Информационная безопасность

КАЛАШНИКОВ Андрей Олегович *– генеральный директор ООО «Центр технологий безопасности ИБС»*

ПОСТРОЕНИЕ ЭФФЕКТИВНОЙ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Последние несколько лет российский ИТ – рынок демонстрирует высокую динамику развития, которая по различным оценкам составляет 10 – 20 % в год. При этом сектор информационной безопасности (ИБ) развивается еще более быстрыми темпами. К основным факторам, определяющим подобные темпы роста можно отнести в первую очередь постоянно возрастающее количество информационных угроз и рисков, а так же недостаточный уровень обеспечения ИБ предприятий и организаций различных форм собственности. Поэтому, именно сейчас особенно актуальными становятся вопросы повышения эффективности затрат на построения наиболее эффективной системы обеспечения ИБ (СОИБ).

Для решения указанной задачи в последнее время было предложено значительное количество подходов (см., например, [1, 2, 3] и другие). Тем не менее, в большинстве работ мало учитывается тот факт, что реальная СОИБ функционирует в условиях случайного воздействия различных факторов, к числу которых относятся и угрозы ИБ. И, если наличие или отсутствие уязвимости в системе обеспечения ИБ является фактором управляемым, то возникновение угрозы и ее реализация представляют собой события вероятностные. Таким образом, при построении эффективной СОИБ и оценке эффективности защиты должны в равной степени учитывать как объективные, так и вероятностные факторы. Одним из возможных подходов к решению данной задачи является использование процедур имитационного моделирования на основе полученных на этапе анализа рисков вероятностных характеристик. Примером подобного подхода могут служить работы [4, 5].

В настоящее время при проектировании СОИБ, по-видимому, наиболее трудной и ответственной является задача выбора инфраструктурного решения данной системы. Под инфраструктурным решением здесь понимается структура и состав программно-технических средств защиты, реализующие определенный набор контрмер направленных на противодействие выявленным угрозам. Конкретный вариант инфраструктурного решения СОИБ в дальнейшем будем называть «проектом».

Задача выбора проекта решается в рамках выделенного объема ресурсов на основе результатов полученных на этапах: определения уровня допустимого риска (*первый этап*), аудита ИБ и анализа текущих рисков ИБ (*второй этап*) и выбора контрмер для снижения уровня текущего риска до уровня допустимого риска (*третий этап*). Положим, что на указанных этапах были определены: набор угроз $U = \{U_1, ..., U_M\}$, соответствующий им набор контрмер $K = \{K_1, \ldots, K_N\}$, возможные программно-технические средства защиты, реализующие указанные контрмеры $T(K_i) = \{T^i_1, \ldots, T^i_{N(Ki)}\}$, где $i = 1, \ldots, N$, уровень допустимого риска W^* и объем выделенного ресурса π^*. Предположим, далее, что на основе различных вариантов программно-технических средств защиты $T(K_i)$ было подготовлено несколько проектов $P = \{P_1, \ldots, P_L\}$, реализующих набор контрмер K и удовлетворяющих ограничению на объем выделенного ресурса π^*. Тогда задача выбора проекта СОИБ может быть сформулирована следующим образом: из множества допустимых проектов P выбрать тот, который наиболее эффективно противостоит угрозам из множества U.

Критерии эффективности могу быть различными, однако, учитывая, что основной целью ИБ является максимальное снижение текущего уровня информационного риска, представляется целесообразным рассматривать в качестве критерия разность между расчетным уровнем текущего риска конкретного проекта $W(P_i)$ и заданным уровнем допустимого риска W^*: $H(P_i) = W(P_i) - W^*$. При этом естественно считать, что один проект лучше другого, если соответствующее значение H меньше (здесь, учитывая имеющийся, как правило, дефицит ресурса полагаем, для простоты, что $W(P_i) > W^*$). Значение $W(P_i)$ зависит не только от выбранного проекта, но и от того, как часто возникают те или иные угрозы и насколько успешно они реализуются. Поскольку процесс реализации угроз носит исключительно вероятностный характер, то указанные параметры можно рассматривать как реализацию некоторой многомерной случайной величины (с.в.) ν, параметры распределения которой оцениваются на этапе анализа текущих рисков ИБ.

Сгенерируем для каждого P_i множество $\nu_i = \{\nu_1, \ldots, \nu_{Ni}\}$, реализаций с.в. ν, рассчитаем значения $H(P_i)$ для каждой реализации и обозначим полученные значения ξ^i_j, где $i = 1, \ldots, L$, $j = 1, \ldots, N_i$. Можно считать, что значения ξ^i_j являются реализацией некоторой с.в.. По результатам экспериментов (стохастического имитационного моделирования) каждому варианту проекта P_i сопоставляется выборка из некоторой генеральной совокупности $\xi^i = \{\xi^i_1, \ldots, \xi^i_{Ni}\}$. Предлагаемый подход состоит в том, что бы использовать полученный статистический материал для выбора эффективного проекта.

Рассмотрим множество P и множество соответствующих выборок $\Sigma = \{\xi^i$, где $i = 1, \ldots, L\}$. Процесс выбора эффективного проекта может иметь следующий вид:

1. Введем понятие «меньше» ($\prec$) для с.в. и на Σ установим частичный порядок. При этом предполагаем, что если ξ^m «меньше» ξ^l ($m \neq l$), то соответственно P_m лучше P_l.

2. Во множестве Σ ищем минимальный элемент $\xi^m{}_{min}$, такой, что $\xi^m{}_{min} \prec \xi^l$ (для $\forall\, l \neq m$). Если такого элемента не существует, то рассматриваем «нижний класс» множества Σ: $\Sigma_{min} = \{\xi^i$, где $i \in I \subseteq \{1, \ldots, L\}$, причем для $\forall\, i \in I$ и $j \in \{1, \ldots, L\} \setminus I$: $\xi^i \prec \xi^j\}$.

3. В качестве эффективного проекта рассматриваем P_m или подмножество $\{P_i$, где $i \in I\}$. В последнем случае необходимо проведение дальнейших исследований.

Существуют различные способы введения понятия «меньше» для с.в., например, с помощью функционала $F(F_\xi)$ определенного на классе функций распределения (ф.р.) с.в. F_ξ. При этом можно считать [5], что $\xi^1 \prec \xi^2$, если $F(F_{\xi 1}) < F(F_{\xi 2})$. В работе [4] рассмотрены следующие способы упорядочивания с.в.:

- по стохастическому росту: $\xi^1 \overset{1}{\prec} \xi^2$: $F_{\xi 1}(x) \geq F_{\xi 2}(x)$, для $\forall\, x$;

- по нижней грани носителя распределения: $\xi^1 \overset{2}{\prec} \xi^2$: $a_1 \leq a_2$, где a_i – существенная нижняя грань множества A_i, являющегося носителем распределения с.в. ξ^i, где $i = 1, 2$.

В обоих случаях упорядочение с.в. основывается на соотношении их ф.р.

Отношения $\overset{1}{\prec}$, $\overset{2}{\prec}$ можно применять по отдельности или вместе, в последнем случае имеет место двухкритериальный выбор.

Для сравнения с.в. на основании их выборок из генеральной совокупности по отношению $\overset{1}{\prec}$ можно использовать ранговый критерий Вилкоксона, или, например, критерий серий, для которых имеются статистические таблицы. Как отмечено в [4], реализация на ЭВМ критерия серий более эффективна, поскольку требует значительно меньшего числа операций и объема ресурсов, чем для критерия Вилкоксона.

Для сравнения с.в. по отношению $\overset{2}{\prec}$ необходимо получить оценку нижней грани носителя распределения. В [4] предлагается рассматривать в качестве такой оценки минимальный корень уравнения $f^*(x) = \varepsilon$, $\varepsilon > 0$, где $f^*(x)$ – некоторая сглаженная (например, ядерная) оценка плотности $f(x)$ с.в., а ε – разумно выбранное малое число.

Теперь алгоритм выбора эффективного проекта может иметь следующий вид:

1. Сопоставим каждому элементу множеств P и Σ его порядковый номер: $N(P_m) = m$ и $N(\xi^m) = m$.

2. Положим $m = 1$, $l = 2$.

3. Проверим выполнение соотношения $\prec$ для элементов стоящих на m и l местах во множестве Σ, при этом: если $\xi^m \prec \xi^l$, то перейдем к шагу 4, в противном случае поменяем местами элементы ξ^m и ξ^l, и соответствующие им P_m и P_l и будем полагать, что теперь $N(P_m) = N(\xi^m) = l$ и $N(P_l) = N(\xi^l) = m$.

4. Если $l \leq L - 1$, то положим $l = l + 1$ и перейдем к шагу 3, в противном случае перейдем к шагу 5.

5. Положим $m = 1$, $l = 2$, $k = 1$.

6. Проверим выполнение соотношения $\prec$ для элементов стоящих на m и l местах во множестве Σ, при этом: если $\xi^m \prec \xi^l$, то перейдем к шагу 8, в противном случае положим $k = k + 1$ и перейдем к шагу 7.

7. Если $l \leq L - 1$, то положим $l = l + 1$ и перейдем к шагу 6, в противном случае перейдем к шагу 8.

8. Выберем в качестве множества Σ_{min} первые k элементов множества Σ и будем полагать их оптимальными в смысле отношения $\prec$. В качестве эффективных проектов выберем первые k элементов множества P.

Рассмотренный подход, как уже говорилось выше, не является единственно возможным [1, 2, 3], но, в тоже время, обладает определенными преимуществами. К ним, в первую очередь, можно отнести то, что практически во всех указанных работах построение эффективной СОИБ осуществляется исходя из предположения о наличии некоторой детерминированной оценки возможного ущерба. Однако независимо от воли и предвидения разработчиков возникают и иные, заранее неизвестные при проектировании СОИБ обстоятельства, способные снизить эффективность защиты или полностью скомпрометировать предусмотренные проектом меры ИБ. Рассмотренный в статье подход с использованием процедур стохастического имитационного моделирования на основе полученных на этапе анализа рисков вероятностных характеристик как раз и позволяет учесть данное обстоятельство.

Литература:

1. Петренко С.А., Симонов С.В. Управление информационными рисками. Экономически оправданная безопасность. – М.: Компания АйТи; ДМК Пресс, 2004. – 384 с.

2. Провоторов В.Д. Защитить, чтобы не проиграть. Методика оптимального планирования бюджета на защиту информации в конкурентных условиях // Information Security /Информационная безопасность. № 2, апрель 2004. – с.26 – 28.

3. Теренин А.А. Проектирование экономически эффективной системы информационной безопасности // Информационно – методический журнал «Защита информации. ИНСАЙД», № 1 (1), январь – февраль 2005. – с. 26 – 35.

4. Дерягин Ю.В., Калашников А.О. Использование метода стохастической оптимизации для выбора рациональной компоновочной структуры (КС) ГПС / Межвузовский сборник «Автоматизация, роботизация и интеллектуализация производства». – М.: МИЭМ, 1988. – с. 42 – 47.

5. Калашников А.О., Ротарь В.И. Об одном классе предпочтений в пространстве распределений (учет роста и разброса) / В кн.: Модели и методы стохастической оптимизации. – М.: ЦЭМИ, 1983. – с. 77 – 89.