УДК 65.012.8: 004.492

Гроздов Г.Г., *к.т.н.*

УЛУЧШЕННЫЙ СПОСОБ РЕШЕНИЯ ЗАДАЧИ ФОРМИРОВАНИЯ ЭФФЕКТИВНОЙ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ

Гроздов Г. Г. Покращений спосіб розв'язання задачі формування ефективної комплексної системи захисту інформації автоматизованої системи. Запропоновано спосіб побудови комплексної системи захисту інформації із врахуванням моделей і принципів організації розподілених атак на автоматизовану систему. Приведені очікувані результати використання запропонованих механізмів захисту, дана оцінка витат на реалізацію способу. Окреслені шляхи подальших перспективних досліджень.

Ключові слова: ЗАХИСТ ІНФОРМАЦІЇ, МОДЕЛЬ РОЗПОДІЛЕНОЇ АТАКИ, ЗАЛИШКОВИЙ РИЗИК, КОМЕРЦІЙНА (ВІЙСЬКОВА, ДЕРЖАВНА ТАЄМНИЦЯ), ОЦІНКА ВТРАТ

Гроздов Г. Г. Улучшенный способ решения задачи формирования эффективной комплексной системы защиты информации автоматизированной системы. Предложен способ построения комплексной системы защиты информации с учетом моделей и принципов организации распределенных атак на автоматизированную систему. Приведены ожидаемые результаты использования предложенных механизмов защиты, дана оценка затрат на реализацию способа. Очерчены пути дальнейших перспективных исследований.

Ключевые слова: ЗАЩИТА ИНФОРМАЦИИ, МОДЕЛЬ РАСПРЕДЕЛЕННОЙ АТАКИ, ОСТАТОЧНЫЙ РИСК, КОММЕРЧЕСКАЯ (ВОЕННАЯ, ГОСУДАРСТВЕННАЯ ТАЙНА), ОЦЕНКА ПОТЕРЬ

Grezdov H. H. An improved way to solve the problem for the construction of an effective complex data protection system in automated system. The method of construction of the complex data protection system taking into account models and principles of organization of up-diffused attacks on the automated system is proposed. The expected results of the use of proposed protection mechanisms are presented; cost estimates for the implementation of this method is given. The ways of further advanced research are outlined.

Keywords: DATA PROTECTIONRIV, MODEL OF UP-DIFFUSED ATTACK, RESIDUAL RISK, COMMERCIAL (MILITARY, STATE) SECRET, ESTIMATION OF LOSSES

В настоящее время актуальна задача построения и оценки эффективности механизмов защиты информации в различных комплексных системах защиты информации (КСЗИ) автоматизированных систем (АС). Различают два основных класса информации, защита которых должна обеспечиваться КСЗИ: информация, составляющая *коммерческую* и *государственную (военную)* тайну. В АС указанных классов могут иметь приоритетное значение различные требования к механизмам защиты информации (ЗИ) [1, 2].

В научно-технической литературе рассматриваются два аспекта эффективности системы ЗИ. С одной стороны, система ЗИ должна эффективно противодействовать угрозам [3]. С другой стороны, она должна быть адекватной – расходы на безопасность не должны превышать стоимости самой информации и размера возможных потерь, вызванных успешной реализацией угроз [4].

Существующие методики формирования системы ЗИ. Существует немало алгоритмов, осуществляющих анализ рисков информационной системы (ИС). К наиболее известным алгоритмам относятся CRAMM и RiskWatch [5, 6]. Указанные алгоритмы имеют ряд достоинств и получили широкое распространение. Есть и другие подходы к формированию моделей угроз информации [2, 7].

В работах [4, 7] приведено описание модели формирования эффективной КСЗИ АС.

На рис.1 приведена общая модель процесса формирования эффективной КСЗИ АС. В модели использованы следующие обозначения: $\{A\}$ – множество средств реализации атак на АС; $\{X\}$ – множество потерь АС, вызванных использованием КСЗИ; $\{L\}$ – множество потерь АС; $\{MR\}$ – множество параметров и формальное описание ресурсов, используемых АС на различных этапах обработки информации; $\{P\}$– множество категорий злоумышленников и нарушителей; $\{TS\}$ – формальное описание технологии функционирования АС; $\{U\}$– формальное описанное множества угроз информации АС.

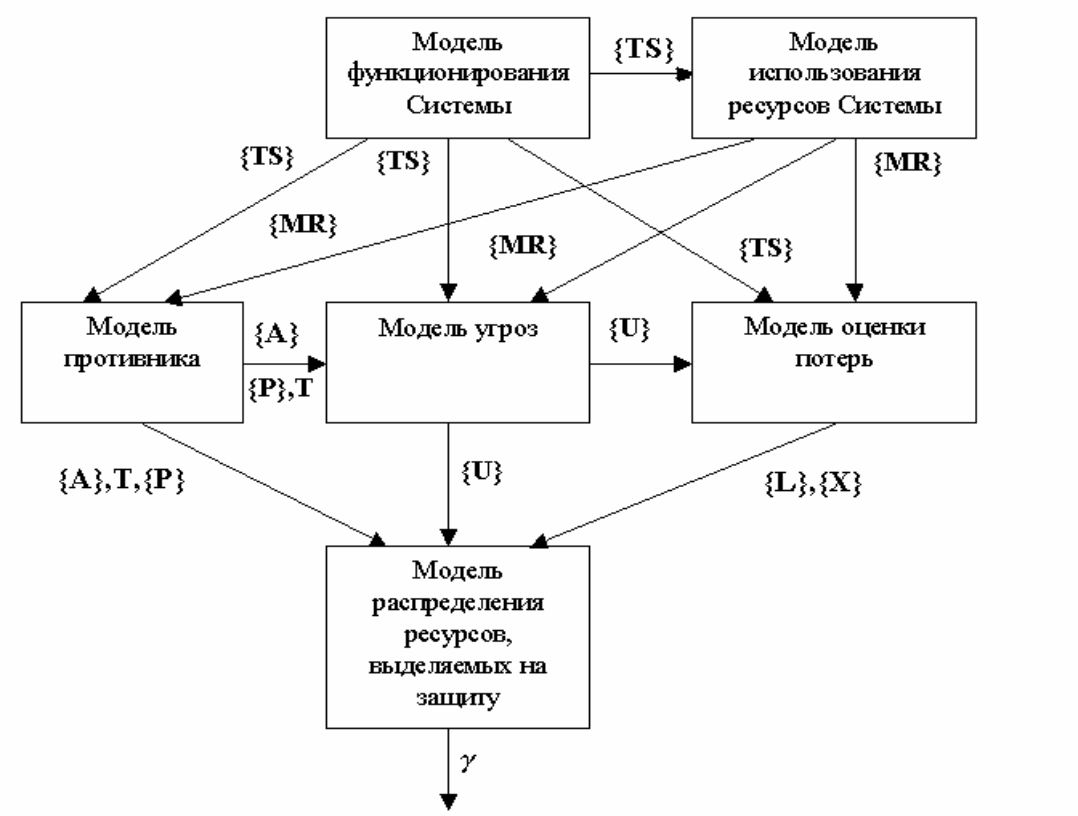

Рис. 1. Общая модель процесса формирования эффективной КСЗИ АС

В статье [7] предлагалось для формирования эффективной КСЗИ АС воспользоваться следующей методикой: минимизировать $f(\gamma)=\sum_{i=1}^{N} L_i(R_i - \sum_{j=1}^{M} GM_{ij}\cdot\gamma_j)$ при ограничении $\sum_{j=1}^{M}\gamma_j\cdot(C_j + X_j)\le C_d$, где N – число угроз информации; L – оценка стоимости потерь в случае реализации каждой из угроз; R – максимальные возможности атакующей стороны по реализации угроз; M – число существующих средств защиты; G – набор показателей эффективности средств защиты информации; γ – вектор применения средств защиты информации защищающейся стороной (γ_i=0, если i-ое средство защиты информации не используется; в противном случае коэффициент равен 1); C_d – финансовые средства, которые могут выделены защищающейся стороной для осуществления защиты информации; X_j – потери, связанные со снижением производительности АС, в случае использования средства защиты информации.

Отметим недостатки существующих методов формирования КСЗИ АС:

1) Потери, связанные со снижением производительности АС, вызванные использованием средств ЗИ (значение X_j), зависят от значений вектора γ. Таким образом, значение C_d также зависит от значений вектора γ и может быть получено после проведения специальных вычислений.

2) Методика, описанная в [4, 7], не позволяет учесть особенности использования механизмов ЗИ в технологической схеме АС, особенностей противодействия распределенной атаки и т.п.

Постановка и решение задачи 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.

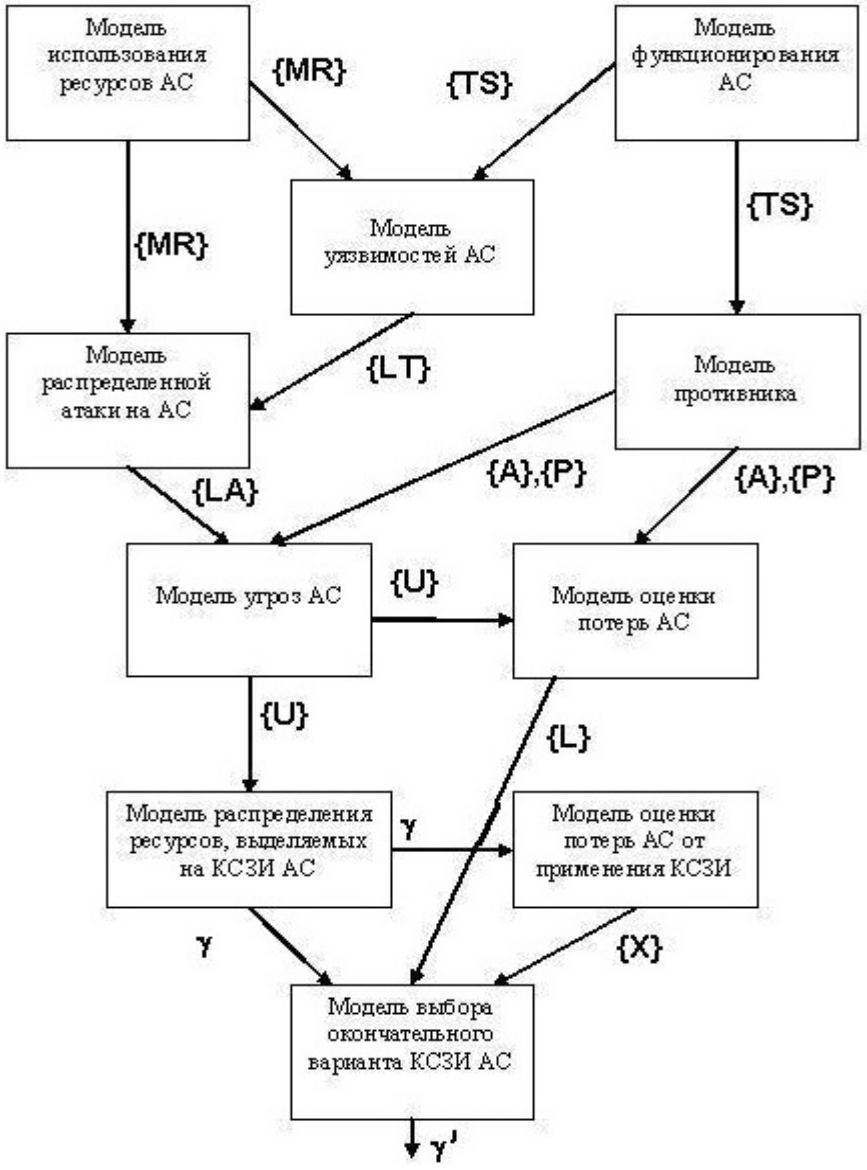

Рис. 2. Новая общая модель процесса формирования эффективной КСЗИ АС

В отличие от методики, описанной в [4, 7], предлагается внести такие дополнения к общей модели формирования эффективной КСЗИ АС (рис. 2).

– В модели оценки потерь АС получать только значения вектора L (оценка стоимости потерь в случае реализации каждой из угроз), значения вектора C_d получать после вычисления значений вектора γ (вектор применения средств защиты информации защищающейся стороной).

– Окончательный выбор состава КСЗИ АС необходимо производить на заключительном этапе, после получения значений векторов C_d и γ, исходя из задач ЗИ в АС (минимизации остаточного риска или уменьшения затрат на КСЗИ АС).

В предложенной новой модели (рис. 2) используются следующие обозначения (см. также рис. 1): {LA} – множество возможных распределенных атак на АС; {LT} – множество уязвимостей компонентов АС; γ – вариант построения КСЗИ АС; $\gamma^{|}$ – окончательный вариант построения КСЗИ АС.

Исходя из вышеизложенного, ***улучшенный способ формирования эффективной КСЗИ АС*** 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. 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 – операционных систем, систем управления базами данных, прикладного и специализированного программного обеспечения.

3. Для каждой из полученных трасс рассмотреть варианты несанкционированного чтения, создания, 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*.

6. Сформировать граф распределенной атаки на ресурсы АС. Для этого получить множество условий для реализации атак *{NL}* и множество действий нарушителя политики безопасности *{AP}*. На рис. 3 приведены правила формирования указанного графа.

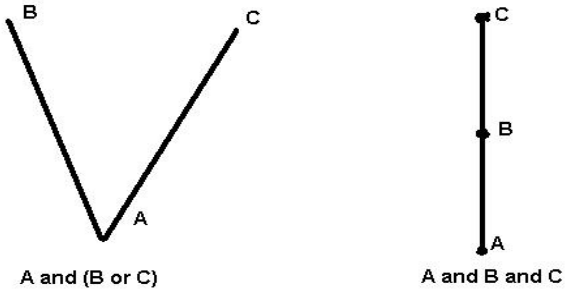

Рис. 3. Правила формирования графа распределенной атаки на АС

7. Используя методы теории графов, найти остов графа, полученного в пункте 6. В теории графов разрезом называется множество ребер, удаление которых делит граф на два или более изолированных подграфа. Используя методы теории графов, получить множество разрезов графа *{RZ}*.

8. Все найденные в пункте 7 разрезы графа распределенной атаки на АС занести в таблицу вида $< RZ(i) >< \{NL\} >< \{\gamma_i\} >$, где:

{RZ(i)} – множество разрезов графа распределенной атаки;

{NL} – множество необходимых условий – вершин графа распределенной атаки на АС;

γ_i – вектор механизмов защиты информации в составе КСЗИ АС, для обеспечения разреза *RZ(i)* графа распределенной атаки. Представляет собой бинарный вектор длиною *M*. Элемент указанного бинарного вектора γ_{ij} равен 1, если механизм G_{ij} задействован в составе КСЗИ АС, в противном случае γ_{ij} равен нулю.

9. Для каждого из полученного в пункте 7 разрезов графа бинарных векторов γ необходимо вычислить размер остаточного риска (1):

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

10. Для каждого из полученного в пункте 7 разрезов графа бинарных векторов γ необходимо вычислить размер средств, выделяемых на обеспечение ЗИ в АС (2):

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

11. В результате будет сформирована таблица, в которой первый столбец – вектор *RZ(i)*, второй – размер остаточного риска при использовании варианта (*R*), третий – размер затрат на построение КСЗИ (C_{d}).

Методика вычисления величин G_{ij} приведена в [4], методики получения величин C_{j}, L_i, P_i – в [6]. Методика получения величины X_j будет описана в следующем разделе статьи.

Предлагаемый способ формирования эффективной КСЗИ АС позволяет найти решение, оптимальное или рациональное в среднем. При формировании КСЗИ АС, обрабатывающих информацию, которая составляет государственную, военную или коммерческую тайну могут быть использованы различные критерии:

– для обеспечения эффективной защиты может быть выбран вариант с наименьшим остаточным риском;

– для минимизации расходов на формирование КСЗИ АС может быть выбран вариант с наименьшим значением C_{d}, у которого значение остаточного риска является наименьшим из рассматриваемых.

Методика выбора варианта построения эффективной КСЗИ АС. Порядок разработки КСЗИ АС описан в [3], вопросы построения эффективной КСЗИ АС рассматривались автором в [2, 4, 7]. В качестве математического аппарата для построения новой модели будет использована математическая теория игр. Из теории игр известен способ обеспечить гарантированную границу своего проигрыша, хуже которого быть не должно [8].

Новая методика предполагает следующий подход: должны быть рассмотрены все без исключения варианты использования существующих механизмов ЗИ в составе КСЗИ АС. При этом каждый вариант применения 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. Для каждого из бинарных векторов γ необходимо вычислить размер остаточного риска согласно формуле (1) и размер средств, выделяемых на обеспечение ЗИ в АС, согласно формуле (2).

В табл. 1 приведено описание переменных, используемых в модели КСЗИ АС.

Параметры переменных, используемых в модели формирования КСЗИ АС Табл.1

Обозначения переменных	Значения переменных	Ограничения переменных	Размерности переменных
R	Размер остаточного риска	$R_i > 0$	гривны
N	Число угроз информации	$N > 0$	–
L_i	Стоимости потерь при реализации *i*-ой угрозы	$L_i > 0$	гривны
P_i	Вероятность реализации *i*-ой угрозы	$0 \le P_i \le 1$	–
M	Число существующих средств защиты	$M > 0$	–
G_{ij}	Эффективность *j*-го механизма ЗИ по нейтрализации *i*-ой угрозы	$0 \le G_{ij} \le 1$	–
γ_{i}	Признак использования *i*-го механизма ЗИ в составе КСЗИ АС (равен 1, если механизм задействован в составе КСЗИ, иначе – 0)	$\gamma_{\text{i}} \in (0;1)$	–
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 ЗИ	$C_{\text{j}} > 0$	гривны
X_j	Размер потерь АС, вызванных использованием *j*-го механизма ЗИ в составе КСЗИ АС	$X_j > 0$	гривны

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 [8]. Ходами в игре выступают варианты использования существующих механизмов ЗИ в АС (варианты вектора γ_i).

Как отмечается в [8], теория игр позволяет найти решение, оптимальное или рациональное в среднем. При формировании КСЗИ АС, обрабатывающих информацию, которая составляет государственную, военную или коммерческую тайну могут быть использованы различные критерии:

– для обеспечения эффективной защиты может быть выбран вариант, с наименьшим остаточным риском;

– для минимизации расходов на формирование КСЗИ АС может быть выбран вариант с наименьшим значением C_{d}, у которого значением остаточного риска является наименьшим из рассматриваемых.

Методика вычисления потерь, связанных с применением механизмов защиты. Указанные потери зависят от двух обстоятельств.

Во-первых, любое, даже самое совершенное средство защиты информации (будь то шифратор, средство разграничения доступа или средство сокрытия данных) для выполнения своих задач расходует ресурсы защищаемой системы. В частности, любая операция, выполняемая средствами защиты информации, требует некоторого времени.

Во-вторых, следует учесть, что любое средство защиты информации должно отвечать ряду требований по эргономике. Связано это с удобством эксплуатации указанного средства обслуживающим персоналом. В случае отсутствия документации на средство защиты информации в должном объеме (а также сложности его обслуживания), обслуживающий персонал будет расходовать свое рабочее время на “самоподдержку” и “взаимоподдержку” [9, 10]. Под этими терминами будем понимать расход рабочего времени персоналом для выяснения вопросов эксплуатации средств защиты информации.

Исходя из вышеизложенного, потери от снижения производительности АС, связанные с использованием средств защиты данных, могут быть рассчитаны следующим образом:

$L_{зи} = D \cdot \sum_{i=1}^{N} \frac{t_{сз_i} + t_{сп_i}}{t_{сз_i} + t_{сп_i} + t_{оп_i}}$, где D – годовой доход от использования АС; N – количество узлов АС; $t_{сз_i}$ – время, расходуемое средствами защиты информации для выполнения своих функций на і-м узле АС; $t_{сп_i}$ – время, расходуемое персоналом *i*-го узла АС на “самоподдержку” и “взаимоподдержку”; $t_{оп_i}$ – время, необходимое для обработки информации на *i*-ом узле АС (без учета времени, необходимого средствам ЗИ).

Рассмотрим методику вычисления значений $t_{сз}$ и $t_{сп}$. Для получения указанных величин необходимо внести выбранные средства защиты информации в модель функционирования АС. Указанные значения переменных могут быть получены как сумма потерь времени на участках технологических маршрутов АС. Потери времени могут быть рассчитаны по приведенным ниже зависимостям:

Для линейного участка: $t_{сз} = \sum_{i=1}^{N} t_{сзи_i}$ (N – число средств ЗИ на участке; $t_{сзи_i}$ – время, расходуемое *i*-м средством ЗИ на выполнение своих функций); $t_{сп} = \sum_{i=1}^{N} t_{сп_i}$.

Для циклического участка: $t_{сз} = \sum_{j=1}^{K} \sum_{i=1}^{N} t_{сзи_i}$ (K – число циклов); $t_{сп} = \sum_{j=1}^{K} \sum_{i=1}^{N} t_{сп_i}$.

Для участка ветвления значения $t_{сз}$ и $t_{сп}$ могут быть получены как максимальные значения из числа возможных альтернатив.

Выводы из исследования и перспективы дальнейших разработок. Предложенная методика формирования КСЗИ АС имеет следующие преимущества:

– учитываются принципы организации распределенных атак на АС;

– при создании КСЗИ АС можно определить значение величины C_{d};

– применение предлагаемой методики при модификации существующей КСЗИ АС наглядно демонстрирует возможные затраты на защиту информации (ΔC_{d}) и ожидаемые результаты применения новых механизмов защиты информации (ΔR);

– модифицированный способ формирования КСЗИ АС обладает меньшей вычислительной сложностью, чем по способу, основанному на методах нелинейного программирования [6].

В перспективе представляется рациональным использовать методы математической теории игр для описания процесса ЗИ как процесса бесконечной антагонистической игры с неполной информацией. При этом могут быть рассмотрены различные стратегии игроков, в зависимости от их возможностей, особенностей функционирования АС, а также возможностей игроков.

Литература

1. Арзуманов С. В. Оценка эффективности инвестиций в информационную безопасность / С. В. Арзуманов // Защита информации. INSIDE. – 2005. – №1. – С. 23-25.

2. Гроздов Г. Г. Новый способ оценки величины остаточного риска при формировании экономически эффективной комплексной системы защиты информации в автоматизированных системах / Г. Г. Гроздов // Радиоэлектроника. Информатика. Управление. – 2006. – № 2. – С. 109-115.

3. Герасименко В. А. Защита информации в автоматизированных средствах обработки данных. Книги 1, 2 / В. А. Герасименко. – М. : Энергоатомиздат, 1994. – 400 с. и 176 с.

4. Гроздов Г. Г. Модифицированный способ решения задачи формирования эффективной комплексной системы защиты информации автоматизированной системы / Г. Г. Гроздов; монография. – К.: ДУІКТ, 2009. – 32 с.

5. Петренко С. А. Обоснование инвестиций в безопасность / С. А. Петренко, Е. М. Терехова // Защита информации. INSIDE. – 2005. – №1. – С. 49-53.

6. Петренко С. А. Оценка затрат на защиту информации / С. А. Петренко, Е. М. Терехова // Защита информации. INSIDE. – 2005. – №1. – С. 36-47.

7. Гроздов Г. Г. Способ решения задачи формирования комплексной системы защиты информации для автоматизированных систем 1 и 2 класса / Г. Г. Гроздов; препр. – К.: НАН Украины. Отделение гибридных моделирующих и управляющих систем в энергетике ИПМЭ им Г. Е. Пухова. – 2005. – №1. – 66 с.

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

9. Скрипкин К. Г. Экономическая эффективность информационных систем / К. Г. Скрипкин. – М.: ДМК, 2002. – 252 с.

10. Гроздов Г. Г. Новая постановка задачи формирования экономически эффективной комплексной системы защиты информации в автоматизированных системах первого и второго класса / Г. Г. Гроздов // Электроника и системы управления. – 2005. – № 4. – С.88-96.