УДК 004.056.53

В.В. Мохор, д-р техн. наук, ИПМЭ им. Г.Е. Пухова НАНУ, г. Киев,
А.М. Богданов, д-р техн. наук, ИССЗИ НТУУ «КПИ», г. Киев,
О.Н. Крук, ИПМЭ им. Г.Е. Пухова НАНУ, г. Киев,
В.В. Цуркан, ИССЗИ НТУУ «КПИ», г. Киев

ПОСТРОЕНИЕ ОЦЕНОК РИСКОВ БЕЗОПАСНОСТИ ИНФОРМАЦИИ НА ОСНОВЕ ДИНАМИЧЕСКОГО МНОЖЕСТВА АКТУАЛЬНЫХ УГРОЗ

Considered approach to building risk assessments of information security based on a dynamic set of actual threats.

Прежде чем приступить к изложению материала, отметим, во-первых, что в настоящее время в международной практике существует много методик управления рисками, в частности это Austrian IT Security Handbook, AS/NZS4360, BSI 100-3, CRISAM, EBIOS, HB167:200X, ISF IRAM, ISO 27005:2008, ISO 31000, MAGERIT, MARION, MEHARI, NIST SP800-3,OCTAVE, OSSTMMRAV, SOMAP и другие. Вместе с тем в подходах к построению оценок рисков все методики оказываются сходными и не имеют существенных различий. По этой причине мы выберем в качестве методической базы для нашей работы наиболее актуальную в настоящее время ISO 27005:2008, подразумевая, что полученные результаты могут быть распространены и на другие методики. Руководящими материалами при работе по данной методике являются стандарты ISO/IEC [1-3] и ассоциированные с ними стандарты ГОСТ Р [4-6].

Во-вторых, акцентируем внимание на использовании терминов *«оценка риска»* (*Risk Assessment)*, *«количественная оценка риска»* (*Risk Estimation*) и *«оценивание риска»* (*Risk Evaluation*), предписанном стандартами [4-6]. Отметим, что указанные понятия отражают различные сущности. Этому различию сущностей соответствует явное различие семиотики англоязычных терминов *Assessment, Estimation, Evaluation.* Соответствующие же русскоязычные термины «*оценка риска*», «*количественная оценка риска*» и «*оценивание риска*» являются весьма близкими семиотически и интенсионально, т.е. как в смысле использования знакового образа, так и в смысле связанных с ним психологических и модальных ассоциаций. По этой причине использование терминов «*оценка риска*», «*количественная оценка риска*» и «*оценивание риска*» в русскоязычных текстах стандартов [5, 6] существенно усложняет процесс восприятия их содержания. Ограничившись констатации этого факта, мы, тем не менее, попытаемся, по возможности, придерживаться терминологии, предписанной стандартами [4-6], устраняя, по мере необходимости, неопределенности и неоднозначности комментариями, опирающимися на первоисточники [1 - 3].

Стандарт ISO/IEC 27001 [2, 5] предписывает при разработке системы

управления информационной безопасностью, среди прочего, достичь следующих целей:

Список 1.

1. Определить подход к построению оценок (*Assessment*) рисков, для чего, в частности, следует выбрать или разработать соответствующую методику;
2. Идентифицировать риски, в том числе:
   a. идентифицировать угрозы информационным активам;
   b. идентифицировать уязвимости информационных активов, которые могут быть использованы угрозами;
3. Проанализировать и оценить (*Evaluate)* риски, для чего необходимо, помимо всего иного, оценить (*Assess*) реальную вероятность возникновения проблем с безопасностью в контексте превалирующих угроз/уязвимостей и произвести количественную оценку (*Estimation*) риска.

Прежде всего, отметим два важных для нас аспекта, присутствующих в пункте 3 *Списка 1*:

Во-первых, это одновременное использование трех сущностей *Assessment, Estimation, Evaluation*, что будет требовать от нас в дальнейшем особо внимательного отношения к использованию терминов и оборотов, производных от глагола «оценивать» и отглагольного существительного «оценка». В связи с этим мы вынуждены сразу перейти к использованию термина «*аттестация риска»* вместо термина *«оценивание риска»* (в смысле *Risk Evaluation*), вместо термина *«количественная оценка риска»* (*Risk Estimation*) использовать термин *«исчисление риска»,* а вместо термина «оценка риска» (*«Risk Assessment»*) - термин *«построение оценок риска»* и соответствующие, очевидные производные от этих терминов.

Во-вторых, мы можем констатировать, что при оценке рисков стандарт ISO/IEC 27001 делает акцент на ***превалирующих*** угрозах и уязвимостях.

Следует отметить, что в стандарте ISO/IEC 27001 нет указаний, каким образом можно достичь целей, обозначенных в списке 1. Общие рекомендации по сути того, каким образом поставленные цели могут быть достигнуты, приводятся в ISO/IEC 27005 [3, 6]. В соответствии с этими рекомендациями управление рисками безопасности информации является итерационным процессом, схематично представленным на *Рис. 1.*

Из *Рис.1* видно, что задачами, решаемыми, условно говоря, в процессе «прямого хода» являются:

a) установление контекста *(Context Establishment);*
b) построение оценок рисков (*Risk Assessment*);
c) обработка рисков (*Risk Treatment*);
d) принятие рисков (*Risk Acceptance*).

А задачами в процессе «обратного хода»:

e) обмен информацией по рискам (*Risk Communication*);
f) мониторинг и пересмотр рисков (*Risk Monitoring and Reviev*).

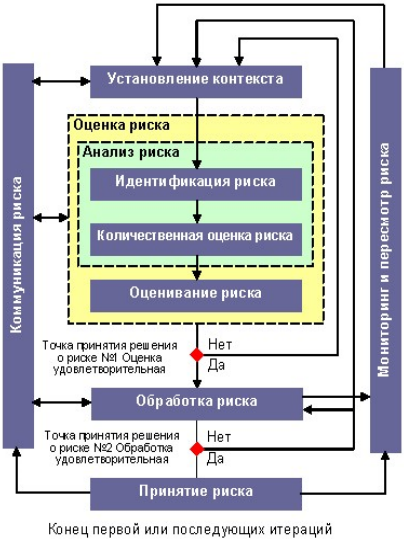

Рис.1. Процесс управления рисками безопасности информации.
(рисунок приведен по источнику [6]).

При этом задача построения оценок риска (*Risk Assessment*) включает два этапа, а именно:

1. этап анализа рисков (*Risk Analysis*)
2. этап аттестации рисков (*Risk Evaluation*).

В свою очередь, для этапа анализа рисков (*Risk Analysis*) необходимо пройти две стадии:

i. осуществить идентификацию рисков (*Risk Identification*);
ii. исчислить значение рисков (*Risk Estimation*).

Объектом нашего интереса является задача построения оценок рисков. Стандарт ISO/IEC 27005 дает лишь общие рекомендации по поводу того, как решать эту задачу: предписано, что риски должны быть идентифицированы, количественно определены (или качественно описаны) и ранжированы в соответствии с приоритетами и критериями аттестации рисков, уместными для организации целям. Выбор подхода к построению оценок рисков зависит от самой организации. Организация может использовать любой метод, но важно, чтобы к этому методу было обоснованное доверие, и метод был способен обеспечивать воспроизводимые результаты [3, 6].

Проведя анализ процесса решения задачи построения оценок рисков, описанного в ISO/IEC 27005, можно сделать вывод, что выбор метода построения оценок рисков будет сводиться, в конечном счете, к выбору метода оценки вероятностей потерь, возможных вследствие реализации результативных сценариев инцидентов для заданного множества уязвимостей и заданного множества угроз. В подтверждение сказанного изложим в нашем

переводе пункт 8.2.2.3 стандарта, где представлены рекомендации по оценке (*Assessment*) вероятности инцидентов информационной безопасности:

8.2.2.3. Оценка вероятности инцидента.

Входные данные:

Перечень идентифицированных сценариев развития инцидентов информационной безопасности, в том числе список идентифицированных угроз, уязвимых активов, используемых уязвимостей, а также установленных последствий для активов и бизнес-процессов.

Кроме того, списки всех существующих и планируемых мер безопасности, оценок их эффективности, показателей состояния внедрения и использования.

Рекомендации:

Для идентифицированных сценариев необходимо ***оценить вероятность каждого сценария и его последствий*** *с использованием качественных или количественных методов расчетов.*

Следует принять во внимание, сколь активно возникают угрозы и эксплуатируются уязвимости.

При этом следует учитывать:

- *существующий опыт и наличие статистических данных, применимых для расчета вероятности угрозы;*
- *для источников умышленных угроз:*
  - *возможности и ресурсы, доступные возможному злоумышленнику,*
  - *мотивации, восприятие привлекательности и уязвимости активов для возможного злоумышленника;*
  - *возможность изменения с течением времени параметров, принятых по предыдущим пунктам;*
- *для источников случайных угроз:*
  - *географические факторы, например, близость к химическим или нефтеперерабатывающим предприятиям;*
  - *возможность экстремальных погодных условий;*
  - *факторы, которые могут повлиять на человеческие ошибки и сбои в работе оборудования;*
- *уязвимости, как раздельно, так и агрегировано;*
- *существующие меры безопасности и показатели их эффективности в отношении конкретных уязвимостей.*

В зависимости от требуемой точности, активы могут быть либо сведены в группы, либо разделены по элементам. Соответственно сценарии могут быть привязаны либо к группам активов, либо к элементам активов.

Выходные данные:

Вероятности сценариев развития инцидентов информационной безопасности.

Несмотря на достаточно общий характер приведенных рекомендаций, они оказываются полезными для решения нашей задачи тем, что:

Список 2.

1. Предписывают иметь на входе список угроз и уязвимостей. Список угроз и уязвимостей формирует пространство, в котором нам нужно будет решать задачу расчета вероятностей. Т.к. уязвимости являются свойствами активов, то вместо пространства угрозы/уязвимости можно использовать пространство угрозы/активы.
2. Апеллируют к статистикам инцидентов.
3. Акцентируют внимание на необходимости учесть, сколь активно возникают угрозы и эксплуатируются уязвимости. (Этот согласуется с отмеченным выше положением стандарта ISO/IEC 27001:2005 о необходимости учета превалирующих угроз).
4. Допускают использование методов агрегирования и декомпозиции в отношении активов и сценариев.
5. Констатируют возможное наличие зависимости параметров расчетов от времени.

Акцентируя внимание на отмеченных положительных аспектах, не следует упускать из внимания ограничения и недостатки, присущие известным методам оценки вероятностей риска информационной безопасности [7]:

Список 3.

1. При сборе собственных статистик принципиально сложным и практически невыполнимым является требования неизменности условий.
2. При использовании заимствованных источников статистических данных, как правило, неизвестными является объемы исходных статистик и конкретные условия, для которых эти статистики являются справедливыми; следовательно, возникает вопрос о применимости этих статистик к данным условиям.
3. Использование качественных, экспертных методов страдает недоверием к результатам в связи с субъективной составляющей восприятия риска и неопределенностью оценки квалификации экспертов применительно к конкретным условиям решаемой задачи. Кроме того, есть основания считать, что качественные методы построения оценок риска имеют смысл лишь при надлежащей интерпретации результатов, которая сама по себе может потребовать количественных исходных данных. Дополнительным ограничением для восприятия качественных оценок риска является сложность обеспечения неизменных условий при проверке результатов на повторяемость.
4. Построение решений «по аналогии», осуществляемое на основе сравнимости (эквивалентности) условий, активов, уязвимостей, угроз и сценариев [9], оставляет оценки вероятностей фактические неизвестными.
5. Использование аналитических и прогнозирующих методов (метод «дерева неисправностей», «дерева событий») требует знания значений вероятности результативных реализаций сценариев развития угроз по каждой известной уязвимости [8].

В контексте сказанного попытаемся оценить размерность задачи построения оценок рисков в том объеме, как это следует из непосредственного восприятия рекомендаций стандарта ISO/IEC 27005. Априори каждому информационному активу с присущими ему уязвимостями можно поставить в соответствие статическое множество угроз, актуальных именно для данного актива. Очевидно, что статическое множество актуальных угроз является подмножеством множества всех угроз. В дальнейшем множество угроз будем обозначать $\mathbf{H}$, а подмножество актуальных угроз $\mathbf{H}_A$. В принципе, анализ множества угроз, его свойств и характеристик представляет собой отдельную тему исследований, развитие которой выходит за рамки данной работы. На данном этапе мы лишь отметим, что множество $\mathbf{H}$, очевидно, является счетным. Мы не знаем, является ли это множество конечным или счетно бесконечным, поэтому для оценки количества элементов множества $\mathbf{H}$ необходимо использовать понятие мощности множества. Но очевидно, что множество угроз, известных в данный k-й момент времени, представляет собой подмножество множества $\mathbf{H}$ и является конечным, и в этом случае количество элементов множества определяется его кардинальным числом. Подмножество угроз, известных в момент времени k, может отличаться от подмножества угроз, известных в момент времени $(k+1)$, т.е. подмножество известных угроз является некоторой функцией от k. Для отражения этого факта подмножество угроз, известных в момент дискретного времени k, будем обозначать $\mathbf{H}(k)$. Допустим, что кардинальное число (количество элементов) множества $\mathbf{H}(k)$ равно μ_k.

$$\left|\mathbf{H}(k)\right| = \mu_k .$$

(Сразу отметим очевидный факт, что в нашем случае последовательность чисел $\{\mu_k\}$, $k = 0, 1, \ldots$ является неубывающей). Для дальнейших рассуждений нам нужно оценить порядок величины μ_k, полагая, что k соответствует текущему моменту дискретного времени. Такую оценку можно сделать на основании существующих каталогов угроз. В настоящее время наиболее полный, по-видимому, список известных угроз безопасности информации приведен в каталоге IT-Grundschutz [10]. Этот каталог в редакции 2009 года содержит 483 наименования угроз, разбитых на 5 групп. В данной статье мы не будем анализировать и обсуждать методологию, положенную в основу построения каталога [10] и формирования его групп, ограничимся лишь констатацией того, что:

1. В первую группу каталога включены 19 угроз, возникающих при обстоятельствах непреодолимой силы (форс-мажорных обстоятельствах), например:
    - наводнения,
    - землетрясения, разрушение зданий и сооружений,
    - техногенные катастрофы,

- общественные беспорядки.

2. Ко второй группе каталог относит 147 угроз, обусловленных организационными причинами, например:
   - отсутствие системы организации и контроля пожарной безопасности,
   - недостатки в системе сопровождения технической документации,
   - нарушение в организации обращения с информацией с ограниченным доступом,
   - отсутствие контроля соблюдения установленных регламентов,
3. Третья группа объединяет в себе 98 угроз, являющихся следствием человеческого фактора, например:
   - резкое изменение в состоянии здоровья и самочувствия, в т.ч. чрезмерная усталость;
   - проявление неадекватного поведения;
   - халатное отношение к должностным обязанностям;
   - недостаточный уровень квалификации.
4. Четвертая групп насчитывает 73 угрозы, возникающие в связи с техническими отказами, например:
   - отказ источников электропитания;
   - выход из строя носителей информации;
   - сбой в работе аппаратуры;
   - недокументированные возможности программного обеспечения.
5. В пятой группе каталога приведено 146 угроз, обусловленных умышленными действиями, например:
   - удаленные атаки на компьютерные системы;
   - внедрение вредоносного кода;
   - злоупотребление полномочиями доступа к ресурсам;
   - манипулирование данными.

В целом, для нас важным является то, что на основе каталога [10] мы можем сделать вывод о порядке величины текущего значения μ_k :

$$\mu_k \sim 400.$$

Очевидно, что формирование подмножества актуальных угроз $\mathbf{H}_A$ для каждого информационного актива с присущими ему уязвимостями будет представлять следующую задачу. Пусть для текущего момента времени k задано множество $\mathbf{H}(k)$ известных угроз h_i, где $i = 1, 2, \ldots, \mu_k$, и множество $\mathbf{A}(k)$ известных информационных активов a_j, где $j = 1, 2, \ldots, \nu_k$. Для каждого текущего момента дискретного времени k введем функцию уязвимости $\mathrm{v}_k(i, j)$, значением которой является вероятность поражения угрозой h_i актива a_j в текущий момент дискретного времени, а именно, если вероятность поражения актива a_j угрозой h_i равна $\lambda_{i,j}(k)$, то

$$\mathrm{v}_k(i,j) = \lambda_{i,j}(k).$$

Для задания функции уязвимости $\mathrm{v}_k(i,j)$ может быть использована матрица V_k следующего вида:

$$V_k = \begin{Vmatrix} \lambda_{1,1}(k) & \lambda_{1,2}(k) & \dots & \lambda_{1,j}(k) & \dots & \lambda_{1,\nu_k}(k) \\ \lambda_{2,1}(k) & \lambda_{2,2}(k) & \dots & \lambda_{2,j}(k) & \dots & \lambda_{2,\nu_k}(k) \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \lambda_{i,1}(k) & \lambda_{i,2}(k) & \dots & \lambda_{i,j}(k) & \dots & \lambda_{i,\nu_k}(k) \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \lambda_{\mu_л,1}(k) & \lambda_{\mu_л,2}(k) & \dots & \lambda_{\mu_л,j}(k) & \dots & \lambda_{\mu_л,\nu_k}(k) \end{Vmatrix}.$$

Очевидно, что размерность матрицы V_k равна произведению $(\mu_k \cdot \nu_k)$. Столбцами матрицы являются векторы уязвимостей $\overline{V}_j^{(A)}$ для активов a_j ($j = 1, 2, \dots, \nu_k$), а строками являются векторы опасностей $\overline{V}_i^{(H)}$ для угроз h_i ($i = 1, 2, \dots, \mu_k$). Если все компоненты вектора уязвимостей для некоторого актива a_j равны нулю

$$\overline{V}_j^{(A)} = \left\{ \begin{array}{|c|c|c|c|c|c|} \hline 0 & 0 & \dots & 0 & \dots & 0 \\ \hline \end{array} \right\}^T,$$

то это означает, что данный актив не является уязвимым для любых угроз, известных в момент времени k. Частным случаем является ситуация, когда актив в принципе существует и известен, но в текущий момент дискретного времени k он не является элементом рассматриваемой системы.

Если все компоненты вектора опасностей для некоторой угрозы $h_i(k)$ равны нулю

$$\overline{V}_i^{(H)} = \left\{ \begin{array}{|c|c|c|c|c|c|} \hline 0 & 0 & \dots & 0 & \dots & 0 \\ \hline \end{array} \right\},$$

то такая угроза не может причинить вред ни одному из активов системы. Такую угрозу естественно назвать неактуальной.

Множеству $\mathbf{A}(k)$ известных информационных активов можно поставить в соответствие вектор $\overline{C}_k$ значений оценок ценности соответствующих активов:

$$\overline{C}_k = \left\{ \begin{array}{|c|c|c|c|c|c|} \hline c_1 & c_2 & \dots & c_j & \dots & c_{\nu_k} \\ \hline \end{array} \right\}.$$

Тогда произведение матрицы V_k на вектор $\overline{C}$ будет давать матрицу потерь для всех активов по всем угрозам:

$$L_k = V_k \cdot \overline{C}_k$$

Оценим размерность вектора $\overline{C}_k$, т.е. величину ν_k. Для этого обратимся к стандарту [3, 6], где приводится следующий пример классификации

информационных активов:

1. Основные активы
   1.1. Бизнес-процессы
      1.1.1. Процессы, утрата или ухудшение которых делает невозможным выполнение целевой задачи организации
      1.1.2. Процессы, включающие в себя секретные процессы или процессы, созданные с использованием высокоуровневой технологии
      1.1.3. Процессы, модификация которых может значительно повлиять на выполнение назначения организации
      1.1.4. Процессы, которые необходимы организации для выполнения договорных, правовых или регулирующих требований
   1.2. Информация
      1.2.1. Информация, необходимая для реализации назначения или бизнеса организации
      1.2.2. Информация личного характера, если она может быть определена особым образом, соответствующим национальным законам о неприкосновенности частной жизни
      1.2.3. Стратегическая информация, необходимая для достижения целей, определяемых стратегией деятельности организации
      1.2.4. Информация с высокой себестоимостью, сбор, хранение, обработка и передача которой требуют продолжительного времени и/или связаны с большими затратами на ее приобретение
2. Вспомогательные активы.
   2.1. Аппаратные средства
      2.1.1. Аппаратура обработки данных
      2.1.2. Мобильная аппаратура
      2.1.3. Стационарная аппаратура
      2.1.4. Периферийное обрабатывающее оборудование
      2.1.5. Пассивные носители данных
      2.1.6. Электронные носители данных
      2.1.7. Другие носители данных
   2.2. Программное обеспечение
      2.2.1. Операционные системы
      2.2.2. Программное обеспечение обслуживания, сопровождения и администрирования
      2.2.3. Пакетное программное обеспечение или системное программное обеспечение
      2.2.4. *Би*знес-приложения
         2.2.4.1. Стандартные бизнес приложения
         2.2.4.2. Специфические бизнес-приложения
   2.3. Сети
      2.3.1. Среда и поддержка

2.3.2. Пассивные или активные ретрансляторы
2.3.3. Связной интерфейс
2.4. Персонал
2.4.1. Лицо, принимающее решение
2.4.2. Пользователи
2.4.3. Персонал эксплуатации и сопровождения
2.4.4. Разработчик
2.5. Место функционирования организации
2.5.1. Размещение
2.5.2. Внешняя среда
2.5.3. Владения организации
2.5.4. Зона
2.5.5. Основные сервисы
2.5.6. Связь
2.5.7. *Коммуникации*
2.5.7.1. Сервисы электроснабжения
2.5.7.2. Водоснабжение
2.5.7.3. Удаление отходов
2.5.7.4. Сервисы кондиционирования воздуха
2.6. Организация
2.6.1. Административные органы,
2.6.2. Структура организации,
2.6.3. Организация проекта
2.6.4. Контрагенты

Отметим, что для нас сейчас не важны ни методика классификации информационных активов, ни конкретное наименование групп. Важно лишь количество позиций на нижнем уровне в данном списке (они выделены курсивом). Приведенный список содержит на нижнем уровне 41 наименование. Следовательно, можем принять, что оценкой величины ν_k является значение

$$\nu_k \sim 40.$$

Тогда для произведения $(\mu_k \cdot \nu_k)$ может быть получена оценка

$$(\mu_k \cdot \nu_k) \sim 400 \times 40 = 16000.$$

Это означает, что матрица уязвимости V_k (и матрица потерь L_k), построенная в соответствии с рекомендациями стандарта [3, 6] должна содержать порядка 16 тысяч значений оценок вероятности (потерь). Учитывая, что построение каждой из таких оценок представляет собой интеллектуальный, слабо формализованный процесс, а также наличие в такой постановке проблем с исходными данными, реальность построения 16 тысяч оценок вероятности (потерь) вызывает серьезные сомнения.

Выход из ситуации следует искать в декомпозиции и снижении размерности задачи за счет учета того, как отмечено в вышеприведенных

рекомендациях п.8.2.2.3. стандарта [3], «***сколь активно возникают угрозы и эксплуатируются уязвимости***». В развитие этого тезиса выдвинем положение о целесообразности разделении угроз, воздействующих на конкретный объект, на две категории, а именно: *реальные угроз* и *виртуальные угрозы*. В скобках отметим, что основными толкованиями значения слова «виртуальный» согласно [11] являются *«возможный»*, *«такой, который может или должен проявиться при определенных условиях, но в реальности не существующий»*. В качестве критериев проявления реальности конкретной угрозы, т.е. отнесения ее к категории реальной или виртуальной, будем рассматривать существование и доступность (в явном или в неявном, экспертном виде) статистики, отвечающей трем требованиям:

- объекты, к которым предполагается применять статистику, и объекты, на которых собрана статистика, являются эквивалентными (требование эквивалентности объектов);
- условия, при которых предполагается применять статистику и условия ее сбора являются эквивалентными (требование эквивалентности условий);
- объемы выборок статистики являются достаточными, методы обработки – корректными, а источники сведений – заслуживающие доверия (требование убедительности).

Таким образом, если для угрозы, рассматриваемой применительно к данному объекту, существуют и доступны статистики, отвечающие трем названным требованиям, то такую угрозу будем относить к категории реальных угроз. Соответственно, угрозу, для которой не существует или не доступна статистика, отвечающая названным требованиям, будем относить к категории угроз виртуальных, т.е. «таких, которые могут или должны проявиться при определенных условиях, но в реальности не существуют». Следствием этого положения будет вывод о том, что виртуальные угрозы можно исключить из рассмотрения при оценке рисков безопасности информации.

Выдвинутое положение о разделении угроз на реальные и виртуальные представляется логичным в контексте практики, а именно, изучению угроз, которые представляют *реальную* опасность, как правило, уже уделено достаточно внимания. Как следствие, по ним собраны, существуют и доступны (в явном или в неявном, экспертном виде) соответствующие статистики. Угрозы же, по которым нет таких статистик, могут быть отнесены к категории редких или малозначимых, иными словами таких, в отношении которых высказывание «нечто представляет *реальную* угрозу» не является истинным; но поскольку факт существования таких угроз нельзя игнорировать они попадают в категорию возможных, но *виртуальных* угроз.

Формально, сформулированное положение состоит в том, что рассматриваемый объект осуществляет разбиение множества известных

угроз $\mathbf{H}(k)$ на два непересекающихся подмножества: подмножество известных *реальных* угроз $\mathrm{Re}\,\mathbf{H}(k)$ и подмножество известных *виртуальных* угроз $\mathbf{ViH}(k)$

$$\mathbf{H}(k) = \mathrm{Re}\,\mathbf{H}(k) \cup \mathbf{ViH}(k)$$

$$\mathrm{Re}\,\mathbf{H}(k) \cap \mathbf{ViH}(k) = \varnothing$$

Можно высказать предположение, что в практике кардинальное число множества $\mathrm{Re}\,\mathbf{H}(k)$ должно быть существенно меньше числа элементов множества $\mathbf{H}(k)$. Таким образом, выводя виртуальные угрозы за область рассмотрения при построении оценок рисков, мы, тем самым, уходим от рассмотрения вопросов существования и доверия в отношении соответствующих статистик.

Пусть для рассматриваемого объекта известно множество реальных известных угроз $\mathrm{Re}\,\mathbf{H}(k)$. Означает ли это, что все угрозы этого множества постоянно и одновременно проявляют свою активность в отношении данного объекта? Очевидно, что ответ на этот вопрос отрицателен, ибо каждой из угроз можно поставить в соответствие процесс ее жизненного цикла, протекающий во времени. Угроза может быть реальной для данного информационного актива в смысле выполнения требований эквивалентности и убедительности ее статистик, но не актуальной вследствие отсутствия факторов, способствующих ее зарождению и обуславливающих динамику ее жизненного цикла.

Выдвинем следующую гипотезу: для результативной реализации сценария развития угрозы необходимо совпадение (резонанс) во времени и пространстве активной фазы жизненного цикла угрозы и соответствующей фазы жизненного цикла информационного актива. На основании этой гипотезы путем постановки мысленных экспериментов можно прийти к выводу, что конкретный дискретный элемент величины потерь, возможных в каждый конкретный, малый промежуток времени, является результатом успешной реализации сценария развития только одной угрозы. Угрозу, активная фаза жизненного цикла которой совпадает по времени и пространству с соответствующей фазой жизненного цикла соответствующего актива, будем называть актуальной угрозой. В качестве меры актуальности угрозы следует принять, как отмечалось выше, вероятность поражения данной угрозой соответствующего актива $\lambda_{i,j}(k)$.

Как следствие приходим к выводу о том, что на достаточно малом отрезке дискретного времени

$$\Delta k = (k_1 - k_0)$$

вероятные потери являются следствием небольшого количества реальных угроз, которые являются актуальными на данном отрезке времени. Для описания множества угроз, актуальных на данном отрезке времени Δk

предлагается использовать понятие динамического множества актуальных угроз, близкое к понятиям динамического множества в программирование и теории расписаний. Динамические множества в программировании – это структуры данных, размерность которых изменяется в процессе выполнения алгоритма. Известными примерами таких структур являются, например, списки, стеки, очереди, деки [12] с присущими им дисциплинами добавления или удалении элементов. Динамическое множество в теории расписаний [13] – это множество заявок с известными характеристиками, которые нуждаются в обслуживании в данный момент времени, при этом количество заявок, составляющих динамическое множество и их типы в каждый момент времени являются случайными величинами. (В этом контексте представляет интерес рассмотреть возможность постановки задачи менеджмента информационной безопасности в виде задачи теории расписаний).

Очевидно, что изменяя значение k_1 при фиксированном значении k_0 можно изменять величину Δk, определяющую диапазон изменения кардинального числа динамического множества актуальных угроз. В результате получаем возможность целенаправленно изменять величину анализируемого пространства угроз/активов и, как следствие, обеспечивать возможность решения задачи построения оценок риска безопасности информации в реальных условиях.

1. ISO/IEC Guide 73:2002 “Risk management – Vocabulary – Guidelines for use in standards”
2. ISO/IEC 27001:2005 “Information technology – Security techniques – Information security management systems - Requirements”
3. ISO/IEC 27005:2005 “Information technology – Security techniques – Information Security Risk Management”
4. ГОСТ Р 51897-2002 «Менеджмент риска. Термины и определения». — http://www.complexdoc.ru/text/ГОСТ Р51897-2002
5. ГОСТ Р ИСО/МЭК 27001:2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» . — http://www.complexdoc.ru/ГОСТ Р ИСО|МЭК 27001-2006
6. Проект ГОСТ Р ИСО/МЭК 27005:2008 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент рисков информационной безопасности».— http://docs.cntd.ru/document/1200075254/
7. *Лукацкий А.В.* Семь способов оценки вероятности риска. — http://lukatsky.blogspot.com/ Risk measurement © 2008 Cisco Systems, Inc. All rights reserved.
8. ГОСТ Р 51901.13-2005 «Менеджмент риска. Анализ дерева неисправностей».— http://www.complexdoc.ru/text/ГОСТ Р 51901.13-2005
9. ГОСТ Р 51344-99 «Безопасность машин. Принципы определения и оценки риска».— М., «Госстандарт России», 2004.— 20 с.
10. *IT-Grundschutz-Kataloge*. - https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/download/it-grundschutz-kataloge_2005_pdf_en_zip.zip?__blob=publicationFile
11. Новейший словарь иностранных слов и выражений. – М.: Современный литератор, 2003. – 976 с.

12. *Кнут Д.* Искусство программирования для ЭВМ. Т.1. Основные алгоритмы. – М.: «Мир», 1976. – 735 с.
13. Теория расписаний и вычислительные машины/*Под ред. Э.Г.Кофмана*. – М.: «Наука», 1984. – 334 с.

Поступила 1.09.2010р.

УДК 004.942:691.342

Т.В. Бибик, Т.И. Носенко, Д.А. Пурич, Л.А. Одукалец

ДЕСИНХРОНИЗАЦИЯ ПОСЛЕДСТВИЙ АВАРИЙ НА АТОМНЫХ ЭЛЕКТРОСТАНЦИЯХ

Резюме. Отказы сложных систем часто определяются совпадением во времени (синхронизацией) событий, которые по отдельности не являются катастрофически опасными. Предложен метод поддержки проектных решений в САПР, позволяющий заранее выявлять наборы опасных совпадений событий и на этапе проектирования принимать меры к их недопущению впоследствии.

Многие современные технические системы из различных сфер человеческой деятельности имеют избыточную сетевую структуру либо легко сводятся к таковой, а надежность их функционирования зависит от факторов, моделирование которых невозможно без учета анализа такой структуры и требований, предъявляемых к системе пользователями. Проблема сетевой надежности исследуется достаточно давно, однако и в настоящее время точного решения даже для сетей ограниченного размера эта задача не имеет.

Важным компонентом надежности систем является их живучесть, т.е. способность сложной технической системы выполнять основные функции после ряда повреждений и аварий и быстро восстанавливать эти функции в процессе дальнейшей эксплуатации [1]. Для повышения живучести системы ответственного назначения, как правило, проектируются так, чтобы их основные элементы были зарезервированы на случай отказа. Поиск оптимального резервирования – одна из основных задач САПР таких систем. Особо актуальными являются случаи, когда к таким задачам относится проектирование защиты некоторого объекта от техногенной катастрофы и ее последствий.

Расследование многих техногенных катастроф в промышленности, энергетике, на транспорте и в других сферах человеческой деятельности чаще всего заканчивается выводом о том, что их причиной стал ряд детерминированных или случайных, но обязательно совпавших во времени событий [2 – 4].

