

## **СРЕДСТВА УПРАВЛЕНИЯ РИСКАМИ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ**

Одним из важных аспектов повышения защищенности компьютерных систем является анализ существующих рисков безопасности информационных ресурсов. Предлагается комплексная система управления рисками безопасности, позволяющая анализировать возможные вторжения в компьютерные системы и выбирать наиболее эффективные средства защиты информации.

The prominent aspect of computer systems security level increasing is the analysis of existing risks for information resources safety. The complex safety risks control system is suggested. This system allows analyze the potential intrusions into computer systems and makes recommendation how to choose the most effective mechanisms for the information security.

### **Введение**

Риск безопасности компьютерных систем представляет собой возможность использования уязвимостей компьютерных систем с целью вторжения в них и нанесения определенного ущерба, при этом под уязвимостью понимаются ресурсы системы, используемые для реализации вторжений [1].

Для повышения защищенности компьютерных систем необходимо выполнять анализ рисков их безопасности, т.е. оценивать в какой степени применяемые средства безопасности информационных ресурсов способны защитить систему от угроз [2]. Процедура анализа рисков безопасности включает в себя: выделение защищаемых ресурсов, выявление угроз этим ресурсам и оценку вероятности реализации угроз безопасности. В процессе анализа рисков также оцениваются возможные потери вследствие реализации вторжений в систему, а также формируются рекомендации по применению средств защиты. Конечной целью процедуры анализа рисков является выбор эффективных средств защиты компьютерной системы, т.е., в частности, таких средств защиты, стоимость которых не превышает величины возможных потерь в результате совершения атак на систему.

В целом, анализ и управление рисками безопасности направлены на минимизацию возможных материальных и нематериальных потерь вследствие атак на систему.

### **Методы анализа рисков безопасности**

Современные методы анализа рисков безопасности подразделяются на две категории – количественные и качественные. [3]

*Количественные методы анализа рисков* основываются на оценке уровня риска для каждой угрозы с последующим расчетом суммарной величины возможных потерь в случае реализации вторжения. Средства на основе количественных методов анализа рисков позволяют сгенерировать специальный сводный отчет возможных потерь по каждой угрозе, в который входят два параметра:

1. вероятность реализации вторжения за определенный период времени;
2. величина потенциальных потерь в случае успешной реализации вторжения.

Далее, путем перемножения данных показателей, формируется обобщенная оценка возможных потерь вследствие совершенной атаки.

*Качественные методы анализа рисков*, в отличие от количественных, не предусматривают расчет точных значений параметров, а наличие риска выражается качественными параметрами, такими как "высокая", "средняя" или "низкая" степень риска. Данный подход обусловлен еще и тем, что некоторые потери ввиду вторжений, такие как искажение или модификация данных, не всегда могут быть выражены в терминах конкретных единиц (например, финансовых).

### **Сравнение количественных и качественных методов и средств анализа рисков безопасности**

В настоящее время расчет величины возможных потерь ввиду наступления страхового случая широко используется страховыми компаниями, т.е. фактически они применяют количественные методы анализа рисков. Однако, в отличие от страховых случаев, для которых необходимо лишь оценить затраты по выплате страховых премий, риски безопасности компьютерных систем имеют более сложный характер и оцениваются на основе анализа всего комплекса возможных последствий вследствие вторжений. Кроме того, риски безопасности компьютерных систем не всегда могут быть выражены лишь в финансово-кредитных терминах. Потенциальные потери часто могут быть вызваны такими факторами, как, например, взаимное доверие субъектов в системе или подобными.

Преимущество *количественных методов* состоит в возможности соотносить затраты на реализацию средств защиты с потенциальными потерями вследствие вторжения и выбирать эффективные средства защиты системы. Таким образом, анализ величины возможных потерь ввиду успешной атаки позволяет рассчитать величину требуемых затрат для предотвращения угроз, но с другой стороны, при расчетах используются данные, которые не всегда имеют достаточный эмпирический базис, и, в результате, полученные количественные оценки могут оказаться некорректными.

Главное преимущество *качественных методов* – минимизация времени и затрат на проведение анализа рисков. Количественные методы тре-

буют проведения детального анализа параметров безопасности компьютерной системы для выявления угроз и уязвимостей, а также оценки вероятности их реализации и величины требуемых затрат на средства защиты системы. На практике данный анализ требует значительных ресурсов. Качественные методы позволяют быстрее получить результат с меньшими затратами ресурсов, т.к. данные методы не требуют сбора дополнительных данных и сложных вычислений. Однако, анализ рисков безопасности по качественным параметрам (“высокий”, “средний” и “низкий” риск) представляет собой не строго детерминированный подход. Одну и ту же угрозу разные администраторы безопасности могут оценивать различно: одни ее воспринимают как “высокий” риск для системы, тогда как другие, наоборот, как “низкий” риск.

В целом, при выборе средств анализа рисков необходимо учитывать следующие факторы [4,5]:

- стоимость – величину затрат на организацию средств анализа и управления рисками;
- эффективность – необходимо выбрать наиболее эффективный метод анализа риска с учетом специфики функционирования данной компьютерной системы;
- адаптируемость – средства должны быть настраиваемыми для данной компьютерной системы.
- полноту – применяемые средства должны выявлять все возможные риски безопасности в системе.

Второй фактор (эффективность) особенно важен для администраторов безопасности, принимающих решения по организации системы безопасности. Оценка эффективности средств анализа и управления рисками безопасности включает в себя следующие действия:

1. устанавливается ряд показателей, которые характеризуют эффективность средства;
2. выполняются количественные оценки показателей эффективности с учетом вероятности реализации вторжения;
3. формируется интегральная оценка показателя эффективности, которая используется для сравнения различных методов и средств управления рисками безопасности.

В качестве показателей эффективности средств анализа и управления рисками безопасности предлагается использовать следующие 7 параметров:

1. постоянство – полученные результаты при независимом анализе варьируются незначительно при различных системных конфигурациях;
2. оптимальность – затраты на реализацию средств анализа и управления рисками безопасности не превышают величину потерь при вторжении;
3. гибкость – методы и средства должны быть применимы к различным конфигурациям компьютерной системы, при этом входные данные должны легко обновляться, т.к. они периодически изменяются;

4. доступность – требуемые для средств данные должны быть постоянно доступны;

5. комплексность – необходимо выполнять анализ всех параметров, характеризующих риски;

6. подлинность – результаты анализа рисков должны быть корректными;

7. доверие – результаты анализа рисков безопасности должны быть реалистичными и нести семантическую нагрузку.

Предлагается использовать комбинацию качественных и количественных методов анализа рисков для создания системы управления рисками безопасности информационных систем.

### **Система управления рисками безопасности компьютерных систем**

Предлагается система управления рисками безопасности, позволяющая оценивать применяемые средства защиты с учетом рисков безопасности, анализировать возможные вторжения в компьютерные системы и выбирать наиболее адекватные и эффективные средства защиты компьютерных систем. Структура данной системы управления рисками безопасности показана на рис.1.

Рассмотрим детальнее все пять подсистем в предложенной системе управления рисками безопасности.

1. *Подсистема анализа стоимости ресурсов и информации компьютерных систем.*

Данный анализ выполняется в два этапа. Вначале оценивается критичность обрабатываемой информации и каждому программному приложению присваивается уровень критичности, который связан с требуемой степенью защищенности обрабатываемых данных. На втором этапе оценивается стоимость аппаратных ресурсов компьютерной системы.

2. *Подсистема анализа вторжений и рисков безопасности.*

Данный анализ проводится в три этапа:

- выявляются уязвимости: устанавливаются “узкие” места или недостатки в проектировании или реализации средств управления безопасностью системы; проверяется совпадают ли данные уязвимости с ранее выявленными угрозами безопасности;
- оцениваются веса уязвимостей: для выявленных уязвимостей устанавливаются их взаимосвязи, после чего они ранжируются по степеням опасности их реализации;
- оценивается вероятность реализации угрозы.

3. Подсистема оценки потерь вследствие вторжений в компьютерные системы и затрат на реализацию средств защиты.

Потери вследствие реализации вторжений и затраты на средства защиты компьютерных систем оцениваются с учетом предоставляемого сред-

ствами защиты уровня безопасности. Учитывается стоимость средств защиты, вероятность того, что угрозы безопасности будут реализованы, а также возможные потери в результате реализации угрозы и определяется требуемый уровень защищенности системы с учетом минимизации затрат на реализацию средств защиты.

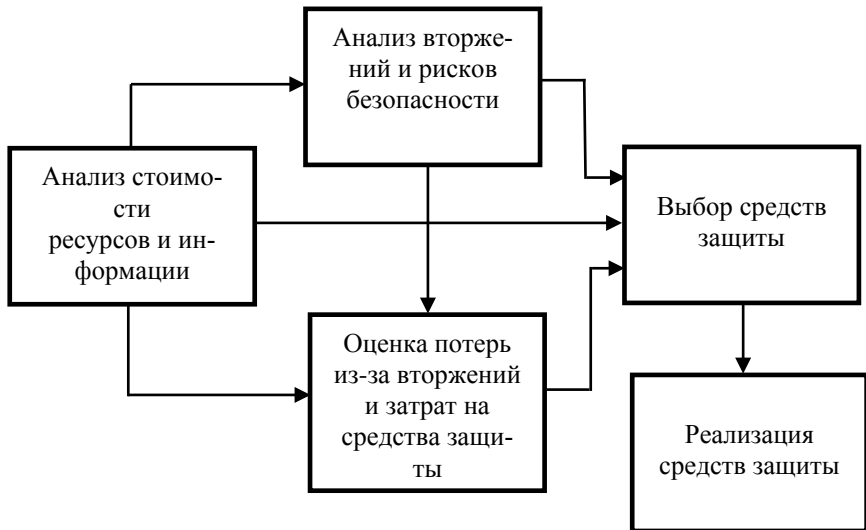


Рис. 1. Система управления рисками безопасности

#### 4. Подсистема выбора средств защиты компьютерных систем.

Данный блок позволяет выбрать эффективные средства защиты. Для выбора средств защиты компьютерных систем предлагается использовать метод поиска в пространстве решений.

В процессе выбора средств защиты используются следующие параметры:

$i$ :  $i$ -тое средство защиты,  $i = 1 \dots I$ ;

$j$ :  $j$ -тая угроза,  $j = 1 \dots J$ ;

$c_i$ : стоимость  $i$ -того средства защиты;

$f_{ij}$ : эффективность  $i$ -того средства защиты для предотвращения  $j$ -той угрозы (предполагается независимость средств защиты друг от друга);

$l_j$ : возможные потери, вызванные  $j$ -той угрозой;

$P_j$ : вероятность реализации  $j$ -той угрозы;

$V_i$ : ожидаемый эффект от применения  $i$ -того средства защиты;

$L$ : суммарные возможные потери вследствие реализации угроз безопасности;

$C$ : суммарная стоимость средств защиты;

ТС : суммарная величина стоимости средств защиты и потерь вследствие реализации угроз безопасности;

$v_j$  : рейтинговая оценка.

Алгоритм выбора средств защиты компьютерной системы включает следующие шаги:

1. Оценка возможных потерь вследствие реализации угрозы:

$$l_j = P_j * v_j \quad (1)$$

2. Расчет эффективности средств защиты:

$$B_i = \sum_{j=1}^J l_j * \left\{ 1 - \prod_{i=1}^I (1 - f_{ij}) \right\} \quad (2)$$

3. Расчет общих возможных потерь по всем средствам защиты:

$$L = \sum_{j=1}^J l_j * \prod_{i=1}^I (1 - f_{ij}) \quad (3)$$

4. Оценка суммарной стоимости средств защиты:

$$C = \sum_{i=1}^I c_i \quad (4)$$

5. Оценка величины суммарных возможных затрат по всем средствам защиты с учетом угроз безопасности:

$$TC = C + L \quad (5)$$

Главная задача средств анализа и управления рисками состоит в минимизации параметра ТС путем выбора соответствующих средств защиты.

Реализация средств защиты компьютерных систем.

Осуществляется в три этапа. На первом этапе устанавливается специфика реализации средств защиты, при этом учитывается степень опасности осуществления несанкционированных действий. На втором этапе собственно имплементируются средства защиты. На третьем этапе параметры средств защиты оцениваются и верифицируются. Критичные компьютерные системы, к безопасности которых предъявляются особые требования, проходят оценку и тестирование применяемых в них средств защиты в процессе разработки и начальной эксплуатации системы. Задача тестирования состоит в подтверждении эффективности применяемых средств защиты и отсутствия нежелательных побочных эффектов.

Для демонстрации предложенной системы управления рисками безопасности проведем экспериментальные исследования. Предположим, что существует 5 возможных угроз: 1) вирус, 2) превышение полномочий легальным пользователем, 3) вход злоумышленника в систему при отказе в обслуживании легальному пользователю, 4) нарушение функционирования системы и 5) несанкционированный доступ незарегистрированным пользователем.

Рассмотрим три варианта реализации средств управления доступом к ресурсам компьютерных систем: 1) Контролируемое управление доступом (DAC), 2) Мандатное управление доступом (MAC) и 3) Ролевое управление доступом (RBAC).

В табл. 1 и табл. 2 представлена информация по вероятностям реализации угроз безопасности и соответствующим возможным потерям, а также по эффективности средств защиты в зависимости от типа угроз безопасности. Оценка стоимости суммарных затрат по всем угрозам безопасности для различных средств защиты информации проводится с учетом вероятности реализации угроз безопасности и величины возможных потерь и составляет: для средства на основе DAC – 3840 условных единиц (у.е.), на основе MAC – 2020 у.е., на основе RBAC – 1350 у.е. Таким образом, для средств на основе RBAC характерны наименьшие возможные потери в случае попыток реализации угроз безопасности и данные средства являются наиболее эффективными.

Табл. 1. Угрозы безопасности, вероятности их реализации и возможные потери

Тип угрозы	Вероятность реализации	Возможные потери, у.е.
Вирус	0.3	2000
Превышение полномочий легальным пользователем	0.1	4000
Вход при отказе в обслуживании	0.1	3000
Нарушение функционирования системы	0.2	5000
Несанкционированный доступ незарегистрированным пользователем (НП)	0.5	4000

Табл. 2. Эффективность средств защиты (управления доступом) в зависимости от типа угроз безопасности

Угроза/Средство защиты	Вирус	Превышение полномочий легальным пользователем	Вход при отказе в обслуживании	Нарушение функционирования системы	Несанкционированный доступ НП
DAC	0.1	0.1	0.2	0.1	0.1
MAC	0.5	0.5	0.6	0.4	0.6
RBAC	0.8	0.9	0.7	0.7	0.6

Таким образом, предлагаемая система управления рисками безопасности является вспомогательным инструментом администратора безопасности для определения требуемого уровня безопасности ресурсов компьютерной системы, выявления угроз, для оценки величины потерь, которые

могут возникнуть в случае реализации угроз безопасности, и, наконец, для выбора эффективных средств защиты.

### **Заключение**

В настоящий момент весьма актуальными являются исследования в области:

- разработки эффективных методов принятия решения в условиях множественных угроз безопасности;
- дифференциации средств защиты компьютерных систем в соответствии с используемыми в них механизмами защиты в зависимости от типа угроз безопасности;
- разработки методов анализа требуемого уровня защищенности компьютерных систем с учетом оценки вероятности реализации угроз безопасности.

Также актуальным является усовершенствование системы управления рисками безопасности для более корректной работы с расширенным набором исходных данных по событиям безопасности в компьютерных системах, в частности, на основе статистических данных компаний, например, занимающихся электронной коммерцией, для верификации корректности полученных результатов и рекомендаций на практике.

### **Список использованной литературы**

1. C. Alberts, A. Dorofee. Managing Information Security Risks. The Octave Approach. SEI Series, Addison Wesley, 2003. – 205 p.
2. F. Farahmand, S. B. Navathe, P. Sharp Gunter, P.H. Enslow. Managing Vulnerabilities of Information Systems to Security Incidents.//ACM ICEC September 2003, Pittsburg, USA. – pp. 125-133.
3. A. Freeman. Cyber Risk Management and National Strategy to Secure Cyberspace.// The Open Group Conference Proceedings, Feb. 2003. – pp. 63-69.
4. L.A. Gordon, M.P. Loeb, T. Sohail. A Framework for Using Insurance for Cyber-Risk Management. //Communications of ACM, Vol. 46, N. 3, March 2003. – pp. 81-85.
5. П. Покровский. Оценка информационных рисков. // LAN, 2004. – Т. 10, N.10. – с.90-95.