УДК 65.012.8: 004.492

Г.Г. Гроздов
Служба безопасности Украины

Стратегии построения эффективной комплексной системы защиты информации в автоматизированных системах

Рассматриваются вопросы построения эффективной комплексной системы защиты информации. Предложена методика, построенная на математической теории игр.

Эффективная система защиты информации, математическая теория игр

В наши дни особо остро стоит проблема защиты информации в автоматизированных системах (АС). Для решения указанной задачи каждая АС должна включать подсистему защиты информации, которая должна обеспечивать комплексную защиту информации (КСЗИ).

В настоящее время актуальна проблема разработки эффективных систем защиты информации. При этом следует рассматривать различные аспекты эффективности. Во-первых, система защиты информации должна эффективно противодействовать угрозам, которые могут нанести ущерб защищаемой информации (проблема эффективности механизмов защиты информации). Во-вторых, процесс защиты информации в автоматизированной системе можно рассматривать как процесс распределения ресурсов, выделяемых на защиту информации (проблема экономической эффективности).

Существующие методики формирования эффективной системы защиты информации, их недостатки

К наиболее известным методикам формирования эффективной КСЗИ относятся метод ожидаемых потерь и методика совокупной стоимости владения. Несмотря на свои достоинства, указанные методики имеют ряд недостатков:

- метод ожидаемых потерь рассматривает риски как математическое ожидание потерь. Эта методика не учитывает многих факторов, оказывающих влияние на безопасность информации. Например, не были учтены потери, которые могла понести АС вследствие применения механизмов защиты информации;
- метод ожидаемых потерь и методика совокупной стоимости владения эффективны для оценки СЗИ АС, обрабатывающих информацию, составляющую коммерческую тайну и не учитывают многих аспектов защиты информации, составляющую государственную тайну.

Постановка целей исследования

Сформулируем задачи исследования:

- разработка методики решения задачи формирования эффективной КСЗИ АС, которая бы гарантировала существование варианта построения КСЗИ из имеющихся в наличии механизмов ЗИ;
- указанная методика должна предоставлять возможность выбора между разными вариантами построения КСЗИ АС; должны быть видны преимущества и недостатки каждого из вариантов;
- методика должна обеспечивать единый подход формирования КСЗИ АС для защиты информации, которая составляет государственную, военную или коммерческую тайну. Кроме того, методика должна учитывать возможности формирующей КСЗИ и атакующей сторон.

В работах [1, 2] приведено описание модели формирования эффективной КСЗИ АС. На Рис.1 приведена общая модель процесса формирования эффективной КСЗИ АС. В работе рассматривались два аспекта эффективности КСЗИ АС: для АС, обрабатывающих информацию, которая является коммерческой и государственной (военной) тайной.

В модели использованы следующие обозначения:

$\{A\}$ - множество средств реализации атак на АС;

$\{LA\}$ - множество возможных распределенных атак на АС;

$\{LT\}$ - множество уязвимостей компонентов АС;

$\{MR\}$ - множество параметров использования ресурсов АС;

$\{P\}$- множество нарушителей;

$\{TS\}$ - технологическая схема функционирования АС;

$\{U\}$- множество угроз информации.

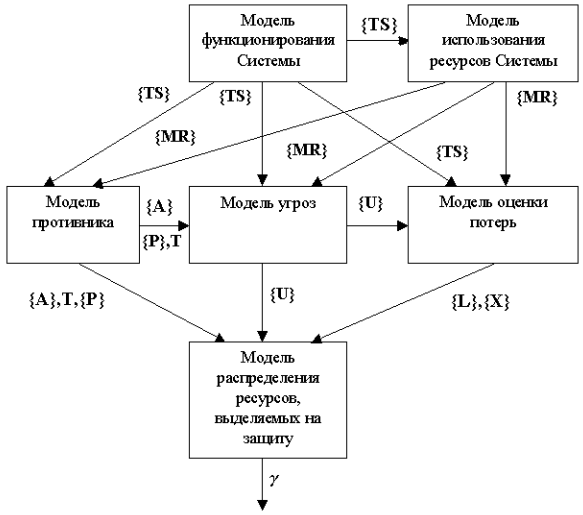

Рисунок 1 – Общая модель процесса формирования эффективной КСЗИ АС

Новая методика построения модели угроз АС

На рис. 1 приведена общая модель процесса формирования множества угроз информации в АС.

Сформулируем задачи, которые должны быть решены для построения модели угроз АС:

1. Разработать модель функционирования АС и модель использования ее ресурсов. Результатом должна быть технологическая схема функционирования АС ({TS}) и множество параметров использования ресурсов АС ({MR}).

2. На основании результатов предыдущего этапа построить модель уязвимостей АС. Указанный этап необходим для адекватной оценки уязвимостей АС, что позволит в последствии разработать модель распределенных атак на АС. Результатом этапа станет множество уязвимостей компонентов АС ($\{LT\}$). (К компонентам АС относятся информация, аппаратное и программное обеспечение, обслуживающий персонал и физическая среда [19]).

3. Исходя из множества уязвимостей компонентов АС ({LT}), а также результатов первого этапа, сформировать модель распределенной атаки на АС. Результатом моделирования станет полный перечень возможных атак на АС ($\{LA\}$). Классы уязвимостей компонентов АС приведены в приложении А.

4. На основании технологической схемы АС ({TS}) построить модель противника, оценить его возможности. Результатом построения указанной модели должны стать сведения о категориях противника ($\{P\}$), его возможностях по реализации атак ($\{A\}$).

5. Разработать модель угроз информации АС. В качестве исходных данных для построения этой модели необходимы: множество уязвимостей компонентов АС ($\{LT\}$), полный перечень возможных атак на АС ($\{LA\}$), сведения о категориях противника ($\{P\}$), его возможностях по реализации атак ($\{A\}$). Результатом этого этапа моделирования должен стать список угроз информации ($\{U\}$). При этом для каждой угрозы АС будет поставлен в соответствие способ ее реализации (элемент множества $\{LA\}$), а также необходимые условия для реализации угрозы (элемент множества $\{LT\}$).

Таким образом, общая модель формирования с учетом распределенных атак на АС примет такой вид (Рис.2).

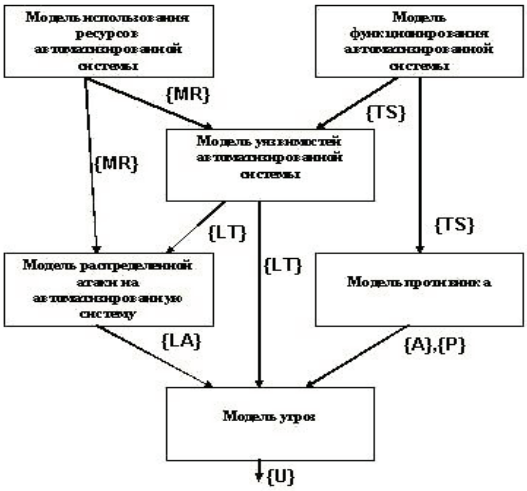

Рисунок 2 – Общая модель процесса формирования множества угроз информации в АС

Модель функционирования АС может быть формально представлена в виде функции:

$$F\_MF(AS) \rightarrow \{TS\}$$

В качестве исходных данных функции будет выступать АС. Результатом указанной функции будет формальное описание технологии функционирования системы.

Модель использования ресурсов АС представляет собой функцию:

$$F\_IR(\{AS\},\{TS\}) \rightarrow \{MR\}$$

где $\{TS\}$- формальное описание технологии функционирования АС;

$\{MR\}$-формальное описание ресурсов, используемых АС на различных этапах обработки информации.

Модель уязвимостей АС представляет следующую функцию:

$$F\_MT(\{TS\},\{MR\}) \rightarrow (\{LT\});$$

где {*TS*} - формальное описание технологии функционирования АС;

{*MR*} - формальное описание ресурсов, используемых АС на различных этапах обработки информации;

{*LT*} - множество уязвимостей компонентов АС.

Модель распределенной атаки представляет следующую функцию:

$$F\_MA(\{LT\},\{MR\}) \rightarrow (\{LA\});$$

где {*TS*} - формальное описание технологии функционирования АС;

{*MR*} - формальное описание ресурсов, используемых АС на различных этапах обработки информации;

{*LA*} - множество возможных распределенных атак на АС.

Модель противника представляет следующую функцию:

$$F\_MP(\{TS\},\{MR\}) \rightarrow (\{P\},\{A\});$$

где {*TS*} - формальное описание технологии функционирования АС;

{*MR*} - формальное описание ресурсов, используемых АС на различных этапах обработки информации;

{*P*} - множество категорий злоумышленников;

{*A*} - множество средств для реализации атак на АС.

Модель угроз описывает следующая функция:

$$F\_MU(\{MR\},\{TS\},\{LA\},\{LT\},\{A\},\{P\}) \rightarrow \{U\}$$

где {*TS*} - формальное описание технологии функционирования АС;

{*MR*} - формальное описание ресурсов, используемых АС на различных этапах обработки информации;

{*LA*} - множество возможных распределенных атак на АС.

{*LT*} - множество уязвимостей компонентов АС.

{*A*} - множество средств реализации атак на АС;

{*P*}- множество категорий злоумышленников;

{*U*} - формально описанное множество угроз информации АС.

Рассмотрим порядок взаимодействия моделей. На первом этапе производится разработка модели функционирования АС. Результаты этого этапа будут использованы во всех последующих моделях процессов защиты информации. Итогом моделирования должна стать технология функционирования АС, которая описана формально.

После получения описания технологии функционирования АС необходимо определить ресурсы АС, то есть определить, какие ресурсы используются АС для решения задач по обработке информации. Далее, необходимо формально описать схему использования ресурсов. В дальнейшем эта схема будет нужна для определения возможных объектов атак злоумышленников, она понадобится при формировании каналов утечки информации и т. д.

Дальнейшим этапом является разработка модели уязвимостей АС. Исходными данными будут выступать технология функционирования и модель используемых ресурсов. Результатом моделирования будет перечень "пассивных" угроз информации [9]. Иллюстрация множества {LT} для участка функционирования типовой АС приведена в приложении А в табл.А.1.

Следующим этапом является разработка модели противника. Для этого понадобятся результаты предыдущих этапов: технология функционирования и схема использования ресурсов. Указанные данные помогут классифицировать возможного противника, что в свою очередь позволит в дальнейшем построить адекватную систему защиты информации. Результатом построения модели противника должно стать множество возможных категорий злоумышленников, а также объем финансовых средств и возможностей, которыми они обладают.

Следующим этапом является разработка модели распределенной атаки на АС. В качестве исходных данных будут выступать модель ресурсов АС {*MR*}и перечень уязвимостей АС {*LT*}. Результатом этапа выступит список возможных распределенных атак на АС {*LA*}.

Когда указанные выше этапы будут завершены, можно приступать к работам по формированию модели угроз информации. Исходными данными для моделирования будут списки уязвимостей {*LT*}и распределенных атак на АС {*LA*}, а также множества средств для реализации атак на АС {*A*}и категорий злоумышленников {*P*}. Результатом этого этапа моделирования должен быть перечень угроз информации системы {*U*}. При этом каждый элемент перечня должен содержать информацию о категориях злоумышленников, которые могут реализовать указанную угрозу. Кроме того, должны быть указаны свойства информации, которые будут нарушены в случае успешной реализации угрозы.

Будем полагать, что переменные {*AS*} и {*A*} заданы изначально.

Рассмотрим размерности и ограничения, накладываемые на переменные общей модели.

Множество средств реализации атак на объект защиты {*A*} представляет собой массив из двух столбцов и *N* строк, где *N* - число средств реализации атак. К параметрам средства реализации атак относятся название средства и его цена.

К числу параметров, описывающих объект защиты ({*AS*}) относятся характеристики АС: режим эксплуатации, количество пользователей, характеристика обрабатываемой информации, параметры аппаратного и программного обеспечения и т. д.

Множество параметров использования ресурсов АС {*MR*} представляют множества ресурсов аппаратного и программного обеспечения, формы представления информации во время ее обработки, категории обслуживающего персонала и пользователей, параметры внешней среды.

Множество категорий противника {*P*} хранится в массиве из трех столбцов и *N* строк, где *N* - число категорий противника. Для каждой категории противника указываются уровни знаний и навыков, а также арсенал методов, которыми располагает противник.

T - время, которым располагает атакующая сторона для реализации угроз.

Технологическая схема функционирования АС ({*TS*}) включает в свой состав два множества: участок функционирования АС и связей между ними.

Список уязвимостей {*LT*} представляет собой вектор известных пассивных угроз для компонентов АС.

Список возможных распределенных атак на АС {*LA*} представляет собой вектор возможных путей реализации распределенных атак на АС. Каждый путь реализации атаки включает множество уязвимостей компонентов АС, которые должны быть использованы нарушителем политики безопасности.

Множество угроз информации ({*U*}) - это массив из *N* строк, где *N* - число угроз информации, и двух столбцов. Для каждой угрозы указывается ее словесное описание, а также свойства информации, которые она нарушает.

Методика построения модели распределенной атаки на автоматизированную систему

В предлагаемой методике построения модели распределенной атаки на АС воспользуемся математическим аппаратом теории графов. Будем называть графом атаки такой граф, в котором приведены все возможные последовательности действий нарушителя для достижения своих целей. Каждую из указанных последовательностей назовем трассой атаки. Исходя из вышеизложенного, методика формирования модели распределенной атаки будет выглядеть следующим образом:

1. Составить вектор *IR* для элементов формального описания информационных ресурсов, используемых АС на различных этапах обработки информации ({*MR*}).

2. Для каждого элемента вектора *IR* составить множество путей доступа к элементу *IR(i)*. Для этого использовать алгоритм поиска всех путей в графе [5]. Результаты занести в таблицу вида < *IR(i)* >< {*T*} >< {*NL*} >, где:

   IR(i) - элемент формального описания информационных ресурсов, используемых АС на различных этапах обработки информации;

   {*T*}-множество возможных трасс доступа к нему. Под трассой доступа будем понимать необходимую последовательность действий, которую необходимо выполнить – успешное прохождение процедур аутентификации и авторизации на уровне различного ПО компонентов АС и т.п.;

   {*NL*}-множество необходимых условий. Под условиями будем понимать необходимые настройки в ПО компонентов АС: ОС, СУБД, прикладного и специализированного ПО. К ним относятся – учетные данные пользователей, полномочия по доступу к ресурсам, настройки подсистем безопасности – ОС, СУБД, прикладного и специализированного ПО.

3. Для каждой из полученных трасс рассмотреть варианты несанкционированного чтения, создания необходимых условий для доступа к информации *IR(i)*.

4. Совокупность полученных вариантов даст множество трасс атак для *IR(i)*.

5. Повторить пункты 2-4 для всех элементов вектора *IR*.

Методика формирования эффективной комплексной системы защиты информации автоматизированной системы на основе методов теории игр

Порядок разработки КСЗИ АС описан в [2], вопросы построения эффективной КСЗИ АС рассматривались автором в [1, 2, 3]. В качестве математического аппарата для построения новой модели будет использована математическая теория игр.

Из теории игр известен способ, как обеспечить гарантированную границу своего проигрыша, хуже которого быть не должно [6]. Новая методика предполагает следующий подход: должны быть рассмотрены все без исключения варианты использования существующих механизмов ЗИ в составе КСЗИ АС. При этом каждый вариант использования механизмов ЗИ будет описан бинарным вектором γ.

Всего необходимо рассмотреть $2^m - 1$ вариантов построения КСЗИ. Множеством поиска решений будут все значения бинарных векторов размерности *M*, за исключением вектора, состоящего из одних нулей. Вызвано это тем обстоятельством, что КСЗИ должна функционировать в составе всех АС [1, 2, 3].

Для каждого из бинарных векторов γ необходимо вычислить размер остаточного риска (1), а также размер средств, выделяемых на обеспечение ЗИ в АС (2).

$$R(\gamma) = \sum_{i=1}^{N} L_i (P_i - \sum_{j=1}^{M} G_{ij} \cdot \gamma_j); \quad (1)$$

$$C_{\text{d}} = \sum_{j=1}^{M} \gamma_{\text{j}} \cdot (C(\gamma)_{\text{j}} + X(\gamma)_j); \quad (2)$$

Таблица 1 содержит описание переменных, используемых в модели формирования КСЗИ АС, где 1 - обозначения переменных, 2 - значения переменных, 3 - ограничения переменных, 4 - размерности переменных.

Таблица 1

Параметры переменных, используемых в модели формирования КСЗИ АС

1	2	3	4
R	размер остаточного риска	$R_i > 0$	гривны
N	число угроз информации	$N > 0$	-
L_i	оценка стоимости потерь в случае реализации *i*-ой угрозы	$L_i > 0$	гривны
P_i	вероятность реализации *i*-ой угрозы	$0 \le P_i \le 1$	-
M	число существую-щих средств защиты	$M > 0$	-
G_{ij}	Эффектив-ность *j*-го механизма защиты информации по нейтрализации i-ой угрозы	$0 \le G_{ij} \le 1$	-
γ_{i}	признак использования *i*-го механизма защиты информации в составе КСЗИ АС (равен 1, если механизм задействован в составе КСЗИ, в противном случае равен нулю)	$\gamma_{\text{i}} \in (0;1)$	-
C_{d}	средства, которые могут быть выделены на защиту информации в АС	$C_{\text{d}} > 0$	гривны
C_{j}	затраты на приобретение (разработку) и использование *j*-го механизма защиты информации	$C_{\text{j}} > 0$	гривны
X_j	размер потерь АС, вызванных использованием *j*-го механизма защиты информации в составе КСЗИ АС	$X_j > 0$	гривны
$C(A_j)$	стоимость *j*-го средства реализации угроз информации	$C(A_j) > 0$	гривны
$C_{прот}$	размер финансовых средств, которыми располагает противник	$C_{прот} > 0$	-
Ψ_{ij}	возможности *j*-ого средства по реализации *i*-ой угрозы информации (коэффициент равен 1, если *j*-ое средство способно	$\Psi_{ij} \in (0;1)$	-

1	2	3	4
	создать *i*-ую угрозу информации; в противном случае коэффициент равен 0)		

В результате будет сформирована таблица, в которой первый столбец – вектор γ_i, второй - размер остаточного риска при использовании варианта (R_i), третий - размер затрат на построение КСЗИ (C_d).

Полученная таблица будет выступать в качестве информационного множества, описывающего игровую модель [6]. Ходами в игре выступают варианты использования существующих механизмов ЗИ в АС (варианты вектора γ_i).

Как отмечается в [6], теория игр позволяет найти решение, оптимальное или рациональное в среднем.

Определение вероятности проявления i-ой угрозы

В настоящее время одним из важнейших требований к КСЗИ АС является ее адекватность реальным условиям [4]. Для построения адекватной системы защиты информации необходимо реально оценить возможности вероятного противника.

При определении вероятностей проявления угроз информации будем полагать, что все множество угроз информации АС формируется из множества активных и пассивных угроз. Причиной возникновения пассивных угроз будем считать уязвимости и особенности компонентов АС, активных – действия вероятного противника.

Будем полагать, что вероятность любой угрозы информации определяется через вероятность "активной" (R_{a_i}) и "пассивной" (R_{n_i}) составляющей угрозы.

Значение R_{n_i} может быть получено статистическими методами, или выведено с помощью метода экспертных оценок [4].

При оценке возможных действий противника сложно определить, какой именно из доступных способов будет им выбран для нанесения ущерба объекту защиты. Таблица 2 содержит порядок средств, выделяемых на реализацию атак различными категориями злоумышленников.

Таблица 2

Сравнительный анализ возможностей вероятного противника

Категории вероятного противника	Средства, выделяемые для реализации атак (доллары США)
Одиночки	100
Группы хакеров	1.000
Мелкие преступные группы	100.000
Крупные преступные группы	1.000.000
Транснациональные преступные организации, спецслужбы иностранных государств	100.000.000

Поэтому при получении составляющей R_{a_i} будем исходить из наихудших предположений о возможностях противника [4]. Значение R_{a_i}=1, если финансовые возможности противника превышают стоимость хотя бы одного из средств нападения, способного вызвать дестабилизирующий фактор. В противном случае элемент вектора будет равен 0.

Формально эта зависимость может быть описана таким образом:

R_{a_i}=1, если $\min(C(A_j)) \le C_{прот}$, для которых $\Psi_{ij} = 1$,

где A_j - *j*-ое средство реализации угрозы информации;

$C(A_j)$ - стоимость *j*-го средства реализации угроз информации;

$C_{прот}$ - размер финансовых средств, которыми располагает противник;

Ψ_{ij} - возможности *j*-ого средства по реализации *i*-ой угрозы информации (коэффициент равен 1, если *j*-ое средство способно создать *i*-ую угрозу информации; в противном случае коэффициент равен 0).

Вероятность проявления i-ой угрозы может быть получена следующим образом:

$$R_i = \max(R_a; R_n).$$

Выбор стратегии построения комплексной системы защиты информации

При формировании КСЗИ АС, обрабатывающих информацию, которая составляет государственную, военную или коммерческую тайну могут быть использованы различные критерии.

Рассмотрим стратегии, которые могут быть выбраны в случае, когда возможности

атакующей стороны значительно уступают возможностям формирующего КСЗИ.

1. Увеличить размер остаточного риска (*R*) при своих малых значениях средств, которые могут быть потрачены на реализацию атаки.

2. Увеличить затраты на приобретение (разработку) и использование *j*-го механизма защиты информации (C_j), а также размер потерь АС, вызванных использованием *j*-го механизма защиты информации в составе КСЗИ АС (X_j).

3. Дезинформировать формирующего КСЗИ, чтобы существующая КСЗИ была перестроена. Указанная мера приведет к уменьшению C_d.

Рассмотрим стратегии, которые могут быть выбраны в случае, когда возможности атакующей стороны равны возможностям формирующего КСЗИ.

1. Найти такие γ_i, при которых у формирующего КСЗИ не хватит средств, которые могут быть выделены на защиту информации в АС (C_d).

2. Найти такие механизмы реализации атаки, чтобы у атакующей стороны на них C_d средств хватило, а у формирующего КСЗИ – нет.

Рассмотрим стратегии, которые могут быть выбраны в случае, когда возможности атакующей стороны значительно превышают возможности формирующей КСЗИ.

1. Атакующая сторона выбирает много вариантов γ_i для одновременной реализации – у формирующего КСЗИ не хватит финансовых средств (C_d) для противодействия.

2. Атакующая сторона выбирает такие варианты реализации атаки на АС, чтобы у формирующего КСЗИ не хватило финансовых средств для построения эффективной КСЗИ ("тактика истощения").

Заключение

В перспективе представляется рациональным использовать методы математической теории игр для описания процесса защиты информации как процесса бесконечной антагонистической игры с неполной информацией. При этом могут быть рассмотрены различные стратегии игроков, в том числе вопросы формирования коалиций (как атакующей стороной, так и формирующей КСЗИ АС).

Список литературы

1. Гроздов Г.Г. Методика построения модели распределенной атаки на автоматизированную систему / Г.Г. Гроздов // Науково-практичний журнал. Сучасна спеціальна техніка. – 2009. –№3. – С. 82-90.

2. Гроздов Г.Г. Модифицированный способ решения задачи формирования эффективной комплексной системы защиты информации автоматизированной системы: монографія / Г.Г. Гроздов. – К.: ГУИКТ, 2009. - 32 с.

3. Гроздов Г.Г. Методика построения теста на проникновение в автоматизированную систему, основанная на математической теории игр / Г.Г. Гроздов // Наукові записки українського науково-дослідного інституту зв`язку. – 2010. – № 3. – С. 88-94.

4. Лукацкий А.В. Обнаружение атак / А.В. Лукацкий. - С-Пб: BHV, 2001. - 611 с.

5. Майника Э. Алгоритмы оптимизации на сетях и графах / Э. Майника. – М. : Мир, 1981. - 328 с.

6. Мак-Кинси.Д. Введение в теорию игр / Д. Мак-Кинси. – К.: Издательство КВИРТУ, 1959. - 347 с.

Надійшла до редколегії 20.03.2011

Г.Г. ГРЄЗДОВ
Служба безпеки України

G.G. GREZDOV
Security Service of Ukraine

Стратегії побудови ефективної комплексної системи захисту інформації в автоматизованих системах

Розглянуто питання побудови ефективної комплексної системи захисту інформації. Запропоновано методику, яка побудована на математичній теорії ігор.

ефективна система захисту інформації, математична теорія ігор

Strategy of Constructing an Effective Complex System for data Protection in Automated Systems

Questions of constructing an effective complex system for data protection are considered. A technique based on the mathematical theory of games is offered.

effective system for data protection, mathematical theory of games