атаки и вызванные ими компьютерные инциденты опирается на результаты подсистемы прогнозирования.

Основными задачами подсистемы прогнозирования являются:

- формирование множества деструктивных воздействий на элементы информационных систем;
- формирование множества полезных воздействий;
- формирование множества целей компьютерных атак;
- формирование множества альтернатив противодействия компьютерным атакам.

Целью подсистемы прогнозирования является формирование множества возможных альтернатив противодействия компьютерным атакам, структурированное в виде дерева, представленного на рисунке 1. Дерево отображает прогноз развития деструктивных воздействий, начиная

с текущего состояния информационной системы (при обнаружении компьютерной атаки) вместе с соответствующими полезными воздействиями.

Рисунок **Ошибка! Текст указанного стиля в документе отсутствует.** – Множество возможных альтернатив противодействия компьютерным атакам

Для достижения указанной цели необходимо иметь перечень деструктивных и полезных воздействий на элементы информационной системы на каждом этапе времени, а также знать конечную цель компьютерных атак. Построение очередного уровня дерева противодействия будет происходить поэтапно, путем применения известных воздействий к текущему состоянию системы и моделирования реакции системы на эти воздействия. Затем процедура будет повторена для каждого нового узла дерева.

Структурно-функциональную схему подсистемы прогнозирования можно представить в виде, представленном на рисунке 2.

В процессе функционирования в каждый момент времени информационная система может находиться в одном из состояний, которые находят свое отражение при формализации модели состояний [1].

Переход из одного состояния в другое обуславливается изменением значения контролируемых параметров, которое осуществляется по причине различных воздействий на элементы информационной системы. Воздействия могут быть двух типов:

- деструктивные – возникающие при осуществлении компьютерной атаки;
- полезные – формируемые средствами защиты информации (должностными лицами) с целью противодействия деструктивным воздействиям.

На вход модуля формирования множества деструктивных воздействий подается текущий вектор параметров компьютерных атак и ретроспективная выборка сигнатур компьютерных атак.

Рисунок 2 – Структурно-функциональная схема подсистемы прогнозирования

Функционально модуль состоит из следующих блоков:

- блок анализа параметров текущей компьютерной атаки;
- блок анализа ретроспективной выборки сигнатур компьютерных атак.

В процессе анализа параметров текущей компьютерной атаки формируется множество деструктивных воздействий, которые могут быть применены к элементам информационной системы. Ретроспективная выборка нужна для того, чтобы спрогнозировать возможные неочевидные на данный момент времени воздействия при дальнейших действиях нарушителя по развитию текущей компьютерной атаки.

Выходными данными модуля является множество деструктивных воздействий компьютерной атаки на информационную систему, структурированное в виде дерева. Эти данные передаются в модуль формирования множества полезных воздействий и в модуль построения дерева противодействия.

Ниже представлено описание вероятностной модели реализации деструктивных воздействий компьютерной атаки на информационную систему.

Для определения вероятностных значений перехода информационной системы из одного состояния в другое строится математическая модель как некий агрегированный объект. В качестве элементов модели целесообразно рассматривать элементы, законченные с точки зрения информационного, функционального и структурного исполнения [2].

Исходя из подобного построения и для удобства записи, информационную систему можно представить как множество уязвимых элементов, подлежащих защите:

$$\{e_m\} = \{e_1, e_2, \dots, e_m\}.$$

Допустим, множество угроз, реализация которых может являться деструктивным воздействием на элементы информационной системы, конечно и насчитывает N компонент:

$$\{y_n\} = \{y_1, y_2, \dots, y_n\}.$$

Тогда при построении модели необходимо рассмотреть саму возможность реализации каждой угрозы из множества $\{y_n\}$ на каждый элемент информационной системы из множества $\{e_m\}$. Интенсивность воздействия угроз на элементы информационной системы представлена в таблице 1.

Поток реализации угроз является:

- ординарным – угрозы появляются поодиночке, т.е. вероятность попадания на участок Δt двух или более событий пренебрежительно мала по сравнению с вероятностью попадания на него ровно одного события;

– потоком без последствия – для любых не перекрывающихся участков времени $\tau_1, \tau_2, \dots, \tau_n$ числа равные количеству событий, попадающих на эти участки, представляют собой независимые случайные величины, т.е. вероятность попадания любого числа событий на один из участков не зависит от того, сколько их попало на другие.

Таблица **Ошибка! Текст указанного стиля в документе отсутствует.**
Интенсивность воздействия угроз на элементы ИС

	e_1	e_2	$\dots$	e_m
y_1	μ_{11}	μ_{12}	$\dots$	μ_{1m}
y_2	μ_{21}	μ_{22}	$\dots$	μ_{2m}
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
y_n	μ_{n1}	μ_{n2}	$\dots$	μ_{nm}

где μ_{nm} – интенсивность потока n –ой угрозы на m –й элемент информационной системы.

На основе предельной теоремы для суммарного потока можно сделать вывод, что сумма потоков различных событий на любой элемент будет сходиться к пуассоновскому потоку, для которого справедливо утверждение:

– при сложении любого числа N независимых ординарных потоков будет получаться снова ординарный поток, интенсивность которого равна сумме интенсивностей складываемых потоков. То есть для элемента информационной системы e_m интенсивность суммарного потока всех угроз из множества $\{y_n\}$ будет равна:

$$\mu_m = \sum_{n=1}^N \mu_{nm}, \quad (1)$$

а для интенсивности потока в целом будет справедливо:

$$\mu = \sum_{m=1}^M \mu_m = \sum_{n=1}^N \sum_{m=1}^M \mu_{nm}. \quad (2)$$

В соответствии с [2], если параметр μ пуассоновского закона зависит от времени, т.е. поток возникновения атак неоднороден, то вероятность возникновения a событий на участке времени Δt описывается выражениями:

– для элемента m и угрозы n :

$$P_{nm}[X(t, t + \Delta t) = a] = \frac{1}{a!} \left(\int_t^{t+\Delta t} \mu_{nm}(t) dt \right)^a \exp \left(- \int_t^{t+\Delta t} \mu_{nm}(t) dt \right), \quad (3)$$

– для элемента m и множества угроз Y :

$$P_m[X(t, t + \Delta t) = a] = \frac{1}{a!} \left(\int_t^{t+\Delta t} \mu_m(t) dt \right)^a \exp \left(- \int_t^{t+\Delta t} \mu_m(t) dt \right), \quad (4)$$

– для защищаемой системы и множества угроз Y :

$$P[X(t, t + \Delta t) = a] = \frac{1}{a!} \left(\int_t^{t+\Delta t} \mu(t) dt \right)^a \exp \left(- \int_t^{t+\Delta t} \mu(t) dt \right). \quad (5)$$

Интенсивности потоков реализации угроз на элементы системы e_m определяются из таблицы № 1 и соотношениями (1) и (22).

Предполагая, что число событий, попадающих на интервал Δt , распределено по закону Пуассона, и, полагая $a = 0$, получим вероятность того, что за интервал Δt не произойдет ни одного события:

$$P_0(t, t + \Delta t) = \exp\left(-\int_t^{t+\Delta t} \mu(t)dt\right). \quad (6)$$

Событие, состоящее в том, что на систему будет произведена хотя бы одна реализация угрозы на интервале Δt , является противоположным:

$$P(t, t + \Delta t) = 1 - P_0(t, \Delta t) = 1 - \exp\left(-\int_t^{t+\Delta t} \mu(t)dt\right). \quad (7)$$

Таким образом, для построения модели перехода системы из одного состояния в другое необходимо:

- 1) Определить множество уязвимых элементов системы $\{e_m\}$.
- 2) Определить множество потенциальных угроз $\{y_n\}$.
- 3) С каждым элементом системы e_m связать подмножество угроз $\{y'_n\} \in \{y_n\}$, которое может воздействовать на этот элемент.
- 4) Составить таблицу интенсивностей (Таблица №1) **Таблица Ошибка! Текст указанного стиля в документе отсутствует..**
- 5) Определить вероятностные характеристики потока реализации деструктивных воздействий на элемент e_m .
- 6) Определить вероятностные характеристики потока реализации деструктивных воздействий на информационную систему.

Таблица интенсивностей (Таблица 1) первоначально формируется экспертно, накопление данных осуществляется путем применения штатных средств системы защиты.

На вход модуля формирования множества полезных воздействий подаются текущие параметры информационной системы, ретроспективная выборка и множество деструктивных воздействий.

Функционально модуль состоит из следующих блоков:

- блок анализа параметров системы;
- блок анализа ретроспективной выборки;
- блок генерации полезных воздействий для противодействия деструктивным.

В процессе анализа параметров системы формируется множество полезных воздействий (структурированное в виде дерева), которые могут изменить значения контролируемых параметров, что позволит системе перейти в другое состояние. Ретроспективная выборка нужна для того, чтобы проанализировать накопленный опыт по противодействию деструктивным воздействиям и выбрать оптимальные полезные воздействия.

Для формирования множества полезных воздействий необходимо:

- 1) Определить множество состояний информационной системы, в которые возможен переход из текущего.
- 2) Сопоставить с каждым переходом вероятностные характеристики потока реализации деструктивных воздействий.
- 3) Сопоставить полезные воздействия, определяемые при формировании модели состояний информационной системы.

Выходными данными модуля является множество полезных воздействий на систему, структурированное в виде дерева. Эти данные передаются в модуль формирования множества полезных воздействий.

На вход в модуль формирования множества целей компьютерной атаки подается текущая и ретроспективная карта сети, а также параметры текущей атаки.

Функционально модуль состоит из следующих блоков:

- блок анализа параметров текущей компьютерной атаки;
- блок анализа текущей и ретроспективной карты сети.

Основной задачей модуля является прогнозирование перечня узлов информационной системы и служб, функционирующих на них, которые будут задействованы на следующих этапах жизненного цикла текущей атаки.

Для формирования множества целей компьютерной атаки необходимо:

- 1) Сопоставить параметры текущей компьютерной атаки и параметры компьютерной атаки из ретроспективной выборки, таким образом получить перечень элементов КС и служб, которые когда-либо являлись целями похожих атак.
- 2) Сопоставить полученный перечень с текущей картой сети, таким образом получить множество целей текущей компьютерной атаки.

Выходными данными модуля является прогнозируемое множество целей компьютерной атаки

Основной задачей модуля является формирование дерева противодействия компьютерным атакам для оптимального соотношения в каждый момент времени деструктивных и полезных воздействий на элементы информационной системы с множеством конечных целей атаки.

Входными данными для этого модуля являются:

- множество деструктивных воздействий;
- множество полезных воздействий;
- множество конечных целей компьютерной атаки.

Для формирования дерева противодействий необходимо:

- 1) Определить множество состояний информационной системы, в которые возможен переход из текущего.
- 2) Сопоставить множества деструктивных и полезных воздействий. Каждому переходу в новое состояние привести в соответствие воздействия, которые к этому переходу приведут.
- 3) Сопоставить текущее состояние жизненного цикла компьютерной атаки с прогнозируемым множеством конечных целей компьютерной атаки. Таким образом определить приоритеты переходов из текущего состояния информационной системы согласно прогнозируемому вектору развития компьютерной атаки.
- 4) Рассчитать вероятности для каждого перехода из текущего состояния информационной системы. После выполнения указанных действий формируется совокупность состояний системы для текущего момента времени, совокупность состояний для следующего момента времени и совокупность переходов из состояния в состояние.
- 5) Повторить действия 1–4 для каждого следующего момента времени. Таким образом получается множество ветвей дерева противодействия текущей компьютерной атаки (множество альтернатив противодействия).

Выходными данными является множество альтернатив противодействия компьютерной атаке (структурированное в виде дерева). Оно представляет собой однонаправленный граф, в котором каждая вершина характеризует состояние системы, а каждая связь характеризует сумму воздействий, необходимых для перехода в новое состояние. Множество альтернатив противодействия компьютерным атакам передается в подсистему поддержки принятия решения.

С учетом разработанной структурно-функциональной схемы и алгоритма функционирования подсистемы прогнозирования компьютерных атак разработан проект подсистемы прогнозирования компьютерных атак, представленный на рисунке 3.

Таким образом, основываясь на приведенное описание подсистемы прогнозирования компьютерных атак, а также разработанных алгоритмов ее функционирования разработаны структурно-функциональная схема подсистемы и проект архитектуры возможной ее реализации.

Рисунок 3

– Проект архитектуры подсистемы прогнозирования

Функционирование системы прогнозирования позволит СОПКА осуществлять мероприятия предварительного прогнозирования возможных направлений развития компьютерных атак на информационную систему.

Литература:

1. Зокаев, Т. Н. Методика адаптивного прогнозирования результатов деятельности предпринимательских структур Ставропольского края по производству минеральной воды / Т.Н. Зокаев, О.И. Шаталова // Terra Economicus. – 2008. – Т. 6. – № 3-3. – С. 329-331
2. Суханов А.В. Мониторинг безопасности информационных систем на основе модели адаптивной защиты / А.В. Суханов, Л.Г. Нестерук, Ф.Г. Нестерук // Безопасность информационных технологий. Вып. 3, 2008. – С. 33.

References

1. Zokaev, T.N. The method of adaptive forecasting of the results of the activities of business structures of the Stavropol Territory for the production of mineral water / T.N. Zokaev, O.I. Shatalova // Terra Economicus. – 2008. – V. 6. – № 3-3. – P. 329-331
2. Sukhanov A.V. Monitoring the security of information systems based on the adaptive protection model / A.V. Sukhanov, L.G. Nesteruk, F.G. Nesteruk // Bezopasnost' informatsionnyh tehnologij. N. 3, 2008. – P. 33.