УДК 681.3:519.872

А.А. Антонюк

О ФУНКЦИЯХ ЗАЩИТЫ ИНФОРМАЦИИ

Рассматривается понятие функции защиты информации. Приводится их классификация и - формальное описание с помощью булевых функций и теории вероятностей. Формулируются некоторые задачи оптимизации, возникающие при построении систем защиты информации.

Введение

Один из подходов к моделированию процессов и систем защиты информации в информационно-телекоммуникационных системах (ИТС) основывается на понятии функции защиты информации [1]. Суть его заключается в том, что процесс работы системы защиты информации (СЗИ) ИТС моделируется путем определения в ней ряда свойств, благодаря которым она некоторым образом реагирует на события, связанные с обеспечением безопасности информации в ИТС, например, оценивание реальной возможности (меры) проявления нарушений безопасности информации, обнаружение фактов их проявления, принятие мер к предотвращению их воздействия на защищаемую информацию, обнаружение, локализация и ликвидация последствий воздействий на защищаемую информацию и др. Каждому из них ставится в соответствие определенное свойство СЗИ ИТС, называемое функцией защиты информации, которое заключается в конкретных действиях СЗИ относительно некоторого события. Методы реализации этих функций (организационные, программные, аппаратные и др.) для данного рассмотрения не имеют значения.

В рамках такого подхода основную задачу теории и практики защиты информации в любой ИТС можно понимать как формирование и обоснование полного множества функций защиты S [1], которое должно характеризоваться очевидным свойством: S должно содержать такие функции, при реализации которых СЗИ ИТС могла оказывать воздействие на все потенциально возможные нарушения безопасности информации в процессе функционирования ИТС, а также при организации и обеспечении защиты информации.

В [1] установлено, что множество S является объединением $S = S_a \bigcup S_c$: 1) множества функций обеспечения защиты S_a, осуществлением которых создаются условия, необходимые для надежной защиты информации; 2) множества функций управления механизмами защиты S_c, осуществляемых с целью эффективного использования механизмов защиты после реализации функций множества S_a. В дальнейшем рассмотрим только множество S_a.

В [1] представлена одна из возможных схем формирования множества функций S_a. Ниже рассматриваются вопросы обоснования, усовершенствования и дальнейшей формализации схемы подобного рода.

1. Структура множества S_a

Нарушения информационной безопасности непосредственно связаны с угрозами информации. По существу, это реализация угроз информации. В [2-5] угрозы информации определяются следующими ее свойствами: конфиденциальность, целостность, доступность и наблюдаемость. Именно по результату воздействия на эти свойства, вводятся и различаются следующие классы угроз информации, т.е. нарушения:

ISSN 1727-4907. Проблеми програмування. 2005. № 3

- конфиденциальности;
- целостности (логической или физической);
- доступности (или отказ в обслуживании);
- наблюдаемости или управляемости.

К перечисленным выше необходимо добавить еще угрозу несанкционированного использования информационных ресурсов.

Однако определенные таким образом угрозы представляют собой лишь некоторые абстрактные и весьма общие нежелательные воздействия на информацию. Вследствие этого удобным оказывается понятие дестабилизирующего фактора (ДФ) как конкретной причины возникновения угрозы информации. Как определено в [1,6], ДФ – это такие явления или события, которые могут появляться на любом этапе жизненного цикла (ЖЦ) ИТС и следствием которых могут быть угрозы информации и/или нанесение ущерба компонентам ИТС. Таким образом, нарушения информационной безопасности – это возникновение и реализация ДФ.

Следовательно, основной задачей функций защиты информации является контроль над всеми возможными проявлениями ДФ. В любой ИТС всегда можно определить такие условия, при которых могут (хотя бы в принципе) проявиться какие-либо ДФ. Если их не будет, то не будет необходимости в защите, если же проявление ДФ все-таки потенциально возможно, то надо уметь оценивать реальную возможность (меру) их проявления, обнаруживать факты их проявления, принимать меры к предотвращению их воздействия на информацию, к обнаружению, локализации и ликвидации последствий. Именно этими свойствами и должны обладать функции обеспечения защиты S_a.

С учетом анализа и классификации ДФ [6], а также основных задач функций защиты множество S_a будет выглядеть следующим образом:

1. S_{a1} – создание и контроль условий, ограничивающих возможности проявления ДФ. В соответствии с приведенными причинами возникновения ДФ возможность создания таких условий может быть реализована еще на этапах проектирования ИТС при помощи выбора соответствующей архитектуры ИТС, технологических схем обработки информации, модели безопасности, политики безопасности, внедрения механизмов безопасности и т.д., т.е. условий, исключающих даже потенциальную возможность проявления ДФ.

2. S_{a2} – предупреждение возникновения условий, способствующих проявлению ДФ. Эта функция реализуется подобно предыдущей и обе они преследует упреждающую цель.

3. S_{a3} – предупреждение непосредственного проявления ДФ в конкретных условиях функционирования ИТС. Эта функция также преследует упреждающую цель, но применительно к конкретным условиям и для ДФ, которые уже потенциально могут иметь место на различных этапах ЖЦ ИТС.

4. S_{a4} – обнаружение проявившихся ДФ и контроль над ними. Здесь предполагается осуществление таких мероприятий, в результате которых проявившиеся ДФ (или реальная угроза их проявления) будут обнаружены еще до того, как они окажут воздействие на защищаемую информацию. Эта функция фактически представляет собой слежение за потенциальными ДФ.

5. S_{a5} – предупреждение воздействия ДФ на информацию. Ее содержание – не допустить нежелательного воздействия ДФ на информацию даже в том случае, если они реально проявились (здесь это продолжение предыдущей функции). Однако осуществление предыдущей функции может быть как успешным (проявление ДФ обнаружено), так и неуспешным (проявление ДФ не - обнаружено), а воздействие все-таки воз-

можно. Поэтому задачей этой функции является предупреждение воздействия на информацию проявившихся и обнаруженных ДФ.

6. S_{a6} – предупреждение воздействия ДФ на информацию с целью не допустить нежелательного воздействия ДФ на информацию даже в том случае, если они реально проявились (продолжение предыдущего пункта). Однако здесь функция имеет задачу предупреждения воздействия на информацию проявившихся, но не обнаруженных ДФ.

7. S_{a7} – обнаружение и контроль воздействия ДФ на защищаемую информацию. В отличие от функции S_{a3} осуществляется слежение не только за потенциально возможными ДФ, но и за самой защищаемой информацией.

8. S_{a8} – локализация воздействия ДФ на информацию, т.е. недопущение распространения воздействия на информацию за пределы максимально допустимых установленных в ИТС размеров. При этом основная задача – локализация проявившегося и обнаруженного воздействия ДФ на информацию.

9. S_{a9} – локализация воздействия ДФ на информацию, т.е. недопущение распространения воздействия на информацию за пределы максимально допустимых установленных в ИТС размеров. Однако здесь выделяется задача локализации проявившегося, но не обнаруженного воздействия ДФ на информацию.

10. S_{a10} – ликвидация последствий воздействия ДФ на защищаемую информацию. Под ликвидацией понимается проведение таких мероприятий относительно локализованного воздействия ДФ на информацию, в результате которых дальнейшая обработка информации может осуществляться без учета имевшего место воздействия. Иными словами, нужно восстановить то состояние информации, которое имело место до воздействия ДФ. Ясно, что для ликвидации последствий в случае локализации обнаруженных и необнаруженных воздействий необходимы совершенно различные механизмы защиты. Это означает, что в данном случае целесообразно выделить задачу ликвидации последствий обнаруженного и локализованного воздействия ДФ.

11. S_{a11} – ликвидация последствий воздействия ДФ на защищаемую информацию, но здесь выделяется задача ликвидации последствий локализованного, но не идентифицированного воздействия ДФ на информацию.

Для множества S_a отметим следующие характерные особенности:

- S_a является исчерпывающим и полным в том смысле, что включает все возможные действия по обеспечению защиты информации в ИТС;
- ни одну из функций множества S_a нельзя исключить из данного множества;
- S_a должно поддерживаться в любых ИТС, на всех этапах их ЖЦ и в любых условиях их функционирования.

Иначе говоря, реализация множества функций обеспечения защиты информации S_a в ИТС является необходимым условием надежной защиты информации. Это означает, что уровень защищенности ИТС полностью определяется набором конкретных мероприятий, необходимых для поддержки всех функций S_a, каждое из которых имеет свой уровень и полноту реализации.

Теперь рассмотрим возможные итоговые состояния СЗИ, к которым может приводить выполнение или невыполнение каждой из перечисленных функций. Независимо от перечисленных возможностей функций обеспечения защиты S_a для любой СЗИ в любой ИТС

может возникать только следующее множество различных итоговых состояний (событий) A:

1. A_1 – СЗИ полностью выполняет свои задачи, т.е. даже при условии проявления каких-либо ДФ предотвращается их негативное воздействие на защищаемую информацию или полностью ликвидируются последствия такого воздействия.

2. A_2 – СЗИ не полностью выполняет свои задачи, т.е. не удается полностью предотвратить негативное воздействие ДФ на информацию, однако это воздействие локализовано.

3. A_3 – СЗИ не выполняет ни одной из своих задач, т.е. СЗИ нарушена полностью, в результате чего негативное воздействие ДФ на информацию не только не предотвращено, но даже не локализовано.

Очевидно, что организация защиты информации в ИТС заключается в достижении первого события A_1 и/или хотя бы частично второго A_2.

2. Формальное описание функций защиты

Для дальнейшего анализа перечисленные функции защиты из множества S_a и итоговые события (множество A) удобно представить в виде графа (рисунок), в котором приведены все возможные их сочетания. В графе номерами функций защиты отмечены его вершины, дуги описываются булевыми переменными и фиксируют факты выполнения или невыполнения функций защиты, а исходы определяются как конечные вершины – некоторые булевы функции.

Пользуясь графом, легко получить явные выражения для булевых функций:

$$F_1 = x_1;$$

$$F_2 = \bar{x}_1 \wedge x_2;$$

$$F_3 = \bar{x}_1 \wedge \bar{x}_2 \wedge x_3;$$

$$F_4 = \bar{x}_1 \wedge \bar{x}_2 \wedge \bar{x}_3 \wedge x_4 \wedge x_5;$$

$$F_5 = \bar{x}_1 \wedge \bar{x}_2 \wedge \bar{x}_3 \wedge (x_4 \wedge \bar{x}_5 \vee \bar{x}_4 \wedge \wedge \bar{x}_6) \wedge x_7 \wedge x_8 \wedge x_{10};$$

$$F_6 = \bar{x}_1 \wedge \bar{x}_2 \wedge \bar{x}_3 \wedge (x_4 \wedge \bar{x}_5 \vee \bar{x}_4 \wedge \wedge \bar{x}_6) \wedge \bar{x}_7 \wedge x_9 \wedge x_{11};$$

$$F_7 = \bar{x}_1 \wedge \bar{x}_2 \wedge \bar{x}_3 \wedge \bar{x}_4 \wedge x_6;$$

$$F_8 = \bar{x}_1 \wedge \bar{x}_2 \wedge \bar{x}_3 \wedge (x_4 \wedge \bar{x}_5 \vee \bar{x}_4 \wedge \wedge \bar{x}_6) \wedge x_7 \wedge x_8 \wedge \bar{x}_{10};$$

$$F_9 = \bar{x}_1 \wedge \bar{x}_2 \wedge \bar{x}_3 \wedge (x_4 \wedge \bar{x}_5 \vee \bar{x}_4 \wedge \wedge \bar{x}_6) \wedge \bar{x}_7 \wedge x_9 \wedge \bar{x}_{11};$$

$$F_{10} = \bar{x}_1 \wedge \bar{x}_2 \wedge \bar{x}_3 \wedge (x_4 \wedge \bar{x}_5 \vee \bar{x}_4 \wedge \wedge \bar{x}_6) \wedge x_7 \wedge \bar{x}_8;$$

$$F_{11} = \bar{x}_1 \wedge \bar{x}_2 \wedge \bar{x}_3 \wedge (x_4 \wedge \bar{x}_5 \vee \bar{x}_4 \wedge \wedge \bar{x}_6) \wedge \bar{x}_7 \wedge \bar{x}_9.$$

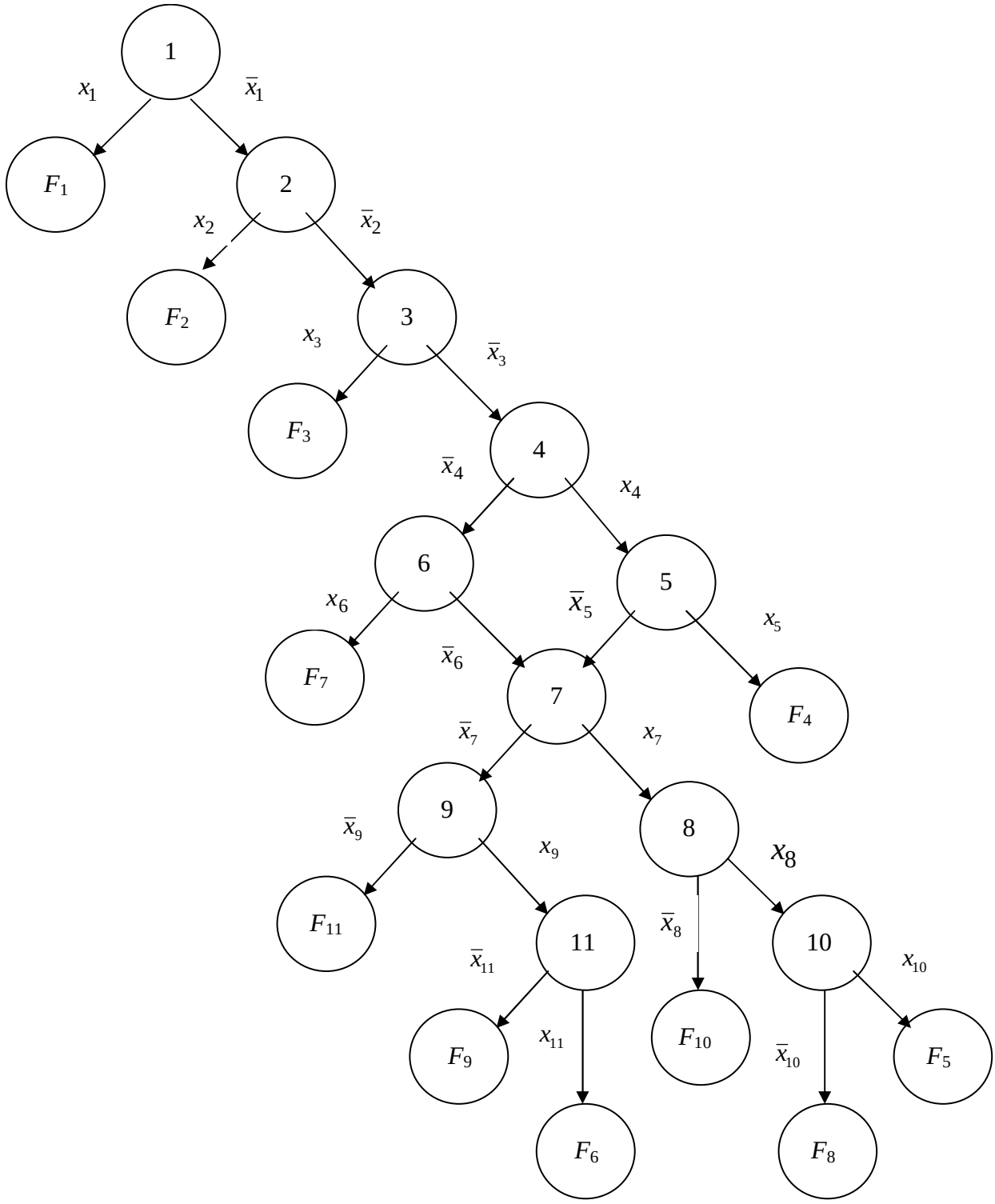
Таким образом, каждой из функций защиты $S_{ai} \in S_a$, i=1,…,11 поставлена в соответствие некоторая булева функция. Нетрудно также убедиться, что каждый из одиннадцати отмеченных исходов является случайным событием, причем эти события в основном независимы и все они составляют полную группу несовместных событий. Поэтому сумма их вероятностей должна равняться 1:

$$\sum_{i=1}^{11} P_i = 1,$$

где P_i – вероятность i-го исхода.

В действительности перечисленные события не являются в полной мере независимыми, однако в большинстве случаев в первом приближении предположение их независимости является вполне удовлетворительным. Более детальный учет этого обстоятельства требует дополнительного исследования.

Из 11 возможных исходов лишь исходы 1-7 приводят итоговому событию $A_1 \in A$; исходы 8 и 9 – к итоговому событию $A_2 \in A$; исходы 10 и 11 – к ито-



говому событию $A_3 \in A$. Для защиты информации благоприятными как раз являются исходы 1-7 (и частично 8-9), поэтому сумма их вероятностей будет не чем иным как вероятностью того, что защищенность информации будет полностью (или частично, если учитывать исходы 8-9) обеспечена. Для случая полного обеспечения защищенности это

$$P_s = \sum_{i=1}^{7} P_i \,. \qquad (1)$$

Вероятности благоприятных исходов можно выразить через вероятности успешной реализации отдельных функций защиты, определение которых является существенно более простой задачей. Это можно сделать, применяя к полученным ранее булевым функциям логико-ве-

роятностный подход [7], поскольку они удовлетворяют всем необходимым для этого условиям. Поэтому, обозначая вероятности успешной реализации функций защиты $P_{fi}, i=1,...,11$, для вероятностей благоприятных исходов получим следующие формулы:

$$P_1 = P_{f1};$$

$$P_2 = (1-P_{f1})P_{f2};$$

$$P_3 = (1-P_{f1})(1-P_{f2})P_{f3};$$

$$P_4 = (1-P_{f1})(1-P_{f2})(1-P_{f3})P_{f4}P_{f5};$$

$$P_5 = (1-P_{f1})(1-P_{f2})(1-P_{f3})\times$$
$$\times(P_{f4}(1-P_{f5})+(1-P_{f4})\times$$
$$\times(1-P_{f6}))P_{f7}P_{f8}P_{f10};$$

$$P_6 = (1-P_{f1})(1-P_{f2})(1-P_{f3})\times$$
$$\times(P_{f4}(1-P_{f5})+(1-P_{f4})\times$$
$$\times(1-P_{f6}))(1-P_{f7})P_{f9}P_{f11};$$

$$P_7 = (1-P_{f1})(1-P_{f2})(1-P_{f3})\times$$
$$\times(1-P_{f4})P_{f6}.$$

Для случая частичного обеспечения защищенности информации следует учесть исходы 8 и 9, т.е. получится соотношение

$$P_s = \sum_{i=1}^{9} P_i, \qquad (2)$$

в котором использованы две соответствующие формулы для вероятностей:

$$P_8 = (1-P_{f1})(1-P_{f2})(1-P_{f3})\times$$
$$\times(P_{f4}(1-P_{f5})+(1-P_{f4})\times$$
$$\times(1-P_{f6}))P_{f7}P_{f8}(1-P_{f10}),$$

$$P_9 = (1-P_{f1})(1-P_{f2})(1-P_{f3})\times$$
$$\times(P_{f4}(1-P_{f5})+(1-P_{f4})\times$$
$$\times(1-P_{f6}))(1-P_{f7})P_{f9}(1-P_{f11}).$$

В обоих случаях для сумм вероятностей (1) и (2) подстановкой в них формул для вероятностей получается общая символическая зависимость

$$P_s = F(P_{f1},..., P_{f11}),$$

из которой видно, что защищенность информации в ИТС полностью определяется вероятностями реализации перечисленных функций защиты, характеризуемыми набором конкретных практических мероприятий по реализации функций защиты и/или уровнем их реализации. Поэтому можно ставить задачу [1] обеспечения определенного уровня защищенности $\overline{P}_s$ путем выбора такой совокупности мероприятий для осуществления каждой из функций защиты S_a, при которых

$$F(P_{f1},..., P_{f11}) \ge \overline{P}_s.$$

Кроме того, становится возможным сформулировать следующую задачу оптимизации СЗИ. Реализация каждой из функций защиты S_a всегда связана с определенными затратами на них, и, естественно, уровень реализации каждой из них будет зависеть от величины этих затрат. Поэтому, если количество затрат (в некоторых условных единицах) на реализацию *i*-й функции обозначить C_i, то $P_{fi} = f_i(C_i)$ и

$$P_s = F(f_1(C_1),...,f_{11}(C_{11})) = G(C_1,...,C_{11}) \qquad (3)$$

Тогда задача оптимизации формулируется следующим образом: минимизировать затраты на защиту, обеспечив ее уровень не ниже заданного:

$$\begin{cases} \min \sum_{i=1}^{11} \alpha_i C_i, \\ G(C_1,..., C_{11}) \ge \overline{P}_s. \end{cases}$$

где α_i – некоторые весовые коэффициенты, значения которых устанавливаются заранее (например, путем экспертных оценок).

Легко также сформулировать задачу максимизации уровня защищенно-

сти при ограничении на затраты сверху. Очевидна практическая важность и ценность таких оптимизационных задач, однако использование их на практике наталкивается на исключительно сложную проблему определения функциональных зависимостей (3). Эти трудности возникают вследствие того, что уровни успешной реализации отдельных функций защиты S_a существенно зависят ряда от других трудно формализуемых факторов (уязвимости, атаки, угрозы, наличия или отсутствия средств защиты, человеческого фактора и др.).

Заключение

Таким образом, описано полное множество функций защиты информации и множества возможных итоговых событий в ИТС. С помощью графа устанавливается взаимосвязь функций защиты и итоговых событий, что позволило получить выражения для вероятностей успешной реализации отдельных функций защиты. В свою очередь, это позволило сформулировать некоторые важные задачи оптимизации СЗИ.

Практическая реализация необходимой совокупности мероприятий для осуществления каждой из функций защиты S_a может осуществляться с помощью наборов функциональных услуг [4-5]. Корректная их реализация и поддержка должны базироваться на соответствующей политике безопасности [3-6].

1. *Герасименко В.А.* Защита информации в автоматизированных системах обработки данных. – М.: Энергоатомиздат, 1994, в 2-х т. – Т.1. – 288 с.; Т.2. – 144 с.
2. *Загальні* положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1–002–99. – Київ: ДСТСЗІ СБ України, 1999. – 16 с.
3. *Критерії* оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 2.2–004–99. – Київ: ДСТСЗІ СБ України, 1999. – 55 с.
4. *Класифікація* автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу: НД ТЗІ 2.2–005–99. – Київ: ДСТСЗІ СБ України, 1999. – 23 с.
5. *Термінологія* в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1–003–99. – Київ: ДСТСЗІ СБ України, 1999. – 26 с.
6. *Антонюк А.А., Боровская Е.Н., Суслов В.Ю.* Модель угроз инфомации в защищенных автоматизированных системах // Безопасность информации. – 2001. – № 2. – С. 17-22.
7. *Тимошенко А.О.* Логико-вероятностный подход в информационной безопасности // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2001. – №1. – С. 35-37.

Получено 12.04.05

Об авторе

Антонюк Анатолий Александрович
канд. физ.-мат. наук, доцент

Место работы автора:
Национальная академия государственной налоговой службы Украины, г. Ирпень Киевской области, ул. К. Маркса, 31
Тел. (044) 4244147