УДК 681.3:519.872

А.А. Антонюк, В.В. Жора, В.Н. Мостовой

УГРОЗЫ ИНФОРМАЦИИ И УСЛУГИ БЕЗОПАСНОСТИ

Рассматривается классификация угроз информации в соответствии с требованиями национального стандарта по защите информации. Дается их формальное описание, а также формальное описание некоторых услуг по обеспечению безопасности информации. Изучаются необходимые условия гарантированного выполнения дискреционной политики безопасности.

Введение

Понятие угрозы информации является основным в теории и практике защиты информации (ЗИ). Анализ угроз является начальным и одним из основных этапов при разработке системы защиты информации (СЗИ) и проводится на основе модели угроз. Согласно [1 – 4], модель угроз — это абстрактное формализованное или неформализованное описание методов и способов осуществления угроз.

В официальных нормативных документах, регламентирующих основные аспекты, связанные с безопасностью компьютерных систем (КС) и защитой информации в них от несанкционированного доступа (НСД) [1 – 4], даются определения таких фундаментальных свойств защищенной информации (ФСЗИ), как конфиденциальность, целостность, доступность и наблюдаемость. Каждое из указанных свойств обеспечивается КС с помощью набора конкретных функциональных услуг, описание и ранжирование по уровням которых приводится в [2, 5]. Однако формального их описания пока нет, что существенно затрудняет возможности использования математических моделей СЗИ.

Ниже рассмотрено формальное описание основных классов угроз информации и услуг, реализация которых позволяет им противостоять. В отличие от [6], где рассмотрены только простейшие случаи угроз конфиденциальности и целостности, а услуги вообще не описываются, здесь изучаются все классы угроз и услуги в соответствии с [2], где определены 22 функциональные услуги безопасности и 67 их модификаций.

1. Конфиденциальность информации

Анализ развития теории и практики ЗИ показывает, что можно выделить основные пути нарушения конфиденциальности [6, 7]:

- потеря контроля над СЗИ;
- каналы утечки информации.

Другие пути нарушения конфиденциальности так или иначе сводятся к ним.

Если СЗИ перестает адекватно функционировать, то может быть реализован НСД к информации. Это также может стать причиной появления скрытых каналов утечки информации. Под скрытым каналом утечки информации или просто каналом утечки понимается способ получения информации за счет использования путей передачи информации, которые присутствуют в КС, но не управляются и не наблюдаются СЗИ [2]. Каналы утечки характеризуют ситуацию, когда либо проектировщики не смогли предотвратить НСД, либо СЗИ не может рассматривать этот доступ как запрещенный.

Среди каналов утечки выделяют каналы по памяти и времени. Канал по памяти реализуется путем прямой или непрямой записи информации в определенную область памяти одним процессом и прямым или непрямым чтением этой области другим процессом.

В [8] определена структура множества $\boldsymbol{A}$ (в частности, описаны его подмножества $\boldsymbol{A}_1$, $\boldsymbol{A}_2$, и $\boldsymbol{A}_3$) возможных доступов к информации. Если ограничиться только доступами read (r) и write (w), то канал по памяти схемати-

чески изображается так:

$$U_1 \xrightarrow{act} P \xrightarrow{r} O \xleftarrow{w} U_2 .$$

Здесь пользователь U_1 (злоумышленник) активизирует (*act*) процесс P, который может получить доступ на чтение к объекту, содержащему конфиденциальную информацию, полученную от пользователя U_2. Защита против утечки информации по этому каналу базируется на выборе правильной политики безопасности (ПБ) [1], а также на возможности контроля информационных потоков и вывода информации.

Канал утечки по времени — это канал, позволяющий передавать информацию от одного процесса к другому путем модуляции первым процессом определенных временных характеристик КС, которые могут наблюдаться другим процессом. Схема канала по времени выглядит следующим образом:

$$U_1 \xrightarrow{act} P_1 \xrightarrow{r} P_{\text{mod}} \xleftarrow{act} P_2 \xleftarrow{act} U_2 .$$

В данном случае пользователь U_2 активизирует процесс P_2, информация о котором является конфиденциальной. Далее эта информация модулирует процесс P_{mod}, к которому имеет доступ на чтение процесс P_1, активизированный злоумышленником U_1. Отличие данного канала утечки от канала по памяти состоит в том, что злоумышленник получает не саму конфиденциальную информацию, а данные о выполнении над ней тех или иных операций. Как правило, он используется с целью дальнейшего получения информации уже с помощью канала по памяти.

В общем случае каналами утечки в КС можно считать неблагоприятные доступы $a_k \in \boldsymbol{A}$, $k = 1, \ldots, K$ следующего вида [6–8]:

$$U_i \xrightarrow{a_k} *O, \quad U_j \xrightarrow{a_l} *O, \quad i \neq j, k \neq l .$$

Будем также считать, что если $O \in \boldsymbol{R}_t$, где $\boldsymbol{R}_t = \bigcup_i D_t(U_i)$, а $D_t(U_i) = \{O_j \mid U_i \xrightarrow{a} *O_j, a \in \boldsymbol{A}, t \in \boldsymbol{N}_0\}$, то при $\forall a \in \boldsymbol{A}$ никакие доступы не могут создать канал утечки информации.

Согласно структуре множества доступов в КС, определенной в [6], можно записать выражение для канала утечки или, другими словами, угрозы конфиденциальности:

$$\exists t \in \boldsymbol{N}_0, \exists a \in \boldsymbol{A}_1, \exists U_i \in \boldsymbol{U}_t, \exists O \in \boldsymbol{O}_t,$$

$$U_i \xrightarrow{a} *O,\ O \in O_t(U_j),\ i \neq j;\ i, j = 1, \ldots, n_U.$$

Содержательный смысл его состоит в том, что в определенный момент времени существует некоторый неблагоприятный вид доступа одного пользователя к объекту, созданному другим пользователем, что, очевидно, является каналом утечки информации.

С целью противодействия угрозам конфиденциальности в КС вводится ряд услуг [2]:

• *доверительная конфиденциальность* — такое управление доступом, при котором средства защиты позволяют обычным пользователям управлять (передают управление) потоками информации между другими пользователями и объектами своего домена (например, на основании права собственности объекта), т.е. назначение и передача полномочий не требуют административного вмешательства; в рамках рассматриваемого формализма доверительная конфиденциальность может быть выражена следующим образом:

$$U_2 \xrightarrow{a} *O,\ a \in \boldsymbol{A}_1 \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} O \in O_t(U_2), \\ O \in O_{t-k}(U_1),\ (U_1 \xrightarrow{a} *O, a \in \\ \in \boldsymbol{A}_2) \Rightarrow O \in D_t(U_2), t, k \in \boldsymbol{N}_0; \end{cases} \qquad (1.1)$$

• *административная конфиденциальность* — управление, при котором средства защиты позволяют управлять потоками информации между пользователями и объектами только специально авторизованным пользователям; формально это запишется так:

$$\exists U \in \boldsymbol{U},\ \forall P, O \in D_t(U, a),$$
$$a \in \boldsymbol{A}_2, \forall t \in \boldsymbol{N}_0 ; \qquad (1.2)$$

• *повторное использование объектов* осуществляется в том случае, если перед предоставлением объекта пользователю или процессу в нем не остается информации, которую он содержал, и отменяются предыдущие права доступа к этому объекту, или, иначе, $\exists O \in \boldsymbol{O}$: если $U_i \xrightarrow{a} *O$ в момент $t \in \boldsymbol{N}_0$, $a \in \boldsymbol{A}$, то $U_j \xrightarrow{a} *O$ в момент $t + k$, $i \neq j$, если $O(t) = O(t + k)$;

• *анализ скрытых каналов* проводится с целью обнаружения и перекрытия существующих потоков информации, которые не контролируются другими услугами; он реализуется с помощью диспетчера доступа (ДД, см. ниже);

• *конфиденциальность при обмене* позволяет обеспечить безопасность обмена информацией между защищенными объектами в незащищенной среде; данная услуга обеспечивается закрытием информации (с помощью средств криптографии).

2. Целостность информации

Язык описания угроз целостности информации в основном аналогичен языку описания угроз конфиденциальности. Однако между угрозами этим свойствам существует принципиальное различие. Так, для конфиденциальности основная угроза — это незаконное ознакомление с информацией, т.е. нет активного влияния на информацию и для описания такой угрозы достаточно понятия канала утечки. Для целостности же основная угроза — это несанкционированная модификация информации, т.е. наличие активного влияния на информацию со стороны нарушителя. Для описания угроз такого типа удобно вместо канала утечки ввести понятие канала действия на целостность, который формально представим следующим образом:

$$\exists t \in \boldsymbol{N}_0, \exists a \in \boldsymbol{A}_2, \exists U_i \in \boldsymbol{U}_t, \exists O \in \boldsymbol{O}_t,$$
$$U_i \xrightarrow{a} *O,\ O \in O_t(U_j),\ i \neq j;\ i, j = 1, \ldots, n_U.$$

Примером возникновения канала действия на целостность может служить использование программы "троянский конь". Такая программа, кроме документированных функций, может выполнять скрытые действия в интересах ее разработчика (злоумышленника). Как правило, "троянский конь" используется для модификации защищенной информации.

Среди механизмов защиты от нарушения целостности выделяют следующие: своевременное резервное копирование ценной информации; введение избыточности в саму информацию, т.е. использование помехоустойчивого кодирования информации, что позволяет контролировать ее целостность; введение избыточности в процесс обработки информации, т.е. применение аутентификации, которая позволяет контролировать целостность объектов; введение системной избыточности, т.е. повышение "живучести" системы.

Услуги, с помощью которых обеспечивается целостность, следующие:

• *доверительная целостность* аналогична доверительной конфиденциальности:

$$U_2 \xrightarrow{a} *O,\ a \in \boldsymbol{A}_2 \Leftrightarrow$$
$$\Leftrightarrow \begin{cases} O \in O_t(U_2), \\ O \in O_{t-k}(U_1),\ (U_1 \xrightarrow{a} *O, a \in \\ \in \boldsymbol{A}_2) \Rightarrow O \in D_t(U_2), t, k \in \boldsymbol{N}_0; \end{cases} \quad (2.1)$$

• *административная целостность* аналогична административной конфиденциальности, записывается так же, как (1.2);

• *откат* позволяет восстанавливаться после ошибок пользователя, сбоев программного обеспечения и аппаратуры, поддерживать целостность баз данных, приложений, построенных на транзакциях, и т.д.; обеспечивает возможность отмены операции или последовательности операций и позволяет вернуть защищенный объект в предыдущее состояние: если в момент $t \in \boldsymbol{N}_0$ $P_i \xrightarrow{a_1} O$, $a_1 \in \boldsymbol{A}_2$, то $\exists P_j \in \boldsymbol{P}$, $i \neq j$, $P_j \xrightarrow{a_2} O$, $a_2 \in \boldsymbol{A}_2$, в момент $t + 1$ такой, что $O(t + 1) = O(t)$;

• *целостность при обмене* позволяет защитить объекты от несанкционированной модификации информации, содержащейся в них, во время их экспорта/импорта в незащищенной среде, обеспечивается закрытием информации.

3. Доступность информации

В большинстве случаев доступность информации в КС определяется работоспособностью самой КС, т.е. отсутствие таковой следует считать основной угрозой. Можно выделить следующие направления повседневной деятельности в КС для поддержки ее работоспособности: поддержка пользователей; поддержка программного обеспечения; конфигурационное управление; резервное копирование; управление носителями, обеспечивающее физическую их защиту; документирование; регламентные работы.

Поскольку результатом действия любой угрозы доступности является отсутствие доступности или каналов доступа, то формально это представляется следующим образом:

$$\exists t \in \boldsymbol{N}_0,\ \overline{\exists} a_k \in \boldsymbol{A}_1 \cup \boldsymbol{A}_2,\ \exists U_i \in \boldsymbol{U}_t,\ \exists O \in \boldsymbol{O}_t,$$
$$U_i \xrightarrow{a_k} {}^*O,\ O \in O_t(U_i),$$

а также

$$\exists t \in \mathbf{N}_0,\ (\overline{\exists} a \in \boldsymbol{A}_1) \vee (\overline{\exists} a \in \boldsymbol{A}_2),\ \exists U_i \in \boldsymbol{U}_t,$$
$$\exists O \in \boldsymbol{O}_t,\ U_i \xrightarrow{a} {}^*O,\ O \notin O_t(U_i).$$

Услуги доступности следующие [2]:

• *использование ресурсов* позволяет пользователям управлять услугами и ресурсами:

$$\exists n_1, n_2 \in \boldsymbol{N} : |D_t(U)| < n_1, |O_t(U)| < n_2,$$
$$\forall t \in \boldsymbol{N}_0,\ \boldsymbol{N} \text{ — множество ресурсов;} \quad (3.1)$$

• *устойчивость к отказам* призвана гарантировать доступность КС (возможность использования информации, отдельных функций или КС в целом) после отказа ее компонента; должна обеспечиваться на аппаратном уровне при построении КС и СЗИ;

• *горячая замена* позволяет гарантировать доступность КС в процессе замены отдельных компонентов:

$$\exists O \in \boldsymbol{O}, \forall t \in \boldsymbol{N}_0, \exists \widetilde{O} \in \boldsymbol{O} : \widetilde{O}(t) = O(t); \quad (3.2)$$

• *восстановление после сбоев* обеспечивает возвращение КС к известному защищенному состоянию после отказа в обслуживании; услуга должна быть реализована в КС на всех уровнях.

4. Наблюдаемость информации

В отличие от конфиденциальности или целостности, где наличие каналов утечки является негативным обстоятельством, наблюдаемость должна иметь каналы наблюдения, с помощью которых можно контролировать процесс обработки информации. Формально это можно представить в таком виде:

$$U \xrightarrow{r,\ act} P \xrightarrow{r} \{P_k, O_l\},$$
$$k = 1, \ldots, K;\ l = 1, \ldots, L,$$

где пользователь U активизирует процесс P, который может получить доступ, например на чтение (r), к определенному множеству процессов и объектов $\{P_k, O_l\}$.

Таким образом, угроза наблюдаемости состоит в том, что пользователь, у которого есть соответствующие полномочия, не может получить доступ из $\boldsymbol{A}_3$ к информации. Запишем математическое выражение:

$$\exists t \in \boldsymbol{N}_0,\ \overline{\exists} a \in \boldsymbol{A}_3,\ \exists U_i \in \boldsymbol{U}_t,\ \exists O \in \boldsymbol{O}_t,$$
$$U_i \xrightarrow{a} {}^*O,\ O \in O_t(U_j),\ \forall j.$$

Очевидно, что угрозы наблюдаемости сводятся к повреждению каналов наблюдения, а главная задача наблюдаемости в КС — их поддерживать. Она реализуется с помощью таких услуг:

• *регистрация (аудит)* позволяет контролировать неблагоприятные для КС действия; услуга должна быть функционально реализована в составе ДД;

• *идентификация и аутентификация* позволяют СЗИ определить и проверить личность пользователя, который пытается получить доступ к КС; механизмы аутентификации должны быть реализованы на аппаратном, аппаратно-программном или программном уровнях и входить во множество процессов КС;

• *достоверный канал* позволяет гарантировать, что пользователь взаимодействует непосредственно с СЗИ и никакой другой пользователь или процесс не могут включиться во взаимодействие; должен реализоваться комплексом средств защиты (КСЗ) с целью адекватного управления безопасностью;

• *разграничение обязанностей* позволяет снизить вероятность умышленных или ошибочных действий пользователя и величину потенциальных убытков от таких действий:

$$\exists U \in \boldsymbol{U},\ \forall P, O \in D_t(U, a),$$
$$\forall a \in \boldsymbol{A}, \forall t \in \boldsymbol{N}_0; \qquad (4.1)$$

• *целостность КСЗ* определяет меру готовности КСЗ защищать себя и гарантировать бесперебойность управления защищенными объектами: очевидно, что целостность КСЗ должна контролироваться ДД;

• *самотестирование* позволяет проверить и на основании этого гарантировать правильность функционирования и целостность определенного множества функций КС; тестовые процедуры должны входить во множество процессов КС;

• *идентификация и аутентификация при обмене* позволяют одному объекту идентифицировать другой и обеспечить другому идентифицировать первый, прежде чем начать взаимодействие;

• *аутентификация отправителя* защищает от отказа от авторства и однозначно устанавливает принадлежность объекта определенному пользователю;

• *аутентификация получателя* предотвращает отказ от получения и однозначно устанавливает факт получения объекта определенным пользователем.

Последние три услуги зависят от полноты реализации КСЗ и, в частности, могут выполняться ДД.

5. Условия защищенности информации

Обсудим условия, которым должна удовлетворять КС, чтобы в ней могла быть реализована какая-либо ПБ.

Обозначим $\boldsymbol{S}$ множество информационных потоков между всеми объектами КС в любой момент времени $t \in \boldsymbol{N}_0$. Разобьем его на два непересекающихся подмножества $\boldsymbol{S}_F$ и $\boldsymbol{S}_L$ так, что $\boldsymbol{S} = \boldsymbol{S}_F \cup \boldsymbol{S}_L$, $\boldsymbol{S}_F \cap \boldsymbol{S}_L = \varnothing$, где $\boldsymbol{S}_F$, $\boldsymbol{S}_L$ — соответственно подмножества потоков, характеризующих НСД, и легальный доступ [9].

Необходимым условием реализации любой ПБ является существование в КС активного компонента, который осуществлял бы разрешение на порождение информационных потоков, принадлежащих только множеству $\boldsymbol{S}_L$. Таким компонентом является диспетчер доступа (ДД) [1, 9]. Разрешение на порождение потока в данном случае следует понимать как осуществление некоторой операции над объектом-получателем, а запрет — как неосуществление или неизменность объекта-получателя.

Таким образом, ДД полностью принимает участие в процессе доступа и, следовательно, должен принадлежать множеству ресурсов общего доступа $\boldsymbol{R}_t$. Очевидно также, что ДД должен контролировать все потоки, т.е. обходные пути ПБ должны отсутствовать (невозможность доступа к объектам без участия ДД), что формально записывается так: $\forall t \in \boldsymbol{N}_0$, $\forall a \in \boldsymbol{A}$, если один объект в момент времени t получил доступ к другому, то это означает, что в момент времени $t - k$, $k \in \boldsymbol{N}_0$ произошел запрос на доступ. Кроме того, при реализации ПБ любого типа необходимым условием является идентификация всех объектов КС, причем их имена должны быть уникальными. Если множеству объектов КС свойственна какая-либо структура, то ДД факти-

чески реализует распределение объектов в соответствии с нею. Наконец, заметим, что кроме наличия ДД реализация ПБ требует также внедрения в КС целого ряда перечисленных выше услуг, которые могут быть реализованы как программно, так и аппаратно.

Итак, в дальнейшем считается, что в КС всегда имеется активный компонент (ДД), который в любой момент времени однозначно определяет множество $D_t(U)$ для каждого пользователя.

В рамках рассматриваемого формализма изучим наиболее простую ПБ — дискреционную (ДПБ) [6, 9]. Сущность ДПБ заключается в том, что большинство прав, в том числе и право разрешать доступ другим пользователям, принадлежит пользователю, породившему объект. Атрибуты доступа, определяющие как множество активных объектов, которые могут получить доступ к пассивным объектам, так и сами виды возможных доступов, содержатся в матрице доступов [6, 9].

Одним из формальных способов выражения ДПБ может быть следующий: пусть имеет место цепочка доступов $U \xrightarrow{act} {*P}$; доступ $P \xrightarrow{a} O$, $a \in \boldsymbol{A}$, в некоторый момент времени $t \in \boldsymbol{N}_0$ может произойти только при условии $O \in D_t(U)$. Тогда справедливо следующее

Утверждение 1. Если все доступы осуществляются в соответствии с данной ДПБ, то каналы реализации угроз конфиденциальности и целостности будут перекрыты.

Доказательство. Сначала рассмотрим угрозу конфиденциальности. Предположим противное, т.е. пусть имеет место утечка информации или формально $\exists t \in \boldsymbol{N}_0$, $\exists a \in \boldsymbol{A}_1$, $\exists U_i \in \boldsymbol{U}_t$, $\exists O \in \boldsymbol{O}_t$, $U_i \xrightarrow{a} {*O}$, $O \in O_t(U_j)$, $i \neq j$; $i, j = 1, \ldots, n_U$. Это означает, что в t-й момент времени произошел НСД $a \in \boldsymbol{A}_1$ некоторого процесса P к объекту O. Согласно же ДПБ $O \in D_t(U_i) = \left\{O_j \mid U_i \xrightarrow{a} {*O_j}, a \in \boldsymbol{A}, t \in \boldsymbol{N}_0\right\}$, причем множество $D_t(U_i)$ определено однозначно. Следовательно, доступ вида $a \in \boldsymbol{A}_1 \subset \boldsymbol{A}$ в момент $t \in \boldsymbol{N}_0$ к объекту O для данного пользователя возможен только с разрешения ДД. Но это означает, что предположение о возможной утечке приводит к противоречию.

Пусть имеет место канал действия на целостность, т.е. в t-й момент времени произошел НСД $a \in \boldsymbol{A}_2$ некоторого процесса P к объекту O. Рассуждая аналогично случаю с конфиденциальностью, снова получим противоречие. Утверждение полностью доказано.

Поставим следующий вопрос: можно ли гарантировать в КС доступность и наблюдаемость информации, ведь по определению ДПБ решает лишь вопрос — давать или не давать доступ. Гарантировать же предоставление доступа пользователю U к объекту O при условии $O \in D_t(U)$ сформулированная ДПБ не может. Выходом из данной ситуации может стать реализация в КС ряда определенных услуг.

Заметим, что в [2] услуги наблюдаемости включены в каждый профиль, поскольку общеизвестно [1 − 9], что наблюдаемость является необходимым условием функционирования как СЗИ, так и КС вообще. Кроме того, на этих услугах базируется и ряд других. Таким образом, путь реализации угроз наблюдаемости может быть исчерпывающе перекрыт с помощью введения в КС услуг наблюдаемости. Доступность информации в КС, как ранее было отмечено, определяется работоспособностью самой КС.

Утверждение 2. Если в КС имеет место уникальная идентификация объектов, реализован ДД и действуют услуги наблюдаемости и доступности, то выполняется ДПБ.

Доказательство. Нужно доказать, что при условии реализации цепочки доступов $U \xrightarrow{act} {*P}$ доступ $P \xrightarrow{a} O$, $a \in \boldsymbol{A}$, в некоторый момент времени $t \in \boldsymbol{N}_0$ может произойти только при условии $O \in D_t(U)$. Пусть осуществился некоторый доступ. Тогда из факта его реализации вследствие уникальности идентификации объектов следу-

ет, что пользователь U единственный. Поскольку в КС реализованы услуги наблюдаемости, т.е. регистрация, идентификация/аутентификация и достоверный канал, то ДД однозначно всегда может определить принадлежность объекта тому или иному множеству. Следовательно, при проверке ДД атрибутов доступа объекта, находящихся в матрице доступа, однозначно будет установлено, что $O \in D_l(U)$. Утверждение доказано.

Следует отметить, что без получения гарантий надежного функционирования услуг принципиально нельзя говорить о гарантированной защищенности информации в КС, а лишь об относительной ее защищенности и пытаться оценить этот уровень.

Заключение

Рассмотренная формализация позволяет детально описывать угрозы информации и соответствующие им услуги. Это дает возможность формально описать ДПБ и в дальнейшем шире и эффективнее использовать доказательный метод [6] для описания, исследования и создания современных СЗИ. В частности, можно получить необходимые (а иногда и достаточные) условия выполнимости той или иной ПБ. Следует отметить, что рассмотренная формализация является несколько упрощенной и не учитывает целого ряда свойств СЗИ (например, разные возможности по доступу для администратора и обычного пользователя и др.). Тем не менее этот подход удобен и полезен при разработке защищенных КС, определении уровня их защищенности, построении ПБ.

Перспективным направлением представляется также исследование других ПБ (мандатной, ролевой) применительно к проблеме их приведения к национальным стандартам. Важной задачей остается моделирование защищенных распределенных вычислительных систем и поиск достаточных условий их защищенности.

1. *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.
2. *Критерії* оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 2.2–004–99. — Київ: ДСТСЗІ СБ України, 1999. — 55 с.
3. *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.
4. *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.
5. *Антонюк А.А., Боровская Е.Н., Суслов В.Ю.* Модель угроз информации в защищенных автоматизированных системах // Безопасность информации. — № 2. — 2001. — С. 17–22.
6. *Грушо А.А., Тимонина Е.Е.* Теоретические основы защиты информации. — М.: Яхтсмен, 1996. — 192 с.
7. *Антонюк А.А., Жора В.В.* Загрози інформації і канали витоку // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. — 2001. — №1. — С. 35–37.
8. *Антонюк А.А., Жора В.В.* Моделювання доступу та каналів витоку в інформаційних системах // Там же. — № 3. — С. 48–50.
9. *Щербаков А.Ю.* Введение в теорию и практику компьютерной безопасности. — М.: Изд. Молгачева С.В., 2001. — 352 с.

Получено 17.07.03

Об авторах

Антонюк Анатолий Александрович,
канд. физ.-мат. наук, старший научный сотрудник

Жора Виктор Владимирович,
аспирант

Мостовой Виталий Николаевич,
аспирант

Место работы авторов:
Институт программных систем НАН Украины,
просп. Академика Глушкова, 40,
Киев-187, 03680, Украина
Тел. (044) 266 3397, 434 4997