4.4. Экономические аспекты и эффективность СИБ

В условиях зарождения возможного конфликта и противостояния, с одной стороны нарушителя, использующего набор доступных средств для внедрения в АИС, и СИБ - с другой, требуется уточнить понятие риска.

Одним из методов оценки качества защиты информации является определение соответствия техническому заданию на создание системы защиты реализованных функций и задач, эксплуатационных характеристик и требований.

Другой способ, используемый в отечественной и зарубежной практике -это анализ функциональной надежности системы, которая также характеризует качественный уровень СИБ.

Количественный уровень защиты АИС характеризуется двумя основными группами показателей - относительными и абсолютными. Рассмотрим более подробно данные показатели.

Относительная количественная оценка представляет собой число (рейтинг, категорию, нормализованное значение), которое требует сравнения с другими числами, принятыми в качестве эталона. Для их определения используются экспертные оценки.

Наиболее важным моментом качественной оценки является вопрос о коррекции и согласовании погрешностей, которые возникают из-за субъективизма оценок экспертов. Наиболее популярным методом проведения экспертизы является метод Дельфи [85] и его модификации.

Экспертиза может быть направлена на оценку эффективности системы защиты, уровня допустимого риска, уровня защищенности отдельных подсистем и др.

В случае, когда объектом оценки выступает АИС следует разработать комплекс механизмов, позволяющих получить количественные показатели защищенности.

Абсолютная количественная оценка защиты информации в АИС

может характеризовать издержки, выраженные в денежном выражении, частоту неблагоприятных событий или другие показатели, которые являются значимыми в части обеспечения защиты информации.

Абсолютные количественные показатели могут быть систематизированы в следующие разновидности:

1. Технические. В эту группу входят следующие показатели:

* *количество распознаваемых угроз* -определяет количество опознаваемых и обрабатываемых угроз. Угроза считается опознанной, если ее характеристики совпадают с описаниями, находящимися в СИБ;

* *качество противостояния угрозам* - определяется способностью СИБ адекватно реагировать на опознанную угрозу. В реальной жизни возникают угрозы, на которые АИС достаточно трудно реагировать. В такой ситуации желательно протоколировать те действия, которые осуществляются угрозой;

* *уменьшение производительности АИС в целом* - отражает уменьшение производительности АИС вследствии необходимости реализации действий предписанных политикой безопасности. Примерами могут служить платы шифрования, которые уменьшают скорость передачи данных из-за необходимости шифровать при передаче и дешифровать при приеме данных, неудобства пользователей из-за необходимости использования паролей и т.д.

2. Организационные. Этот вид показателей характеризует:

* количество дополнительно привлеченного персонала для обслуживания СИБ. При реализации функций безопасности привлекается дополнительный персонал - инженеры, программисты, администраторы систем, менеджеры АИС по безопасности.

3. Экономические. К данной разновидности относятся следующие показатели:

* *стоимость создания, внедрения, эксплуатации и обучения пользователей и поддержки СИБ.* В ней включаются все затраты,

произведенные на всех этапах жизненного цикла СИБ, в том числе и затраты на исследования, приобретение технологий ноу-хау, специальной аппаратуры, и программного обеспечения и др. Сюда также входит заработная плата работников, выполняющих специфические для СИБ работы;

* *затраты специфических материалов.* Предусматривает использование специальных расходных материалов в работе СИБ. В качестве примера можно рассматривать дополнительные магнитные носители, необходимые для реализации резервного копирования;

* *затраты на восстановление нормальной работы после реализации угрозы.* В них включаются затраты информационных, технических, трудовых и других ресурсов на восстановление нормальной работы АИС;

* *коэффициент уменьшения потенциальных потерь.* Характеризует отношение между показателем уменьшения потерь и величины возможных потерь. Величина возможных потерь - это потери, которые могут быть в случае когда СИБ не используется. Показатель уменьшения потерь - это величина на которую уменьшаются потери вследствии использования СИБ:

$$K^{u} = \frac{L - L''}{L} = \frac{L©}{L}, \qquad (4.78)$$

где L - потенциальные потери;

L'' - величина реальных потерь;

L' - величина уменьшения потерь.

В то же время следует отметить, что при оценке проектов в области информационного бизнеса в общем и систем информационной безопасности АИС, в частности, невозможно однозначно определить стоимость того или иного ресурса или актива АИС, который может быть потерян вследствии реализации той или иной угрозы. Поэтому используются верятностные модели, позволяющие расчитывать экономические показатели.

* *эффективность СИБ.* Отражает эффективность вложения средств в

обеспечение безопасности АИС. Данный показатель определяется величиной уменьшения потенциальных потерь, коэффициентом окупаемости и др. показателями, которые будут рассматриваться далее.

При постановке вопроса о том, надо ли защищать АИС, кроме ответов на вопросы что защищать, от кого защищать, как защищать, необходимо ответить также и на следующие вопросы: сколько нужно потратить, какова эффективность затраченных средств. Следует отметить, что, если на первую часть вопросов можно найти ответы в опубликованных научных работах, то единых подходов по поводу второй части вопросов не существует.

Рассматривая потери АИС, необходимо отметить, что они могут быть техническими, организационными, технологическими, экономическими, причем они вытекают друг из друга и потери одного уровня влекут за собой потери следующих уровней.

Потери АИС *- это потеря свойств информации, вычислительных, информационных ресурсов АИС, финансовых и прочих активов, а также потеря доверия между партнерами вследствии реализации угроз.*

При разработке СИБ разработчик должен оценивать потери, которые понесет АИС в результате реализации той или иной угрозы. Исходя из таких оценок, он должен ответить на поставленные выше вопросы.

В то же время, при разработке эффективной СИБ, должна учитываться величина выигрыша нарушителя, и сделать так, чтобы данная величина минимизировалась.

При исследовании возможных потерь АИС вследствии реализации угроз, требуется изучать множество ресурсов АИС и потенциальных угроз и по отношению к каждому ресурсу найти решения, связанные со следующими обстоятельствами:

- определение круга заинтересованных лиц в использовании активов АИС.

- определение целей нарушителя.

- усиановление размеров выгоды полученной нарушителем вследствии реализации одной или комплекса угроз.

- оценка размеров затрат, которые нарушитель готов понести для достижения поставленной цели.

По нашему мнению, при оценке эффективности СИБ необходимо рассматривать свойства информации и ресурсы АИС, которые подлежат защите с точки зрения собственика информации, так как только собственник может определить что нужно защищать и дать стоимостную оценку тому или иному свойству и/или ресурсу.

Расчет абсолютных количественных показателей неразрывно связан с понятиями риска и затрат на уменьшение риска.

В повседневной жизни риск определяется как действие наугад в надежде на счастливую случайность. Данный подход в отношении защиты информации неприемлем. Если опасность строго и четко формализована, то риска нет, поскольку последствия будущего конфликта предсказуемы и, следовательно, устранимы. Когда оценка опасности выполняется приближенно с использованием вероятностных величин (например, вероятность получения несанкционированного доступа, вероятность реализации логического механизма компьютерного вируса и др.), необходимо использование термина “риск” по отношению к действиям нарушителя и последствиям.

Наиболее полное определение риска представлено в [64]. Авторы связывают данное понятие с формальными характеристиками конфликта, лишенным эмоциональной окраски и имеющим количественное значение. Они определяют, что “риск есть способ действия в условиях неопределенности и слабо предсказуемости событий” [64,с.150]. Данное определение

полностью согласуется с природой конфликтов, возникающих в АИС, а также необходимостью учета множества факторов, оказывающих воздействие на функционирование СИБ.

Представляет интерес предложения по определению видов риска в соответствии с используемыми подходами. В частности, стохастическому подходу соответствует вероятностный риск, основанный на заданных вероятностях исхода. Ситуационному подходу соответствует ситуационный риск, характеризующий возможные отклонения реальной ситуации от ее оценки. В свою очередь, оперативному подходу соответствует оперативный риск, определяющий способность к предвидению событий, ограничению последствий и возможности соотнести действия и реакции взаимодействия.

Для полной характеристики риска целесообразно использовать положения, изложенные в монографии [13]. В ней которой излагаются подходы к определению риска в хозяйственной деятельности и количественное определение риска. Согласно данного источника “Риск может иметь место только там, где имеется возможность выбора: при отсутствии реальных альтернатив может быть принято только одно решение” [13, с.21].

В качестве отправной точки в данной работе выделяются два вида риска:

- глобальный (долгосрочный);
- локальный (краткосрочный);

Из [13] можно делать вывод, что долгосрочный риск связан с принятием решений на уровне АИС, а краткосрочный является главным образом особенностью риска локального, то есть риска на уровне используемых методов и средств защиты.

Однако такой вывод неприемлем, из-за того, что события, определенные как локальные, могут привести к последствиям

глобального характера. Прежде всего это относится к тактическим и стратегическим программным злоупотреблениям и возможностям полиморфизма.

Авторы [13] выделяют три большие группы рисков:

- риски хозяйственные;
- субъективные риски, связанные с природой человека;
- естественные риски, связанные с природными факторами.

Приведенная классификация показывает, что риск является неотъемлемой частью всех решений, от самых простых до самых сложных. Из приведенных групп рисков наиболее присущим для нас являются риски, связанные с деятельностью человека (проектировщика, программиста, пользователя, а также злоумышленника), которые могут быть разделены также на временные и объектные. Например, временной риск может проявиться в том, что при разработке концепции СИБ не учитываются новые виды угроз. Объектные риски проявляется в том, что СИБ не покрывает все компоненты АИС (ресурсы БД, отдельные программные приложения и т.д.)

Помимо других признаков классификации все угрозы АИС можно систематизировать в несколько других классов, а именно, по частоте появления. За основу данного подхода примем метод, предложенный в [38], который может быть использован в условиях, когда отсутствуют статистические данные о появлении угроз. Предлагаем расширить предложенный метод для ситуации, когда существует определенная статистика в этой области.

Известно, что некоторые программные злоупотребления имеют относительно четкий “календарь” срабатывания. В приложении 2 представлен каледарь срабатываний компьютерных вирусов. На основе такого “календаря” можно построить таблицу

срабатываний (таб. 4).

Таблица 4

Вероятные срабатывания известных компьютерных вирусов

	Частота появления угрозы	Весовой коэфф.
1	Один или более разов в день	0,6244
2	Раз в три дня	0,2081
3	Раз в неделю	0,0891
4	Раз в две недели	0,0446
5	Раз в месяц	0,0208
6	Раз в 3 месяца	0,0069
7	Раз в полугодие	0,0034
8	Раз в год	0,0017
9	Раз в три года	0,0006
10	Раз в 5 лет	0,0003

Представлется целесообразным составлять подобные таблицы для всех потенциальных угроз АИС и получать абсолютную вероятность возникновения угрозы.

Для описания экономической эффективности разработки, внедрения и эксплуатации СИБ, введем следующие обозначения:

Пусть существует некоторый актив АИС ***A***, который характеризуется множеством свойств D^A. Тогда:

$$D^A = \{d_k^A \mid k = \overline{1,n}\}$$

$$D^A = D_1^A \bigcup D_2^A,$$

где D_1^A - подмножество свойств ресурса А, которые не нуждаются в

защите;

D_2^A - подмножество свойств ресурса А, которые подлежат защите;

P_i^u -вероятность появления ***i***-й угрозы (в соответствии с таблицей) в рассматриваемом интервале времени ***t***, где *i=1,...,n.*

S_{iA_j} - стоимостной эквивалент потери свойства ***j*** ресурсом ***A*** вследствии воздействия угрозы ***i*** (воздействие угроз, потеря одного и того же свойства у одного и того же объекта может быть по разному, например: полная, частичная и т.д.). В дальнейших иследованиях, различные степени потери одного и того же свойства (ресурса) АИС будем рассматривать как разные;

$$S_{iA} = \sum_j S_{iA_j}, \tag{4.79}$$

где S_{iA} -потенциальные потери актива ***A*** АИС вследствии воздействия угрозы ***i***;

$$S_i = \sum_A S_{iA} = \sum_A \sum_j S_{iA_j}, \tag{4.80}$$

где S_i - потенциальные потери АИС вследствии реализации ***i***-й угрозы.

Тогда стоимостной эквивалент вероятных потенциальных потерь АИС вследствии реализации потенциальных угроз (***S***) равен:

$$S = \sum_i \sum_A S_{iA} = \sum_i S_i \tag{4.81}$$

Иначе

$$S = \sum_i \sum_A \sum_j S_{iA_j} \tag{4.82}$$

С учетом вероятности появления ***i***-й угрозы данное выражение можно записать следующим образом:

$$S© = \sum_i P_i^u * (\sum_A \sum_j S_{iA_j})) \tag{4.83}$$

Z - совокупность средств, методов и механизмов защиты АИС, которая определяется как: $Z = \{z_k \mid k = \overline{1, K}\}$;

P_{zi} - вероятность распознавания и противостояния ***z***-м механизмом защиты АИС угрозы ***i***;

$$S'' = \sum_z \sum_i (1 - P_{zi}) * (P_i^u * (\sum_A \sum_j S_{iA_j})), \quad (4.84)$$

где S'' - стоимостной эквивалент вероятных потерь АИС вследствии реализации всех потенциальных угроз при условии использования множества средств, методов и механизмов защиты ***Z***.

$$N^u = \frac{S© - S''}{S©} = \frac{\left(\sum_i (P_i^u * (\sum_A \sum_j S_{iA_j}))\right) - \left(\sum_z \sum_i (1 - P_{zi}) * (P_i^u * (\sum_A \sum_j S_{iA_j}))\right)}{\sum_i (P_i^u * (\sum_A \sum_j S_{iA_j}))} \quad (4.85)$$

N^u - общий показатель уменьшения потерь при использовании СИБ и эффективного противостояния СИБ угрозам;

Величина вероятных затрат (C^v) на восстановление АИС:

$$C^v = \sum_z \sum_i (1 - P_{zi}) * (P_i^u * (\sum_A \sum_j C_{A_j}^v)), \quad (4.86)$$

где $C_{A_j}^v$ - затраты, необходимые для восстановления первоначального ***j***-го свойства состояния нормальной работы АИС в течении планируемого жизненного цикла (***T***).

Показатель “эффективность-стоимость” инвестиций в СИБ АИС (***R***) тогда можно записать следующим образом:

$$R = \frac{S - S''}{C_0 + C_1 + C^v + S''} = \frac{\left(\sum_i P_i^u * (\sum_A \sum_j S_{iA_j})\right) - \left(\sum_z ((1 - P_{zi}) * \sum_i (P_i^u * (\sum_A \sum_j S_{iA_j})))\right)}{C_0 + C_1 + C^v + \left(\sum_z ((1 - P_{zi}) * \sum_i (P_i^u * (\sum_A \sum_j S_{iA_j})))\right)}$$

(4.87)

Предложенный метод является статичным. Актуализацию величин риска и затрат на создание, внедрение и эксплатацию СИБ можно провести с использованием известными методами актуализации из теории экономического анализа [143].

Рассмотрим взаимосвязь между величиной риска и затратами на обеспечение информационной безопасности.

На рис. 32 представлена зависимость между затратами на обеспечение информационной безопасности и величиной риска АИС.

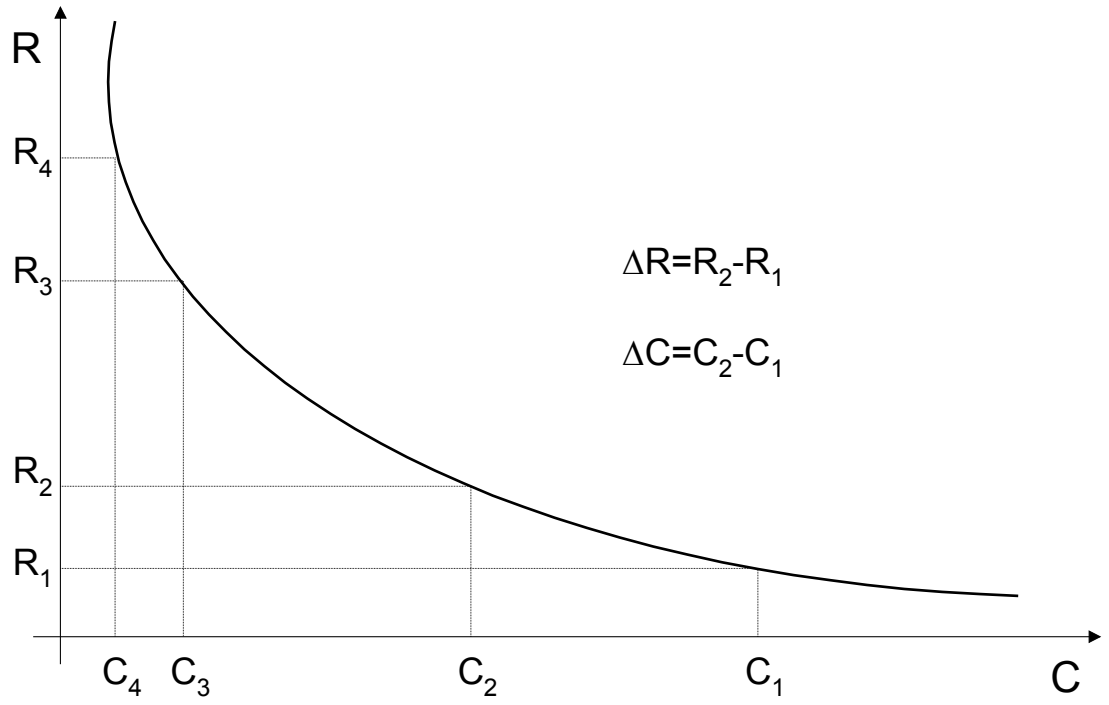

Рис. 32 Характер зависимости затраты-риск в СИБ.

Для количественного анализа зависимости между затратами на обеспечение информационной безопасности и риска используем понятие эластичности.

Эластичность риска по затратам на обеспечение безопасности данных измеряет чувствительность риска к изменению величины затрат на обеспечение безопасности информации (насколько изменятся уровень риска при изменении затрат на обеспечение информационной

безопасности на 1%). Она определяется как отношение процентного изменения величины риска к процентному изменению затрат.

ΔC - изменение затрат на обеспечение безопасности информации;

ΔR - изменение риска при изменении затрат на обеспечение безопасности информации.

$$E_R(C) = \frac{\%\Delta C}{\%\Delta R} = \frac{\Delta C / C}{\Delta R / R} = \frac{\Delta C}{\Delta R} * \frac{R}{C} \qquad (4.88)$$

где $E_R(C)$ - эластичность риска по затратам;

$\%\Delta C$ - процентное изменение затрат на обеспечение безопасности данных;

$\%\Delta R$ - процентное изменение риска при изменение затрат;

Эластичность риска по затратам может быть больше или равна нулю. Когда она равна нулю, то можно утверждать, что даже незначительные затраты на обеспечение безопасности информации приведут к значительному уменьшению риска.

В соответствии с общей теорией экономики [143] оптимальным уровнем риска для коммерческих АИС можно считать тогда, когда эластичность функции риск-затраты равна 1.