УДК 621.34

АНАЛИЗ РИСКОВ ПРИ ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

к.т.н. А.В. Северинов, В.Н. Ткаченко, Ю.А. Избенко
(представил д.т.н., проф. Ю.В. Стасев)

В статье рассматривается один из алгоритмов оценки и определения приемлемости уровня риска при обеспечении информационной безопасности.

В настоящее время для многих организаций очевидна проблема информационной безопасности (ИБ). Под информационной безопасностью понимается защита информации от случайных или преднамеренных воздействий со стороны физических лиц или окружающей среды [1]. Она включает решение таких задач, как сохранение в тайне смыслового содержания информации, ее целостность, доступность, наблюдаемость. Эти задачи должны решаться одновременно с построением автоматизированной системы обработки информации (АСОИ), что позволит реализовать комплексный подход к обеспечению защиты информации. При этом необходимо определить: политику безопасности для защищаемой АСОИ; границы действия ИБ и цели ее создания; решить задачу анализа рисков; провести конечную проверку ИБ.

Одной из самых сложных и трудоемких задач является задача анализа рисков, которая предусматривает изучение модели угроз и модели нарушителей, возможных последствий от реализации потенциальных угроз, и формирование на его основе модели защиты информации в АСОИ.

Риск как общее понятие - мера неопределенности и конфликтности в человеческой деятельности, характеризующаяся возможными опасностью, неудачей, убытком, а как частное понятие - степень успешного (неудачного) достижения защищенности информации в АСОИ. Риски классифицируются по следующим признакам: **по масштабам и размерам**: риск глобальный, локальный; **по аспектам**: риск психологический, социальный, юридический, экономический, политический; **по степени объективности и субъективности**: риск с объективной вероятностью, с субъективной вероятностью; **по степени рисконасыщенности решений**: минимальный, средний, оптимальный, максимальный; **по типам риска**: рациональный (обоснованный), нерациональный (не обоснованный), авантюрный (азартный); **по времени принятия рискованных решений**: риск опережающий, своевременный, запаздывающий; **по численности лиц, принимающих решение**: риск индивидуальный, групповой; **по ситуации**: риск в условиях определенности, в условиях неопределенности, в условиях конфликтности.

При анализе рисков необходимо дать обоснованные количественные и

качественные оценки угроз безопасности, уязвимости, ценности информационных ресурсов. На основе полученных оценок осуществляется определение остаточного риска, который или принимается, или нет. В последнем случае принимаются необходимые контрмеры для снижения уровня риска.

На основе вышеизложенного определим цели анализа рисков: осуществление оценки угроз безопасности, уязвимости, ценности ресурсов; определение остаточного уровня риска; нахождение эффективных контрмер (способных понизить уровень риска с критического до низкого); обеспечение своевременного и точного выполнения поставленных задач на снижение уровня риска. На данный момент проблема решения задачи управления рисками возлагается на администратора АСОИ. Стандартных методов для ее решения нет. Необходимо исходить из описания общего подхода и существующих программных продуктов. При разработке алгоритма анализа рисков необходимо учитывать, что в результате его выполнения должны вырабатываться рекомендации по обеспечению ИБ, а оценка риска осуществляться в реальном масштабе времени с достаточно большой точностью. На рис. 1 предлагается алгоритм решения задачи анализа рисков.

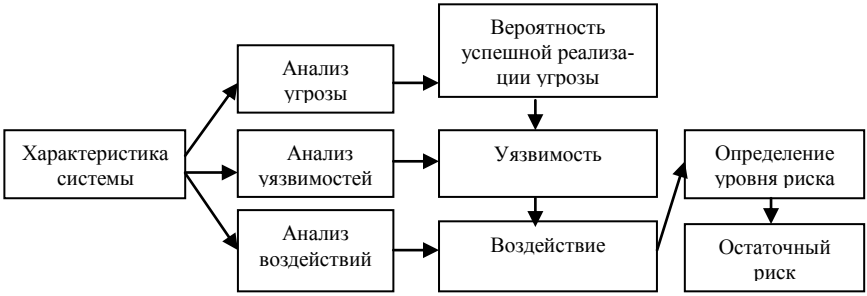

Рис.1. Алгоритм решения задачи анализа рисков

Рассмотрим каждый этап в отдельности.

1. Характеристика системы. На этом этапе проводится сбор информации, необходимой для полного описания защищаемой АСОИ. Администратор должен обладать информацией о границах охраняемой системы и интерфейсов; критичности системы и используемых данных; требуемых задачах безопасности; задачах, выполняемых системой; среде эксплуатации системы; задействованных аппаратных средствах для решения заданных задач. Вся собранная информация используется на следующих этапах.

2. Анализ угрозы. Угроза - это способность источника угрозы использовать одну из уязвимостей системы [2]. В свою очередь, уязвимость - это слабость в защищаемой системе, которая дает возможность угрозам воздействовать на задачи безопасности [2]. Если уязвимость отсутствует, то угроза никакого риска не представляет, соответственно защитных мер принимать не следует. Следуя из вышесказанного, становится очевидным, что анализ угрозы состоит из двух этапов: идентификация источника угрозы; принятие ре-

шения о необходимости защиты. При решении данной задачи рекомендуется использовать стандарт BSI (*www.bsi.bund.de/gshb/english/etc/econten.htm*) [3]. Он содержит каталоги угроз безопасности и контрмер (около 600 наименований в каждом каталоге). Каталоги структурированы следующим образом.

Угрозы по классам: форсмажорные обстоятельства; недостатки организационных мер; ошибки человека; технические неисправности; преднамеренные действия.

Контрмеры по классам: улучшение инфраструктуры; административные контрмеры; процедурные контрмеры; программно-технические контрмеры; уменьшение уязвимости коммуникаций; планирование действий в чрезвычайных ситуациях. Однако, необходимо обоснованно подходить к выбору угроз. К примеру, для АСОИ, которая эксплуатируется в пустыне, не может существовать угроза наводнения.

3. Анализ уязвимостей. На этом шаге необходимо выявить все существующие дефекты и слабости защищаемой АСОИ. Эта задача должна выполняться систематически. Администратор должен быть уверенным в том, что все уязвимости ресурсов идентифицированы, а новые уязвимости не останутся незамеченными.

4. Анализ воздействий. На этапе анализа воздействий определяется уровень наносимого ущерба от воздействия угрозы на задачи безопасности (сохранение в тайне смыслового содержания информации, целостность, доступность, наблюдаемость, гарантий).

Некоторые воздействия оцениваются количественно в потерянном доходе, в затратах на восстановление и т.д. Другие воздействия, как показано в табл. 1, оцениваются качественно и разбиваются на уровни: критический, высокий, умеренный и низкий.

Таблица 1

Качественный подход оценки влияния воздействий на уязвимости

Уязвимости	Воздействие			
	критическое	высокое	умеренное	низкое
высокая	критическое	критическое	высокое	умеренное
средняя	высокое	высокое	умеренное	умеренное
низкая	умеренное	умеренное	низкое	низкое

Преимущество количественного анализа состоит в предоставлении конкретных числовых значений, которые помогают точно оценить нанесенный ущерб от воздействия угроз. Недостатком его является высокая сложность расчёта и зависимостью результата от большого числа различных факторов, учесть которые каким-либо одним показателем не представляется возможным.

Качественный анализ определяет вид риска, разбивает все угрозы по степени наносимого ущерба. Его результаты описываются лингвистическим способом, например «риск отсутствует» или «риск критический».

5. Определение уровня риска. Целью данного шага является определение приемлемости или неприемлемости уровня риска. Для наглядности решения данной задачи рассмотрим следующий алгоритм – рис. 2.

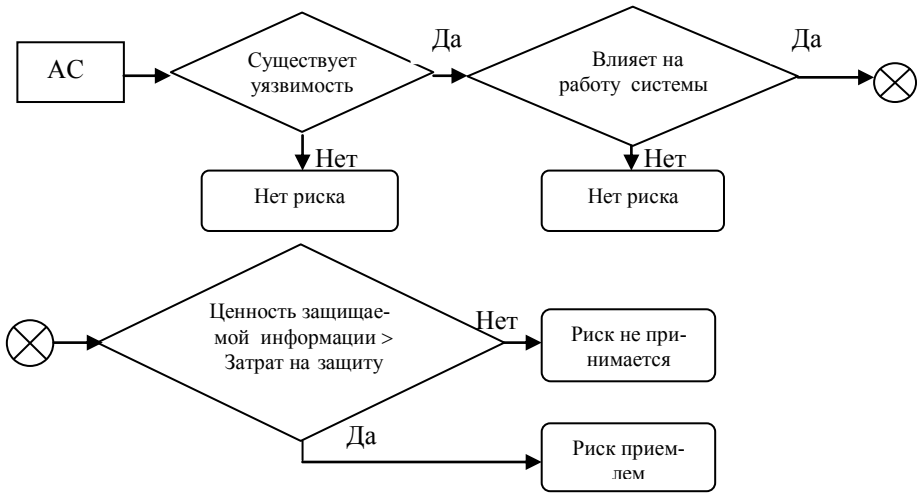

Рис.2. Алгоритм определения приемлемости уровня риска

Если уровень риска неприемлем, то принимаются необходимые контрмеры для снижения уровня риска. Отличительной особенностью предложенного алгоритма решения задачи управления рисками является дополнительный этап "анализа воздействий". Он позволяет:

- повысить информативность данных о степени возможного ущерба от реализации угрозы;
- обосновать необходимость усиления защиты конкретного звена АС;
- оценить уровень риска после принятия контрмер.

Важность решения этих задач обусловлена зависимостью правильности принятия решений от точности оценки наносимого ущерба.

ЛИТЕРАТУРА

1. Домарев В.В. Защита информации и безопасность компьютерных систем. – К. : DiaSoft, 1999. – 450 с.

2. Лукацкий А.В. Обнаружение атак. – СПб.: БХБ - Петербург, 2001. – 624 с .

3. Симонов С. Анализ рисков, управление рисками // Информационный бюллетень : Jet Info. – 2000. – № 4. – С.6 - 23.

Поступила в редколлегию 05.09.2001