Бугайский К.А.

Определение успешности действий нарушителя в однородной среде

Аннотация: В работе представлена модель элемента информационной системы, позволяющая оценивать возможности реализации угроз нарушителем на основе расчета расхождения между текущими и эталонными параметрами.

Ключевые слова: доля восприимчивых элементов, вероятность единичного заражения, вероятность захвата элемента, вероятность продолжения атаки, модель элемента, оценка нарушителя

Построение современных ИС на основе облачных, туманных технологий и технологии «инфраструктура как код» приобретает все большую популярность. Решения Правительства РФ о создании государственной единой облачной платформы, позволяет рассматривать данные технологии как основное направление развития информационных систем (далее – ИС). Неизбежным следствием функционирования ИС на основе таких технологий является размывание границ ИС, что, в свою очередь, приводит к необходимости рассматривать любой отдельный элемент ИС как возможный источник угроз. В работе [1] предложена дискретная модель заражения ИС, дающая возможность оценить вероятность реализации угрозы (успешных действия нарушителя) в:

$$p_s = K_{ss}\frac{p_{SE}(s)p_{EI}(s)p_I(s)(1-L_2)}{1-L_1-L_2-L_3-L_4} \quad (1)$$

где:

– значения переменных L_1-L_4 определяются характеристиками средств защиты информации используемых в элементе ИС;

– K_{ss} – доля восприимчивых элементов;

– $p_{SE}(s)$ – вероятность единичного заражения;

– $p_{EI}(s)$ – вероятность того, что нарушитель захватит элемент;

– $p_I(s)$ – вероятность продолжения атаки на соседние элементы.

Далее будет рассмотрен один из возможных путей определения значений: K_{ss}, $p_{SE}(s)$, $p_{EI}(s)$ и $p_I(s)$ на основе модели элемента ИС.

Модель элемента ИС

Пусть дана ИС, состоящая из конечного множества элементов $E = \{e_1, \dots e_i, \dots e_n\}$, $i \in N = \{1, \dots, n\}$. Традиционно все элементы $e_i \in E$, $i \in N$ ИС описываются кортежем $e =< S, O, R >$, где: S – множество субъектов доступа, O – множество объектов доступа, R – множество прав доступа. В современных ИС в качестве множества субъектов доступа целесообразно рассматривать исполняемые файлы, работающие в пространстве данного пользователя элемента. Можно утверждать (см., например, [2]), что исполняемые файлы непосредственно являются носителями уязвимостей и реализуют ошибки при выполнении правил распределения доступа. Тогда элементы ИС можно описать кортежем: $e =< V, R, A >$, где: V – множество уязвимостей, A – множество исполняемых файлов приложений, которые осуществляют доступ и обработку данных по требованию субъекта, R – множество прав доступа файлов к данным. В каждый конкретный момент времени элемент ИС может быть описан перечнем исполняемых файлов (процессов) или набором состояний $e = \{s_1, \dots, s_i, \dots, s_n\}$, $i \in N = \{1, \dots, n\}$ представленных выборками V известных уязвимостей и R прав доступа. Тогда элемент ИС: $e = \{(v_1, r_1), \dots, (v_i, r_i), \dots, (v_n, r_n)\}$, $i \in N = \{1, \dots, n\}$.

Каждому v_i и r_i может быть поставлена в соответствие оценка по В-бальной шкале – v_i^g и r_i^g соответственно и сформированы функции распределения оценок $P^v(v^g)$ и $P^r(r^g)$. Тогда элемент ИС: $e = \{P^v(v^g), P^r(r^g)\}$. Как правило, v_i^g и r_i^g формируются на основе экспертных заключений, а кроме того, для разных элементов ИС размеры выборок V и R будут различаться, что даст смещение оценок возможности реализации угроз в ИС. Но для каждой выборки V и R можно определить наихудший вариант распределения оценок v_i^g и r_i^g – когда все сопутствующие угрозе оценки имеют максимальное значение, что, в свою очередь, даст эталонные функции (равномерного) распределения $Q^v(\max v^g)$ и $Q^r(\max r^g)$ для $P^v(v^g)$ и $P^r(r^g)$.

Реальное распределение оценок для каждого из β диапазонов B-бальной шкалы будет отличаться от наихудшего (эталонного) варианта. Положим, что чем больше отклонение распределения $P^v(v^g)$ и $P^r(r^g)$ от наихудшего (эталонного) варианта $Q^v(\max v^g)$ и $Q^r(\max r^g)$, тем меньше возможность реализации угроз нарушителем. В ходе исследования будем осуществлять расчет расхождения текущего и эталонного распределений D^* на основе расхождения Реньи и последующей нормализации для шкалы B от 1 до 3 (с учетом качественных оценок «низкий», «средний», «высокий»). Тогда элемент ИС $e = (D^v, D^r)$, где D^v – оценка различия между текущим распределением уязвимостей и наихудшим из возможных, а D^r – оценка различия между текущим распределением прав доступа и наихудшим из возможных.

Расчет D^r основан на функциях отображения $r = a(o)$ и $r = b(s)$, где r, s, o – элементы соответствующих множеств. Функции отображения b, a дают 1, если для данного объекта доступа применим данное право доступа или 0 в противном случае. Тогда получаем множества $E^A(a) = \{r \in R | \exists\, o \in O, r = a(o)\}$, $E^B(b) = \{r \in R | \exists s \in S, r = b(s)\}$, $E^A, E^B = \{0,1\}$. Поскольку E^A и E^B транзитивны относительно R, то можно построить шкалу оценки реализации прав доступа на основании распределения как числа объектов доступа, так и числа субъектов доступа. Учитывая, что число субъектов доступа меньше числа объектов, то будем рассчитывать оценку для каждого субъекта доступа по числу доступных ему прав доступа одновременно с нормированием результатов для диапазона значений шкалы от 1 до 10 по формуле: $\forall s_i \in S: p_i^r = \frac{(k_i - r_{min})(b-c)}{r_{max} - r_{min}} + c$, где: k_i – число прав доступа (элементов множества R) доступных для субъекта s_i, r_{min} – минимальное число элементов множества R ($r_{min} = 1$), r_{max} – максимальное число элементов множества R, b – максимальное значение шкалы ($b = 10$), c – минимальное значение шкалы ($c = 1$). Далее, с использованием расхождения Реньи и приведения к шкале $B = [1, 3]$, получаем значение D^r для элемента ИС.

В настоящее время, разработан алгоритм (подробнее см. [3]) по выборке оценок уязвимостей на основе баз данных MITRE.ORG (далее – MITRE) учитывающего взаимосвязи между сущностями: CAPEC, CWE, CVE. Алгоритм формирует список уязвимостей,

каждому элементу которого сопоставлен вектор из (как минимум) трех экспертных оценок CVE: $L_i^v = \{v_1, \dots, v_i, \dots v_n\}$, $v_i = (v^b, v^e, v^c)$, $i \in N$, где: v^b – базовая оценка CVE, v^e – оценка эксплуатируемости, v^c – оценка влияния на конфиденциальность, целостность и доступность. Расчет D^v предлагается проводить по выборке базовых оценок уязвимостей v^b (как текущего распределения $P^v(v^g)$).

Если учесть, что коэффициенты D^v и D^r рассчитываются единообразно, то тогда можно рассматривать пространство $\Phi = D^v \times D^r$ как пространство состояний элементов ИС. В этом случае любое изменение состава ПО элементов ИС или правил доступа будет приводить к изменению координат точек пространства. Расчет центроида множества по точкам пространства даст интегральную оценку ИС с точки зрения возможности реализации угроз.

Введем метрику $\rho(x, y) = \sqrt{\sum_{i=1}^{n}(x_i - y_i)^2}$ и определим особые точки $x^0 = (3, 3)$ и $y^0 = (0, 0)$ на плоскости, что даст $\varphi_i = \frac{p(x_i, y_i)}{p(x^0, y^0)}$. Величину $1 - \varphi$ можно рассматривать как вероятность того, что данный элемент ИС $e = (D^v, D^r)$ будет использован нарушителем для реализации угроз при заданных распределениях уязвимостей и прав доступа, тогда $p_{SE}(s) = 1 - \varphi$.

Потенциал нарушителя как правило включает в себя возможности по эксплуатации существующих уязвимостей и возможные последствия при их успешной эксплуатации для элементов ИС. С этой точки зрения MITRE – кроме D^v и D^r – позволяет рассчитать оценки: сложности эксплуатации уязвимостей – D^e и их влияния на конфиденциальность, целостность и доступность – D^c. Таким образом, оценки D^* дают полное описание потенциала нарушителя. Пусть имеем множество оценок D, его среднее значение μ^d и среднее квадратичное отклонение σ^d. Определим границы разбиения на подмножества: $y^{min} = infD + \sigma^d$ и $y^{max} = supD - \sigma^d$. Произведем разбиение множества: $d_i \in D^{min}\ \forall d_i: infD \le d_i \le y^{min}$, $d_i \in D^{aver}\ \forall d_i: y^{min} < d_i < y^{max}$, $d_i \in D^{max}\ \forall d_i: y^{max} \le d_i \le supD$. Введем отношения $\frac{|D^{min}|}{|D|}$, $\frac{|D^{aver}|}{|D|}$, $\frac{|D^{max}|}{|D|}$. Тогда для различных оценок D^*получим интегральные

оценки потенциала нарушителя: I^e_{min}, I^e_{aver}, I^e_{max} – на основании оценок эксплуатируемости уязвимостей; I^c_{min}, I^c_{aver}, I^c_{max} – на основании оценок влияния уязвимостей на конфиденциальность, целостность и доступность; I^r_{min}, I^r_{aver}, I^r_{max} – возможности реализации угроз на основании оценок распределения прав доступа.

Тогда *потенциал нарушителя*, как вероятность того, что он захватит элемент ИС: $p_{EI}(s) = (1 - I^e_{min}),\ (1 - I^c_{min}),\ (1 - I^r_{min})$. Соответственно *доля восприимчивых элементов* $K_{ss} = I^e_{max} + I^e_{aver}$.

Полагаем, что вероятность продолжения атаки на соседние элементы $p_I(s)$ тем выше, чем больше сходство элементов ИС. Сходство элементов целесообразно проводить по критерию различия составов слабостей (CWE) и пользователей. MITRE дает возможность получить лексикографически упорядоченный список CWE для отдельного элемента ИС $L^w = \{w_1, \dots, w_i, \dots w_n\},\ i \in N$. Строится лексикографически упорядоченный список $L^u = \{s_1, \dots, s_i, \dots s_n\},\ i \in N$ пользователей для отдельного элемента ИС. Тогда вероятность продолжения атаки рассчитывается [4] по формуле: $p_I(s) = \sqrt{\left(1 - \frac{c}{a}\right)\left(1 - \frac{c}{b}\right)}$, где: a – число L^w или L^u одного элемента, b – число L^w или L^u другого элемента, c – число L^w или L^u общих для сравниваемых элементов.

Представляет интерес проведение исследований по оценке состояния ИС, то есть траекториям движения ее элементов в трехмерном пространстве $\Phi = D^c \times D^e \times D^r$ при различных условиях эксплуатации и различных вариантах атак. Это позволит определять численные значения функции распределения риска необходимую для механизмов анализа и управления рисками в различных ИС предложенных и исследованных в [5,6] с учетом конкретных параметров и условий функционирования ИС.

Заключение

В работе рассмотрена задача расчета исходных данных для оценки вероятности реализации угрозы (успешных действия нарушителя) в дискретной модели заражения ИС. Разработанная модель элемента ИС, позволяет в условиях неопределенности, присущей процессам формирования и оценке угроз и нарушителя в ИС, проводить расчеты доли восприимчивых элементов, вероятности единичного заражения, вероятности захвата элемента

нарушителем, вероятности продолжения атаки на соседние элементы. Также модель позволяет рассматривать вопросы защиты информации ИС в пространстве состояний ее элементов с учетом динамики изменений состава элементов ИС и правил доступа.

Показана возможность применения результатов для оценки рисков, реализации угроз, потенциала нарушителя, а также для определения актуальных угроз безопасности информации.

Литература:

1. *Остапенко А.Г., Радько Н.М., Калашников А.О. Остапенко О.А., Бабаджанов Р.К.* Эпидемии в телекоммуникационных сетях. – М: Горячая линия – Телеком, 2018. – С. 123-149 .

2. Банк данных угроз безопасности информации. Термины // FSTEC.RU: ФСТЭК России. – URL: https://bdu.fstec.ru (дата обращения 27.09.2021).

3. *Калашников А.О., Бугайский К.А.* Методика оценки возможности реализации информационных угроз // Информация и безопасность. – 2020. – Т. 23. № 2(4). – С. 163-178.

4. *Костина Н.В.* Применение индексов сходства и различия для районирования территорий на основе локальных флор // Известия Самарского научного центра Российской академии наук. – 2013. – Т.15. № 3 (7). – С. 2160-2168.

5. *Калашников А.О.* Модели и методы организационного управления информационными рисками корпораций. – М.: Эгвес, 2011. – 311 с.

6. *Новиков Д.А., Остапенко А.Г., Калашников А.О., Остапенко Д.Г., Соколова Е.С., Уразов М.Ю.* Информационные риски и эпистойкость безмасштабных сетей // Информация и безопасность. – 2015. – Том 18. № 1. – С. 5-18.

Муромцев В.В., Муромцева А.В.

Цифровизация – угрозы и риски

Аннотация: Рассматриваются процессы, происходящие в современном информационном пространстве, которые в условиях глобализации цифровых информационных потоков ставят перед современным обществом целый ряд серьезных проблем и прежде всего в сфере безопасности.