УДК 681.3.06

А.А. ЗАМУЛА, канд. техн. наук

МЕТОДОЛОГИЯ АНАЛИЗА РИСКОВ И УПРАВЛЕНИЯ РИСКАМИ

В постоянно расширяющейся области использования средств вычислительной техники и передачи данных появляются новые проблемы, связанные с сохранением конфиденциальности, целостности, доступности информации, а также наблюдаемости за действиями пользователей.

К настоящему времени сложилась общепринятая точка зрения на концептуальные основы обеспечения информационной безопасности (ИБ). Суть ее заключается в том, что подход к обеспечению ИБ должен быть комплексным, сочетающим меры следующих уровней: законодательного, административного, программно-технического.

Тем не менее, можно констатировать, что, несмотря на усилия многочисленных организаций, занимающихся решением проблем обеспечения информационной безопасности, тенденция остается негативной.

Модель процесса информационной безопасности может быть представлена так, как показано на рис. 1. В соответствии с данной моделью [1] обработка информации на объекте осуществляется в условиях воздействия на информацию угроз (совокупность дестабилизирующих факторов). Для противодействия угрозам информации могут использоваться специальные средства защиты, оказывающие нейтрализующее воздействие на дестабилизирующие факторы.

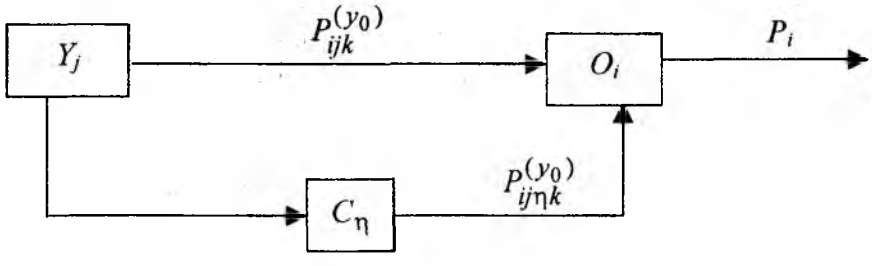

Рис. 1

С учетом обозначений, приведенных на рис. 1, можно вывести такую зависимость:

$$P_i = 1 - \prod_{\forall K} (1 - P_{ik}) a_k \,, \tag{1}$$

где a_k – доля k-го состояния (режима работы) компьютерной системы в анализируемый период времени.

Естественным будет предположить, что система защиты информации может быть неполной, т.е. в ней могут отсутствовать средства предупреждения воздействия некоторых угроз. Тогда:

$$P_{ik} = P'_{ik} \cdot P''_{ik} \,, \tag{2}$$

где P'_{ik} - вероятность защищенности информации на i-м объекте в k-м его состоянии от совокупного воздействия вех тех дестабилизирующих факторов, для противодействия которым в системе защиты не предусмотрены средства защиты; P''_{ik} - то же для тех факторов, для противодействия которым в системе защиты имеются средства защиты.

В свою очередь:

$$P'_{ik} = \prod_{\forall j'} \left(1 - P_{ijk}^{(y_0)}\right), \tag{3}$$

где j – принимает значения номеров угроз, против которых отсутствуют средства защиты, а

$$P''_{ik} = \prod_{\forall \eta} \prod_{\forall j''} \left(1 - P_{ijn\eta}^{(y_0)}\right), \tag{4}$$

где j'' принимает значения номеров дестабилизирующих факторов для противодействия которым в системе защиты предусмотрены средства; η'' - значения номеров тех номеров средств защиты информации, которые оказывают воздействие на угрозу с номером j''.

Вероятность надежного обеспечения безопасности информации в группе объектов определяется зависимостью

$$P = \prod_{\forall i} P_i \,. \tag{5}$$

Применительно к рассмотренной выше модели на объект защиты в любом его состоянии имеется потенциальная опасность воздействия некоторой совокупности дестабилизирующих факторов (угроз). Указанное в свою очередь означает, что функционирование объектов сопряжено с рисками как функции вероятности реализации определенной угрозы.

Управление рисками включает в себя два вида деятельности:

- оценку (измерение) рисков;
- выбор эффективных и экономичных защитных регуляторов (контрмер).

Процесс управления рисками можно подразделить на следующие этапы:

1. Определение границ компьютерной системы, в которых предполагается поддерживать режим ИБ.
2. Выбор методологии оценки рисков.
3. Оценивание угроз и оценивание уязвимости в защите компьютерной системы (КС).
4. Оценивание рисков.
5. Выбор контрмер.
6. Аудит системы управления ИБ.

На первом этапе определяется структура организации и степень детализации ее рассмотрения. Для небольшой организации допустимо рассматривать всю информационную инфраструктуру, однако, если организация крупная, всеобъемлющая оценка может потребовать неприемлемых затрат времени и сил. В таком случае следует сосредоточиться на наиболее важных сервисах, заранее соглашаясь с приближенностью итоговой оценки. Если важных сервисов все еще много, выбираются те из них, риски для которых заведомо велики или неизвестны.

Кроме того, на данном этапе осуществляется классификация и описание ресурсов КС (вычислительных систем, способов связи и коммуникаций, информации, ее категорий, вида представления, мест сохранения, технологии обработки и пр.), разработка информационной модели КС (описание информационных потоков КС, интерфейсов между пользователем и КС и т.д.). Все это важно для оценки последствий нарушений ИБ.

Рекомендуется рассмотреть следующие классы ресурсов: средства вычислительной техники, данные, системное и прикладное программное обеспечение. При этом необходимо учитывать ценность ресурсов КС, выраженную, например, в стоимостных показателях (характеристиках).

Известны табличные методы, учитывающие стоимостные характеристики ресурсов [2]. В методах данного типа показатели физических ресурсов оцениваются с точки зрения стоимости их замены или восстановления работоспособности. Существующие или предполагае-

мые программные ресурсы оцениваются тем же способом, что и физические, на основе определения затрат на их приобретение или восстановление.

Количественные показатели информационных ресурсов оцениваются на основе опросов экспертов. При этом учитывается ценность информации для ее владельца, степень критичности информации и другие ее характеристики. На основе результатов опроса производится оценивание показателей и степени критичности информационных ресурсов для наихудшего варианта развития событий. Рассматривается потенциальное воздействие на КС при возможном нарушении конфиденциальности, целостности, доступности информации. Процесс получения количественных показателей дополняется методиками оценивания информационных ресурсов с учетом факторов: безопасность персонала, требования по соблюдению законодательных и нормативных положений; коммерческие и экономические отношения; финансовые потери и нарушения в производственной деятельности; потеря репутации организации и т.д. Система показателей может быть представлена в виде бальной шкалы (например, восьмибальная). Выбор использования количественных показателей определяется удобством или целесообразностью (в ряде случаев количественные оценки затруднены).

Таким образом, на данном этапе оценки рисков должна быть выбрана система критериев и методология получения оценок по этим критериям.

Выбор методологии оценки рисков (второй этап процесса управления рисками) заключается в постановке задачи оценки рисков и обоснования требований к методике оценки рисков.

Выбор подхода к оценке рисков зависит от ряда факторов: требований к режиму ИБ, спектра воздействия угроз, принимаемых во внимание, эффективности контрмер. В случаях, когда в КС требования в области ИБ не являются жесткими, правила обеспечения режима ИБ обычно основываются на концепции базового уровня ИБ. Существует ряд стандартов, в которых рассматривается минимальный (типовой) набор наиболее вероятных угроз. Для нейтрализации этих угроз должны быть приняты контрмеры. Эти меры носят комплексный характер, т.е. охватывают административный, процедурный, программно-технический уровни и все этапы жизненного цикла информационной технологии. Однако такой подход не учитывает многие факторы, которые могут оказать существенное влияние на реализацию ПБ компьютерной системы. Так, не учитываются вероятности осуществления угроз, уязвимости ресурсов. Кроме того, при таком подходе можно упустить из вида специфические для конкретной информационной системы классы угроз.

При наличии повышенных требований к ИБ должен быть проведен так называемый полный вариант оценки рисков, в рамках которого, в дополнение к базовым, рассматриваются следующие аспекты:

- определение ценности ресурсов;
- расширение набора угроз, определенного на базовом информационном уровне ИБ, перечнем угроз, актуальных для исследуемой информационной технологии;
- оценка вероятности угроз;
- определение уязвимости ресурсов.

Методологические вопросы определения ценности ресурсов рассмотрены ранее. Что касается угроз, то необходимо отметить, что первый шаг в анализе угроз – их идентификация. В пределах выбранных видов угроз следует провести их максимально полное рассмотрение. Для этих целей можно использовать существующие инструментальные средства оценки и управления рисками, например, Германский стандарт BSI [3]. Документ включает в себя следующие блоки:

- Методология управления ИБ (организация менеджмента в области ИБ, методология использования Руководства).
- Компоненты информационных технологий:

- Основные компоненты (организационный уровень ИБ, процедурный уровень, организация защиты данных, планирование действий в чрезвычайных ситуациях).
- Инфрастуктура (здания, помещения, кабельные сети, организация удаленного доступа).
- Клиентские компоненты различных типов (DOS, Windows, UNIX, мобильные компоненты, прочие типы).
- Сети различных типов (соединения «точка-точка», сети Novell NetWare, сети с ОС UNIX и Windows, разнородные сети).
- Элементы систем передачи данных (электронная почта, модемы, межсетевые экраны и т.д.).
- Телекоммуникации (факсы, автоответчики, интегрированные системы на базе ISDN, прочие телекоммуникационные системы).
- Стандартное ПО.
- Базы данных.

• 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.

Все компоненты рассматриваются по следующему плану: общее описание, возможные сценарии угроз безопасности (перечисляются применимые к данной компоненте угрозы из каталога угроз безопасности), возможные контрмеры (перечисляются возможные контрмеры из каталога контрмер). Фактически, в данном стандарте сделана попытка описать, с точки зрения ИБ, наиболее распространенные компоненты информационных технологий и максимально учесть их специфику.

Целесообразно выявить не только сами угрозы, но и источники их возникновения – это поможет в выборе дополнительных средств защиты. После идентификации угрозы необходимо оценить уровни угроз (вероятность их реализации) и уровни уязвимости (легкости, с которой реализованная угроза способна привести к негативному воздействию). Оценивание, как правило, производится в качественных шкалах. Например, уровень угроз можно оценить по шкале «высокий – низкий». Уровни уязвимости оцениваются таким же образом. Информацию о потенциальных и наиболее вероятных угрозах, уязвимостях информационной технологии, о размерах возможного ущерба от реализации угроз можно получить путем опроса сотрудников.

Собственно уровни рисков, соответствующих показателям (ценности) ресурсов, показателям угроз и уязвимости, относящихся к каждому типу негативных воздействий, сравниваются при помощи матрицы, аналогичной приведенной в табл. 1.

Таблица 1

Показатель (ценность) ресурса	Уровень угроз								
	Низкий			Средний			Высокий		
	Уровни уязвимости			Уровни уязвимости			Уровни уязвимости		
	Н	С	В	Н	С	В	Н	С	В
0	0	1	2	1	2	3	2	3	4
1	1	2	3	2	3	4	3	4	5
2	2	3	4	3	4	5	4	5	6
3	3	4	5	4	5	6	5	6	7
4	4	5	6	5	6	7	6	7	8

Количественный показатель риска определяется (для данного примера) по шкале от 1 до 8.

Для каждого ресурса рассматриваются относящиеся к нему уязвимые места и соответствующие им угрозы. Если существует уязвимость и нет связанной с ней угрозы или существует угроза, не связанная с какими-либо уязвимыми местами, то в такой ситуации рисков нет. Каждая строка в матрице определяется показателем ресурса, а каждый столбец – степенью опасности угрозы и уязвимости.

Один из этапов процесса оценки и управления рисками сводится к поиску адекватных контрмер, снижающих риски до допустимых уровней и обладающих наибольшей ценовой эффективностью.

Обеспечение повышенных требований к ИБ предполагает соответствующие мероприятия на всех этапах жизненного цикла информационных технологий. Планирование этих мероприятий производится по завершении этапа анализа рисков и выбора контрмер. Обязательной составной частью этих планов является периодическая проверка соответствия существующего режима ИБ политике безопасности, сертификация информационной системы (технологии) на соответствие требованиям определенного стандарта безопасности.

Целью проведения аудита (завершающий этап работ по обеспечению режима ИБ) является проверка соответствия выбранных контрмер декларированным в политике безопасности целям. Вопросы аудита и процедура сертификации информационной технологии на соответствие требованиям ИБ рассматриваются в [4]. В результате выполнения данного этапа должен быть документ «Ведомость соответствия», в котором содержится анализ эффективности контрмер.

Основные разделы этого документа:

- границы проводимого аудита;
- методика оценки;
- соответствие существующего режима ИБ требованиям организации и используемым стандартам;
- несоответствия и их категории;
- общие замечания, выводы рекомендации.

Таким образом, анализ рисков включает в себя идентификацию и вычисление уровней рисков на основе оценок, присвоенных ресурсам, угрозам и уязвимости ресурсов. Контроль рисков состоит в идентификации и выборе контрмер, позволяющих снизить риски до приемлемого уровня.

В конечном итоге у владельца (пользователя) КС в результате реализации процесса анализа и контроля (управления) рисками должна быть уверенность в том, что:

- все возможные риски идентифицированы;
- уязвимости ресурсов идентифицированы и их уровни оценены;
- контрмеры эффективны;
- расходы, связанные с ИБ, оправданы.

В настоящее время на рынке присутствует достаточно широкий спектр инструментальных средств (программных продуктов) проведения полного анализа и управления рисками. Наиболее известные из них: CRAMM [2], LAVA, CONTMAT и др. [4]

Применение указанных средств позволяет получать обоснованные как количественные, так и качественные оценки рисков, уязвимостей, эффективности защиты. Достоинством таких методов является возможность проведения исследований в сжатые сроки и выполнять документирование результатов.

Список литературы: 1. *Герасименко В.А.* Защита информации в автоматизированных системах обработки данных. Кн. 1. М.: Энергоатомиздат, 1994. 400 с. 2. *Симонов С.* Анализ рисков. Управление рисками//Jet Info 1999. № 1. 3. *Аудит безопасности информационных систем* //Jet Info, 2000, № 1. 4. Bundesamt fur Sicherheit in der Information – stechnik. It Baseline Protection Manual, 1998, http://www.bsi.bund.de/gshb/english/etc/e-conten.htm 4. *Стенг Д., Мун С.* Секреты безопасности сетей. К.: Диалектика, 1995. 544 с.

Харьковский национальный университет радиоэлектроники

Поступила в редколлегию 13.05.2002