БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Дмитриев А.С., Залогин Н.Н., Иванов В.П. и др.* Способ маскировки радиоизлучений средств вычислительной техники и устройство для его реализации // Авторское свидетельство № 1773220, приоритет от 21.09.1981г.

2. *Дмитриев А.С., Иванов В.П., Лебедев М.Н.* Модель транзисторного генератора с хаотической динамикой.// - Радиотехника и электроника. 1988. Т. 23. № 5. – С.1085-1088.

3. *Лебедев М.Н., Иванов В.П.* Генераторы с хаотической динамикой. Приборы и техника эксперимента. – М. Наука, 2002. № 2, – С. 94-99.

4. *Кальянов Э.В., Иванов В.П., Лебедев М.Н.* Принудительная и взаимная синхронизация генераторов при наличии внешнего шума.// - Радиотехника и электроника. 1990. Т. 35. № 8, С.1682-1687.

5. *Кальянов Э.В., Иванов В.П., Лебедев М.Н.* Экспериментальное исследование транзисторного генератора с запаздывающей обратной связью // Радиотехника и электроника. 1982. Т.27. № 5. – С. 982-986

6. *Судаков Ю.И.* Амплитудная модуляция и автомодуляция транзисторных генераторов (теория и расчет). – М.: Энергия, 1969. – 392 с.

7. *Харкевич А.А.* Очерки общей теории связи. – М Государственное издательство научно-технической литературы. 1955.

8. *Лебедев М., Н., Иванов В.П., Сак В.В.* Устройства радиомаскировки информационных излучений СВТ//Информационно-методический журнал «Защита информации. Конфидент». № 1. 2001. – С.35-37.

9. *Безруков В.А., Иванов В.П., Калашников В.С., Лебедев М.Н.* Патент на изобретение № 2170493 "Устройство радиомаскировки" по заявке № 2000112294 от 15.05.2000г. Бюллетень изобретений № 19, 10.07.2001г. Россия.

10. *Безруков В.А., Иванов В.П., Лебедев М.Н.* Патент на изобретение № 2224376 "Устройство радиомаскировки" по заявке № 20002115415 от 07.06.2002г. Бюллетень изобретений № 5, 20.02.2004г. Россия.

11. *Иванов В.П., Лебедев М.Н., Волков А.И.* Устройство радиомаскировки.

12. Патент № 38257, Россия. Дата публ. 2004. 27. 05.

В.В. Анищенко, А.М. Криштофик
Беларусь, г. Минск, ОИПИ НАН Беларуси

КОМПЛЕКСНАЯ ОЦЕНКА УГРОЗ БЕЗОПАСНОСТИ

Введение

Для построения комплексной защиты информации необходимо выявить угрозы безопасности (УБ), оценить их последствия – опасность каждой угрозы и создать адекватные меры защиты. Формирование методологии выявления УБ осуществляется по следующим направлениям:

- систематизация и статистическая оценка атак и попыток несанкционированного доступа к объектам информации;
- экспериментальное тестирование информационных систем на предмет обнаружения уязвимых мест, использование которых возможно для реализации угроз;
- создание аналитических и имитационных моделей процессов функционирования ИС, угроз безопасности и генераторов атак;
- экспертный анализ и экспертные оценки с привлечением специалистов: системных администраторов, администраторов безопасности, аудиторов ИБ и других специалистов в области безопасности информации.

Оценка проводится, как правило, с использованием моделей общей оценки угроз, которые являются основой оценки как самих УБ, так и потерь, которые могут иметь место при их проявлении. Модели данного типа важны еще и тем, что именно на них, в основном выявлены те условия, при которых такие оценки могут

быть адекватны реальным процессам защиты информации. К настоящему времени разработаны различные табличные, диаграммные, формализованные, имитационные модели УБ. Однако, несмотря на достоинства этих моделей, ни одна из них не позволяет одновременно учесть три основных параметра — уязвимость, активизируемая атакой, метод ее реализации и возможные последствия. Другими словами, остаются неразрешенными вопросы комплексности модели.

Комплексная модель угрозы безопасности

Рассмотрим множество угроз активам $Y = \{y_i, \mu(y_i)\},\ i = \overline{1,I}$, которые исходят из окружающей среды объекта оценки (ОО) и создают опасность для его работы и против которых требуется защита. Носителем нечеткого множества Y является универсальное четкое множество всех известных угроз $Y^{\Diamond}$, на котором $\mu(y_i) > 0$. Элементы y_i множества угроз $Y = \{y_i, \mu(y_i)\}, i = \overline{1,I}$ характеризуются нечетким случайным коэффициентом опасности, который является его динамической характеристикой (рис. 1) и в общем случае определяется выражением

$$x_i(t) = \begin{cases} 0 & при\ \ t \le t_{i0} \\ K_i\left(1 - e^{-\lambda_i (t - t_{i0})}\right) & при\ \ t > t_{i0} \end{cases},$$

где $K_i = \prod_{\xi_1=1}^{\Xi_1} k_{i\xi_1}$ – максимальное значение коэффициента опасности угрозы, определяемое через Ξ_1-е характеристики нарушителя (мотивация, квалификация, используемый ресурс и др. в зависимости от метода оценки);

$\lambda_i = \prod_{\xi_2=1}^{\Xi_2} \lambda_{i\xi_2}$ – параметр угрозы, характеризующий скорость ее реализации и определяемый через Ξ_2-е характеристики нарушителя (метод и средство реализации угрозы и др. в зависимости от метода оценки);

t_{i0} - параметр угрозы, характеризующий время начала реализации угрозы - начало стадии вторжения в систему, определяемое длительностью фазы рекогносцировки и зависящее Ξ - х характеристик нарушителя, $\Xi = \cup(\Xi_1, \Xi_2)$ (рис. 2).

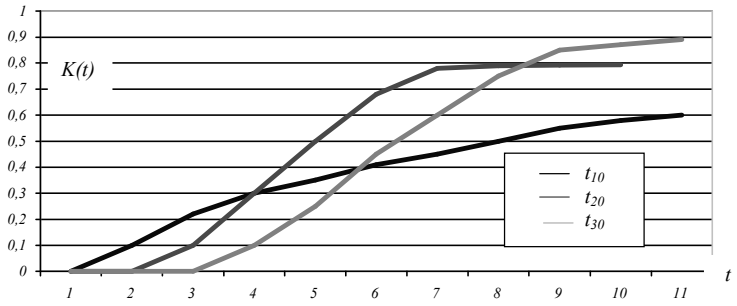

Рис. 1. Зависимость коэффициента опасности угрозы от времени

В основу разработки комплексной модели угрозы безопасности положены ее жизненный цикл и математическая модель объекта информационных технологий [1]. Жизненный цикл угрозы (процесс ее реализации) состоит из четырех стадий ее

реализации: рекогносцировка, вторжение, атакующее воздействие и развитие или завершение атаки.

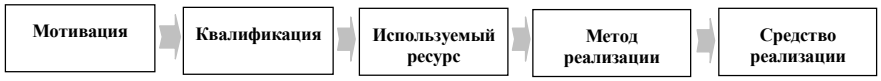

Рис. 2. Диаграмма модели нарушителя

Для построения математической модели угрозы использовались базовая модель объекта информационных технологий (ОИТ), представляющая собой граф взаимодействия элементов безопасности «угрозы – уязвимости – активы – риски – ущерб», характеризующих внешнюю среду безопасности, объект оценки и последствия этого взаимодействия, в плане взаимодействия элементов безопасности и комплексных показателей защищенности, положения Общих критериев.

В отличие от базовой модели ОИТ используется множество остаточных уязвимостей с учетом наличия в нем определенных средств обеспечения безопасности [2], множество которых при использовании общесистемного критерия «эффективность-стоимость» определяется с учетом времени реализации угрозы и реакции средства защиты, нейтрализующего данную угрозу.

Множество остаточных уязвимостей определено как объединение двух подмножеств $V^* = V_1^* \cup V_2^* = \{v_{k^*}\}, k^* = \overline{1, K^*}$,

где $V_1^* = V \times M = \left\{ v_{k_1^*} = \langle v_k, m_q \rangle \right\}$, $k_1^* = \overline{1, K_1^*}$, $K^* = K \times Q$ - подмножество уязвимостей, перекрытых средствами обеспечения безопасности и обусловленное ограниченной их стойкостью, определяемое декартовым произведением множества уязвимостей V и множества средств обеспечения безопасности M объекта оценки;

$V_2^* = \left\{ v_{k_2^*} \middle/ \hat{r}_c = \langle y_i, v_k, a_j \rangle < r_{c\,доп} \right\}, V_2^* \subset V$ - подмножество уязвимостей, не перекрытых средствами обеспечения безопасности.

Элементы множества остаточных уязвимостей характеризуют слабости средств обеспечения безопасности, а также пути реализации угроз, не перекрытые ими, т.е. свойства ОИТ и системы обеспечения безопасности активов, способствующие успешному осуществлению угрозы или которые могут быть использованы для осуществления угрозы.

Дополнительно в модель атаки введено множество нарушителей информационной безопасности $X = \{x_l\}, l = \overline{1, L}$, характеризуемых такими показателями, как квалификация, используемый ресурс и мотивация, учет которых в модели ОИТ условно подразумевался в характеристиках множества угроз $Y = \{y_i\}, i = \overline{1, I}$.

В результате взаимодействия этих множеств возникает остаточный риск нанесения ущерба владельцам активов, обусловленный наличием остаточных уязвимостей

$$R = X \times Y \times V \times M \times A = X \times Y \times V^* \times A = \{r_{c^*} = \langle x_l, y_i, v_{k^*}, a_j \rangle\} = \langle x_l, y_i, v_k, m_q, a_j \rangle,$$

$$c^* = \overline{1, C^*}, \quad C^* = I \times K^* \times J,$$

$$R = R_1 \cup R_2, \quad R_1 = X \times Y \times V_1^* \times M \times A, \quad R_2 = X \times Y \times V_2^* \times A.$$

Модель типовой атаки представлена на рис. 3.

Она отражает процесс нанесения ущерба владельцам активов. Использование модели системы защиты [3] относительно одной угрозы позволяет провести ее детализацию, рассмотреть возможность проведения атаки последовательно, используя несколько уязвимостей, или в обход средств обеспечения безопасности.

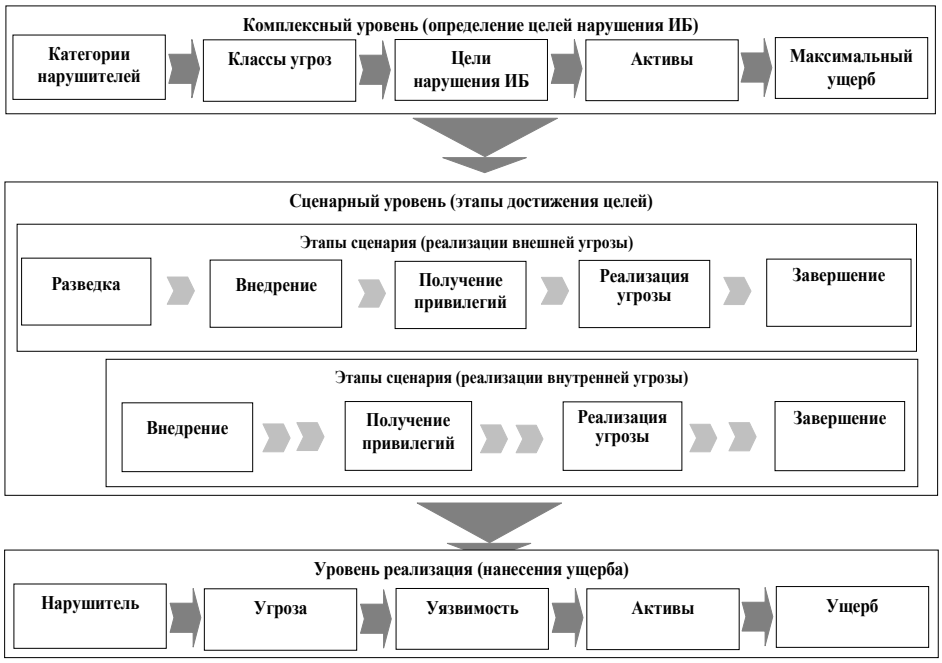

Рис. 3. Модель угрозы безопасности

В качестве показателя, характеризующего комплексный потенциал атаки, будем использовать средний риск нанесения ущерба $R_{cpik} = \sum_j r_{ikj} P_i$ либо ущерб, наносимый владельцам активов $U_{cpik} = \sum_j s_{ijk} r_{ikj} P_i$, в зависимости от назначения ОИТ [4]. В условиях частичной априорной неопределенности относительно вероятностей реализации атак используется минимаксный критерий эффективности. В этом случае в качестве потенциала атаки целесообразно использовать максимальный риск нанесения ущерба $R_{max\,ik} = \sum_j r_{ikj}$ или соответствующий ему ущерб $U_{max\,ik} = \sum_j s_{ijk} r_{ikj}$.

Оценочное значение элемента множества рисков определяется выражением $r^*_{iK^*j} = K_{x_l} K_{y_i} \prod_{k^*}^{K^*} \mu_{y_i v_{k^*}} K_{v_{k^*}} K_{o_j}$, где K_{ξ_ρ} - оценки нарушителя, угрозы, уязвимости и актива, соответственно определяемые на основании характеристик элементов безопасности, $\mu_{y_j v_k}$ - коэффициент корреляции угрозы и уязвимости, оп-

ределяемый на основании характеристик квалификации нарушителя и доступности уязвимости [5].

Таким образом, комплексным показателем потенциала атаки является риск от реализации определенной угрозы через установленные уязвимости на определенный вид активов.

Порядок оценки и ранжирования угроз безопасности

Для ранжирования угроз безопасности целесообразно использовать частный интегральный показатель защищенности, средний риск нанесения ущерба при реализации угрозы определенного вида $R_{cp\,i} = \sum_k \sum_j r_{ikj} P_i = \sum_j r_{ij} P_i$, $j = \overline{1,J}$, характеризующий *степень опасности определенной угрозы,* как отдельный элемент безопасности, характеризующий возможности по нанесению ущерба при реализации угрозы определенного вида, т.е. степень опасности угрозы [5, 6]. Порядок комплексной оценки и ранжирования угроз безопасности приведен на рис. 4 [7].

В зависимости от априорного описания оценки, в том числе нечеткий статистический и нечеткий.

В первом случае для определения элементов множества рисков используются вероятностные оценки нечеткого случайного события:

– вероятность $p(r_{ikj}) = \int_{-\infty}^{\infty} f(r_{ikj})\mu(r_{ikj})\,dr_{ikj}$;

– математическое ожидание $Er_{kji} = \left(E\underline{r}_{ikj}(\mu), E\bar{r}_{ikj}(\mu)\right)$;

– дисперсия $Dr_{ikj} = 0{,}5\int_0^1 \left[\left(\underline{r}_{ikj}(\mu) - E\underline{r}_{ikj}(\mu)\right)^2 + \left(\bar{r}_{ikj}(\mu) - E\bar{r}_{ikj}(\mu)\right)^2 \right] d\mu$, где $\underline{r}, \bar{r}$ - соответствующие ветви функции принадлежности при обратном отображении $\mu = \left(\underline{\mu}, \bar{\mu}\right), 0 \le \mu \le 1$.

Для определения потенциала атаки используются формулы теории вероятностей, поскольку в данном случае кроме нечеткости по Заде используются дополнительные операции, такие как включение, алгебраическая сумма и алгебраическое произведение по Бандлеру и Кохоуту, эквивалентность.

При втором подходе для определения потенциала атаки операция суммирования определяется выражением $\sum_\xi r_\xi = \left\{ \sum_\xi r_{f1}; \sum_\xi \mu\left(\sum_\xi r_{f1} \right) \right\}$, в котором суммирование элементов носителей является скалярным, а значение функции принадлежности вычисляется согласно правила центра тяжести, используем в операции дефазификации $\sum_\xi \mu\left(\sum_\xi r_\xi \right) = \dfrac{\sum_\xi r_\xi \mu(r_\xi)}{\sum_\xi r_\xi}$.

Таким образом, комплексный подход к оценке и ранжированию УБ предусматривает использование частного интегрального показателя защищенности, характеризующего возможности по нанесению ущерба при ее реализации, по которому и производится ранжирование.

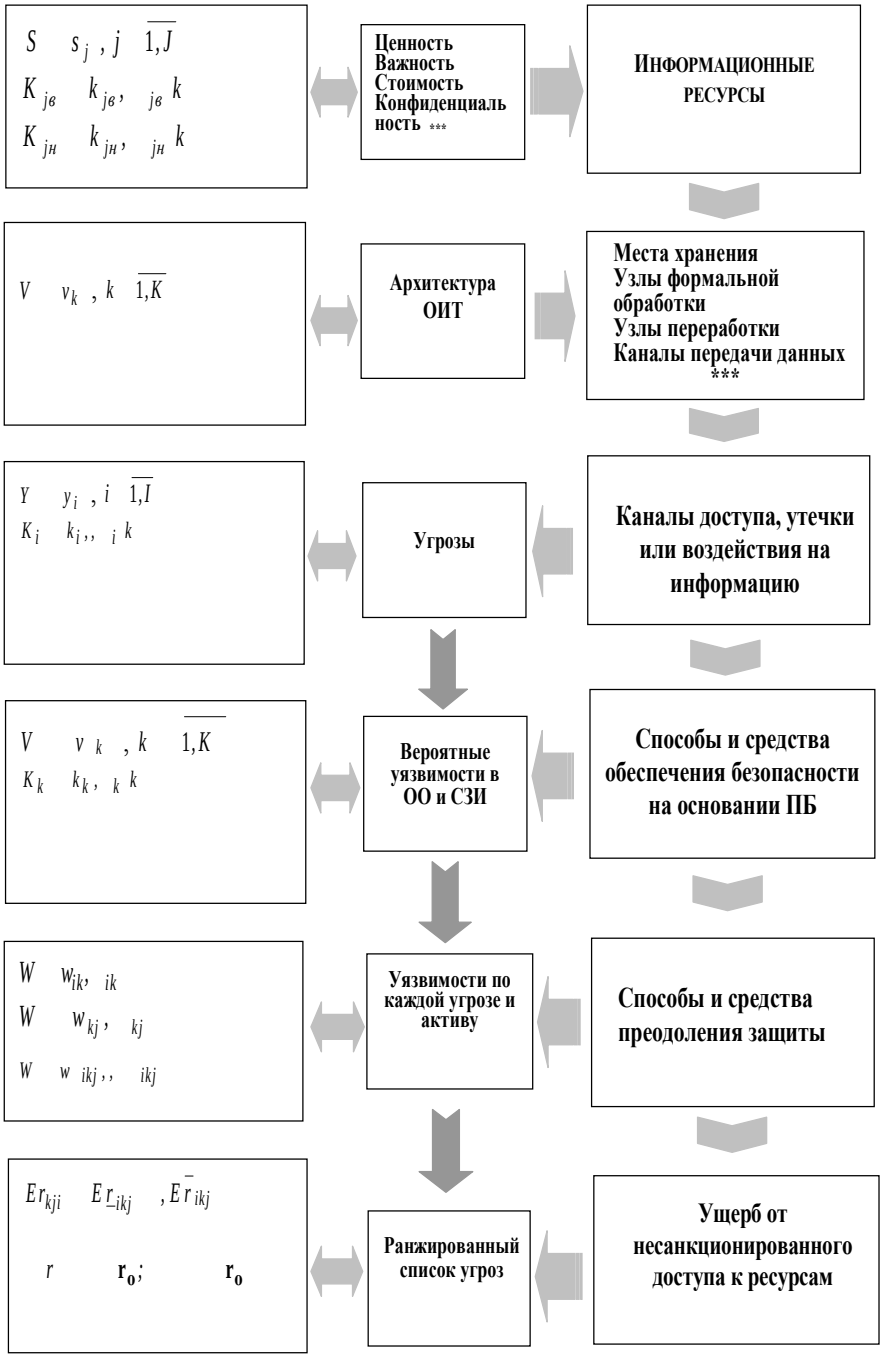

Рис. 4. Порядок оценки и ранжирования угроз безопасности

Заключение

Рассмотрен важный в методическом и прикладном плане вопрос оценки и ранжирования угроз безопасности, основанный на системном подходе, предусматривающий проведение оценки негативных последствий от нарушения ИБ от

реализации определенной угрозы. В зависимости от степени детализации он может быть использован при разработке политики безопасности, проектировании профиля защиты (задания по безопасности, построении системы защиты).

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Анищенко В.В., Криштофик А.М.* Базовая модель объекта информационных технологий. /Информатика № 3 (7). – Минск: ОИПИ НАН Беларуси, 2005. – С. 116-125.

2. *Анищенко В.В., Криштофик А.М.* Базовая модель системы защиты активов объекта информационных технологий. /Материалы докладов и краткие сообщения II Белорусско-российской научно-техн. конф. «Технические средства защиты информации», 17 мая-21 мая 2004, Минск-Нарочь. Доклады БГУИР. – 2004. № 5. – С. 9.

3. *Криштофик А.М., Анищенко В.В.* Управление информационной безопасностью на основе системного анализа рисков//Доклады пятой междун. конференции «Обработка информации и управление в чрезвычайных и экстремальных ситуациях». – Минск.: ОИПИ НАН Беларуси, 2006, – С.117-122.

4. *Анищенко В.В., Криштофик А.М.* Показатели защищенности информационных систем // Материалы конференции «Обеспечение безопасности информации в информационных системах», Минск, 11 ноября 2004 г.- Минск: Академия управления, 2004, – С. 30-33.

5. *Криштофик А.М.* Априорная оценка потенциала атаки /Управление защитой информации, т.10 №1, 2006, Минск-Москва. – Минск.: ООО «Марфи», 2006, – С. 47-49.

6. *Криштофик А.М.* Модель комплексной оценки потенциала атаки // Материалы X междун. конференции «Комплексная защита информации». – Минск.: Амалфея, 2006, – С.111-113.

7. *Анищенко В.В., Криштофик А.М.* Использование комплексного подхода для ранжирования угроз информационной безопасности // Материалы конференции «Обеспечение безопасности информации в информационных системах», Минск, 11 ноября 2004 г. – Минск. Академия управления, 2004, – С. 33-36.

А.М. Криштофик, В.В. Анищенко
Беларусь, г. Минск, ОИПИ НАН Беларуси

МЕТОДОЛОГИЯ ПОСТРОЕНИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Введение

Существующая нормативно-методическая база по вопросам безопасности информационных технологий (ИТ) имеет определенные недостатки. Основными из них являются: игнорирование системного подхода, как методологии построения системы защиты информации (СЗИ); отсутствие механизмов достоверного подтверждения качества и достаточности средств защиты, недостаточность проработки вопросов моделей системы защиты, системы показателей и критериев безопасности ИТ; статический подход к оценке уязвимостей [1].

Это обусловливает необходимость развития нормативно-методической базы, методик и моделей оценки защищенности на основе системного подхода.

1. Системный подход к построению системы защиты

Методология обеспечения безопасности ИС основана на концепциях анализа и управления рисками [1]. Основным недостатком существующих подходов к оценке рисков информационной безопасности (ИБ) является предположение об идеальной стойкости средств защиты.

Методологический подход к построению и оценке СЗИ с использованием системного анализа рисков основан на новых определениях остаточных уязвимостей, риска и ущерба [2]. Он предполагает проведение анализа взаимодействия элементов безопасности, характеризующих внешнюю среду, объект оценки и по-