УДК 004.056.5
ББК 31

ОЦЕНКА УРОВНЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ ЧЕРЕЗ ОСТАТОЧНЫЙ РИСК

А.А. Семкина, А.М. Цыбулин

Для автоматизации процесса оценки уровня информационной безопасности предприятия разработана система мониторинга и аудита. В ее основу положена многозвеньевая система защиты и оценка остаточного риска.

Ключевые слова: *распределенная информационная система, атака, следы атаки, мониторинг, аудит, остаточный риск.*

В настоящее время для защиты информации на предприятии от возможных угроз используются различные средства безопасности, включая межсетевые экраны, антивирусы, системы защиты от спама, системы обнаружения атак, сканеры безопасности, средства защиты от утечки конфиденциальной информации и другие.

Современная распределенная информационная система (РИС) предприятия представляет собой сложную систему, состоящую из большого числа компонентов различной степени автономности, которые связаны между собой и обмениваются данными [1]. Практически каждый компонент РИС подвергается воздействию атак злоумышленника.

Наиболее уязвимыми к атакам являются программные средства и средства защиты информации РИС. Это могут быть атаки на операционную систему (ОС), на системы управления базами данных (СУБД), на межсетевой экран, на web-сервер (сетевые атаки), на коммуникационное оборудование и т. д.

Модель типовой РИС предприятия с воздействием атак на ее компоненты имеет вид, представленный на рисунке 1.

Каждая атака может оставить после себя следы. Следы – это информация, на основании которой можно прийти к выводу о воздействии атаки на какой-либо компонент РИС. Основными источниками такой информации являются журналы событий, системный реестр, сетевой трафик.

По результатам анализа методов мониторинга [2; 3; 5] и аудита [5] построена формальная модель системы мониторинга и аудита РИС.

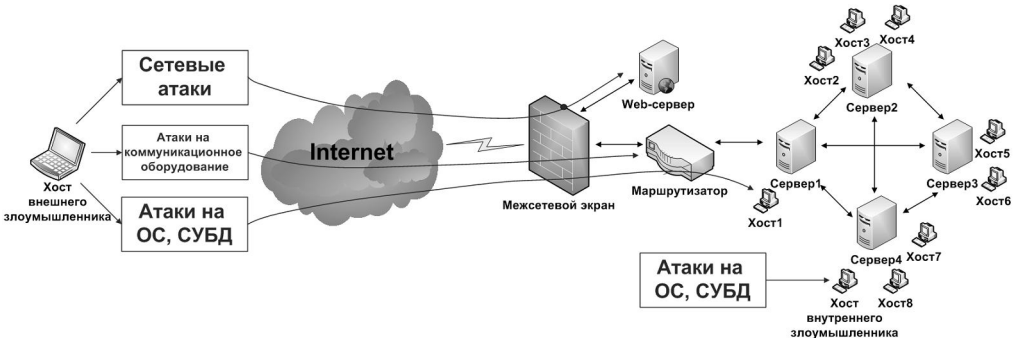

Рис. 1. Модель РИС предприятия с воздействием атак на ее компоненты

Формальная модель. Пусть на компонент K_i из множества рассматриваемых компонентов $K = \{K_1,...,K_n\}$ РИС ($i = \overline{1,n}$, где n – количество уязвимых к атакам компонентов РИС) могут оказывать воздействие атаки A_{i1}, A_{i2},…, A_{ij},…, A_{ir} из множества атак $A = \{A_1,..., A_m\}$ (r = 1,..., m, где r – возможное количество атак на i-й компонент, m – общее число возможных атак на РИС):

$$Aij = \begin{cases} 1, \text{если } i\text{-й компонент подвергся } j\text{-й атаке}, j = \overline{1,r}; \\ 0 \text{ в противном случае.} \end{cases}$$

На i-м компоненте j-я атака оставляет след G_{ijp} (p = 1,..., s , где s – количество следов), зарегистрированный в журнале событий, реестре или сетевом трафике:

$$Gijp = \begin{cases} 1, \text{если } j\text{-я атака оставляет след;} \\ 0 \text{ в противном случае.} \end{cases}$$

Таким образом, под следами j-й атаки понимается информация об одном или нескольких событиях, которые могут быть отнесены к аномальному поведению. Обработкой следов занимаются программные агенты, осуществляющие связь с другими агентами. После обработки следов агенты мониторинга производят выборку нужных событий и их параметров, после чего полученная информация вносится в базу данных.

Если в результате аудита эти данные расценены как атаки, они заносятся в таблицу атак базы данных (БД) и специалист по защите информации оповещается об их воздействии.

Результатом работы системы мониторинга и аудита являются данные об атаках, позволяющие оценить уровень безопасности РИС – информационный риск.

Наибольшее распространение среди методов оценки рисков получил метод «матрицы рисков».

Общий риск – это риск, перед лицом которого стоит предприятие, не внедрившее никаких защитных мер. Если его уровень недопустим для компании, она внедряет защитные меры, чтобы снизить риск до приемлемого уровня. Однако систем или сред, имеющих нулевой риск, не существует – всегда есть некоторый остаточный риск. Уровень остаточного риска должен быть приемлемым для компании [4].

На подготовительном этапе оценки риска экспертами определяются вероятности возникновения каждого риска P, размеры связанных с ним потерь Y (стоимость ущерба), а также допустимый остаточный риск $R_{ост\ доп}$ и заносятся в БД.

Все оценки рисков представляются в виде матрицы [8], которая представлена в таблице. В рассматриваемой матрице рисков стоимостная мера ущерба определяется в процентах от ценности информационного ресурса на i-м компоненте.

Остаточный риск вычисляется по формуле:

$$R_{ост}=P * Y, \qquad (1)$$

где P – вероятность воздействия атак, Y – стоимость ущерба. Оценка $R_{ост}$ будет достоверной только при условии учета одновременного воздействия всех атак на все компоненты РИС от всех категорий злоумышленников.

Пусть на i-й компонент ($i = \overline{1,I}$, где I – количество уязвимых к атакам компонентов рассматриваемой РИС) воздействует j-я атака ($j = \overline{1,J}$, где J – количество возможных атак злоумышленника на объект) в l-й зоне компонента со стороны нарушителя k-й категории ($k = \overline{1,K}$, K – число категорий нарушителей).

Матрица рисков (согласно рекомендациям NIST «Risk Management Guide for Information Technology Systems»)

Вероятность атаки (P)	Ущерб		
	Низкий 0 < Y < = 10 (%)	Средний 10 < Y < = 50 (%)	Высокий 50 < Y < = 100 (%)
Высокая (0,5 < P < = 1)	Низкий 5 < R < = 10 (%)	Средний 10 < R < = 50 (%)	Высокий 50 < R < = 100 (%)
Средняя (0,1 < P < = 0,5)	Низкий 1 < R < = 5 (%)	Средний 5 < R < = 25(%)	Средний 10 < R < = 50 (%)
Низкая (0 < P < = 0,1)	Низкий 0 < R < = 1 (%)	Низкий 0 < R < = 5 (%)	Низкий 0 < R < = 10 (%)

Вероятности P_{ijkl} воздействия j-й атаки на i-й компонент через l-ю зону уязвимости. При этом вероятность несанкционированного доступа к информации на i-м компоненте РИС путем проведения j-й атаки через l-ю зону будет равна произведению воздействующих на него атак от k-го злоумышленника:

$$P_{ikj} = \prod_{l} P_{ikjl}, \qquad (2)$$

где $l = \overline{1, L_k}$, L_k – количество защитных зон компонента для k-го злоумышленника.

Вероятность воздействия атак со стороны k-го злоумышленника будет равна:

$$P_{ik} = \sum_{j=1}^{J} P_{ikj}. \qquad (3)$$

Тогда вероятность несанкционированного получения информации на i-м компоненте со стороны всех потенциальных злоумышленников:

$$P_i = \sum_{k=1}^{K} P_{ik}. \qquad (4)$$

Вероятность несанкционированного доступа к информации РИС в целом будет равна:

$$P = \sum_{i=1}^{I} P_i. \qquad (5)$$

При этом стоимость ущерба для всей РИС предприятия будет равна:

$$Y = \sum_{i=1}^{I} Y_i. \qquad (6)$$

Таким образом, при подстановке формул (5) и (6) в формулу (1) получена формула общего остаточного риска для всей РИС предприятия:

$$R_{ост} = \sum_{i=1}^{I} P_i * \sum_{i=1}^{I} Y_i. \qquad (7)$$

Невыполнение условия:

$$R_{ост} \le R_{ост\ доп} \qquad (8)$$

означает, что система не защищена и необходимо обновить механизмы защиты.

Для реализации формальной модели разработана система мониторинга и аудита (на первом этапе для операционной системы РИС), архитектура которой представлена на рисунке 2.

Источниками информации об атаках на данном компоненте РИС являются журнал безопасности Windows и системный реестр.

Разработанный программный комплекс модели мониторинга и аудита состоит из следующих компонентов: программного комплекса, включающего программные агенты, экспертную систему, базу данных и пользовательский интерфейс, осуществляющий управление программным комплексом и взаимодействие со специалистом по защите информации; модели злоумышленника, необходимой для реализации программного комплекса; модели операционной системы.

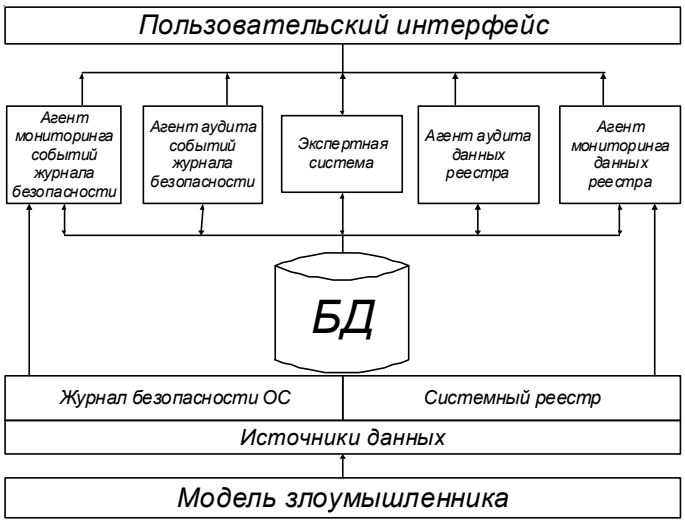

Рис. 2. Архитектура модели мониторинга и аудита

База данных. Для каждого объекта РИС в БД имеется 3 таблицы: таблица сведений о событиях, в которую внесена информация, собранная в результате мониторинга; таблица контрольных значений, с которыми в процессе аудита сравниваются значения из таблиц первой группы; таблица событий, идентифицированных как атаки на РИС, в которой содержится информация, полученная в результате аудита событий из первой таблицы.

Пример. Оцениваемый компонент РИС – хост 1, подключенный к серверу 1. На данный хост оказывают воздействие инсайдер и внешний злоумышленник (2 категории злоумышленников). Пусть со стороны злоумышленника первой категории могут оказывать воздействие следующие атаки: атака 1 «несанкционированный вход в систему» посредством подбора пароля входа в систему, атака 2 «несанкционированный доступ к объектам», атака 3 «несанкционированная загрузка системы». При этом инсайдер совершает злоумышленные действия только посредством атаки 1, то есть $A_{11}= 1$, $A_{12}= 0$, $A_{13}= 0$.

Данная атака оставляет след в журнале безопасности – событие 4625 – «не удалось осуществить вход в аккаунт»: $G_{111} = 1$.

На основании этих данных, а также данных экспертной системы, вычисленный по формуле (7) остаточный риск для компонента РИС составляет 23 % от ценности защищаемого ресурса в 100 тыс. рублей. Допустимый остаточный риск составляет 10 %. Так, условие (8) для данного компонента не выполняется. Согласно матрице рисков (см. таблицу), допустимый остаточный риск является низким, а вычисленный остаточный риск – средним. Следовательно, система не защищена и необходимо принять меры по снижению остаточного риска до приемлемого уровня и по усилению защиты РИС.

СПИСОК ЛИТЕРАТУРЫ

1. Варлатай, С. К. Аппаратно-программные средства и методы защиты информации / С. К. Варлатай. – Владивосток : ДВПИ, 2007. – 318 с.

2. «ДиалогНаука». – Электрон. текстовые дан. – Режим доступа: www.dialognauka.ru. – Загл. с экрана.

3. Дружинин, Е. Л. Мониторинг информационной безопасности ИТ-инфраструктуры / Е. Л. Дружинин. – М. : Презентация : Крок, 2008. – 12 с.

4. Информационная безопасность и управление рисками. – Электрон. текстовые дан. – Режим доступа: http://dorlov.blogspot.com/2009/06/issp-01-8.html. – Загл. с экрана.

5. Использование средств обнаружения вторжений. – Электрон. текстовые дан. – Режим доступа: http://www.lghost.ru/lib/security/kurs5/theme14_chapter01.htm. – Загл. с экрана.

6. Мельников, В. П. Информационная безопасность и защита информации / В. П. Мельников. – М. : Издат. центр «Академия», 2008. – 336 с.

7. Многофакторный анализ рисков информационной безопасности. Подходы и методы. – Электрон. текстовые дан. – Режим доступа: http://www.nestor.minsk.by/kg/2008/44/kg84403.html. – Загл. с экрана.

8. Stoneburner, G. Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology / G. Stoneburner, Goquen A., Feringa A. – Gaithersburg, USA, 2002. – 55 p.

ASTIMATION LEVEL OF INFORMATION SECURITY COMPANY THROUGH THE RESIDUAL RISK

A.A. Semkina, A.M. Tsybulin

The monitoring and audit system is developed for automation of process of performing the estimation f the level of information security of the enterprise. The iterative system of protection and an estimation of residual risk is put in its basis.

Key words: *distributed information system, attack, attacktraces, monitoring, audit, residual risk.*