УДК 681.3.067

ОБОСНОВАНИЕ МЕРОПРИЯТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В. Ю. Осипов,
доктор техн. наук, профессор
И. А. Носаль,
аспирант
Санкт-Петербургский институт информатики и автоматизации РАН

Предложен подход к обоснованию мероприятий информационной безопасности с учетом ценности защищаемых информационных ресурсов. Рассмотрена модель ценности этих ресурсов. Приведены математическая формулировка и алгоритм решения задачи поиска целесообразных мероприятий информационной безопасности, предусматривающие синтез и анализ возможных программ деструктивных воздействий на защищаемые информационные ресурсы. Отражены результаты моделирования.

Ключевые слова *— информационная безопасность, оптимизация, методы, программы.*

Введение

Одной из актуальных научно-технических задач в области информационной безопасности (ИБ) выступает обоснование мероприятий ее обеспечения. От успешности решения этой задачи во многом зависят затраты на разработку (модернизацию) систем ИБ, а также потенциальные потери из-за нарушений безопасности. Из известных подходов к решению этой задачи [1–8] некоторые сводятся к минимизации стоимости мероприятий ИБ при выполнении требований к показателям безопасности. Когда затраты на реализацию мероприятий ИБ ограничены, при поиске целесообразного варианта минимизируют потери от нарушения ИБ или максимизируют эффект защиты, получаемый от проведения этих мероприятий [3–5]. Есть попытки обоснования мероприятий ИБ при минимизации суммы потерь на их реализацию и потерь в виде возможных информационных ущербов из-за деструктивных действий злоумышленников [1, 8]. В качестве показателей информационного ущерба используют абсолютные и относительные положительные или отрицательные приращения характеристик (свойств) защищаемых информационных ресурсов (ЗИР), систем, в которых они хранятся и обрабатываются, а также их потребителей. При этом в интересах оценки мероприятий ИБ во многих случаях строят графы (схемы программ) атак на ЗИР со стороны злоумышленников и оценивают их с помощью математических методов [3, 6–8].

Несмотря на значительное число работ, посвященных ИБ, многие аспекты оставлены без должного внимания, например вопросы в части обоснования мероприятий ее обеспечения по новым показателям (целевым функциям) с условиями, отражающими объективные закономерности неисследованных процессов. В частности, не уделяется должного внимания ценности ЗИР, потенциальной осведомленности и мотивациям злоумышленников, изменению во времени свойств каналов и программ деструктивного воздействия, характеристик применяемых средств защиты. Несовершенны также методы генерации и анализа таких программ с циклами.

Предлагается подход к обоснованию мероприятий ИБ по новым показателям с применением методов автоматического синтеза и анализа возможных программ деструктивного воздействия на ЗИР со стороны злоумышленников.

Задача обоснования мероприятий ИБ

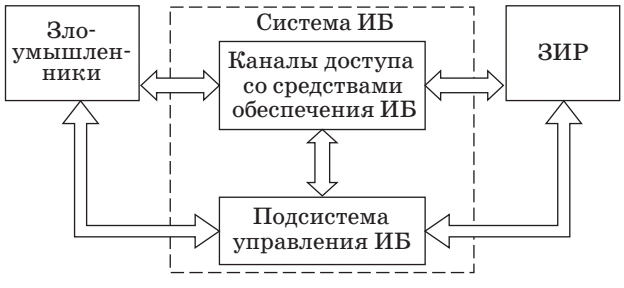
Рассмотрим постановку задачи на примере обеспечения ИБ в учреждениях высшей школы и науки. Определены виды защищаемых информационных ресурсов, форма их хранения и обработки. Такими ресурсами могут выступать персональные данные, отдельные сведения об учебной, научной и воспитательной работе, о финан-

сово-экономической деятельности, результаты перспективных научных исследований и разработок, учебно-методические материалы, имеющие существенную ценность, различные компьютерные программы, базы данных и др. Храниться информационные ресурсы могут в электронной форме (магнитные, лазерные диски, флеш-память), на бумажных носителях, в памяти сотрудников и обучаемых. Каждому такому информационному ресурсу свойственна своя ценность и возможные последствия от нарушений ИБ (незаконного копирования и распространения, искажения, уничтожения). Известно, что злоумышленники будут стараться деструктивно воздействовать на ЗИР по различным программам (схемам атак), используя уязвимости в системе ИБ и в системе обработки информации. При этом ценность ЗИР, как и потенциальные угрозы, со временем могут существенно изменяться.

Уже существует некоторая организационно-техническая система ИБ в учреждении, но она несовершенна.

Согласно схеме (рис. 1), комплекс мероприятий ИБ может предусматривать как исключение или затруднение деструктивных воздействий на ЗИР по многим каналам, так и непосредственное воздействие на злоумышленников. Среди этих мероприятий выступают мониторинг, применение различных средств защиты, изменение их параметров, ограничения физического доступа лиц к ЗИР и др. Кроме этого, на систему ИБ возлагаются функции по устранению последствий деструктивных воздействий и восстановлению ЗИР. Обоснование и реализация мероприятий ИБ осуществляются подсистемой управления ИБ, в качестве которой в частном случае могут выступать лица, ответственные за безопасность, со средствами управления.

Для совершенствования обеспечения ИБ необходимо разработать метод обоснования мероприятий ИБ, учитывающий особенности возникающих ситуаций и их динамику, позволяющий минимизировать возможные потери ценности ЗИР и затраты на реализацию этих мероприятий.



■ ***Рис. 1.*** Обобщенная структура системы информационной безопасности

Модель ценности защищаемых информационных ресурсов

В интересах разработки метода обоснования мероприятий ИБ определимся сначала с моделью ценности ЗИР. Опираясь на работу [9], определим ценность ЗИР как $V(t) = V_2(t) - V_1(t)$. Здесь $V_2(t)$, $V_1(t)$ — конечные эффекты на момент времени t, пересчитанные к входу системы, — санкционированного потребителя информации при наличии и отсутствии ЗИР соответственно. Пересчет конечных эффектов к входу предусматривает в нашем случае вычитание из них затраченных материальных и других ресурсов на получение интересующей информации. При этом предполагается, что потребитель использует полученную информацию оптимальным способом. Потребителем в частном случае может выступать сама система — обладатель ЗИР.

В соответствии с этими исходными посылками конечные эффекты $V_1(t)$, $V_2(t)$ могут быть представлены следующей аналитической зависимостью:

$$V_{1(2)}(t) = \max_{i(j)\in I(J)} \left\{ W_{1(2)i(j)}(t) - \sum_{r=1}^{N} a_r \cdot C_{1(2)r_{i(j)}}(t) \right\}, \quad (1)$$

где $W_{1i}(t)$, $W_{2j}(t)$ — эффекты, получаемые потребителем на момент времени t при достижении одних и тех же целей, соответственно, без интересующих ЗИР и при их наличии; I, J — множества всех возможных способов получения конечных эффектов в первом и втором случаях; $C_{1ri}(t)$, $C_{2rj}(t)$ — расходы r-го ресурса потребителя информации на достижение результатов $W_{1i}(t)$, $W_{2j}(t)$ соответственно; a_r — коэффициент приведения расхода r-го ресурса потребителя к единицам измерения конечных эффектов; N — число видов ресурсов потребителя, которые он может расходовать на получение и использование ЗИР.

Если выделить среди всех затраченных ресурсов на достижение эффекта $V_2(t)$ ресурсы, которые израсходованы на получение использованных ЗИР (на их разработку, покупку, восстановление, добывание), тогда

$$\sum_{r=1}^{N} a_r \cdot C_{2rj}(t) = \sum_{r=1}^{N} a_r \cdot C_{2.1rj}(t) + \sum_{r=1}^{N} a_r \cdot C_{2.2rj}(t). \quad (2)$$

Первое слагаемое в правой части выражения (2) соответствует затратам ресурсов на достижение эффекта $W_{2j}(t)$ при условии, что необходимые ЗИР в наличии, а второе — на получение ЗИР. Заметим, что наличие ЗИР означает и присутствие когда-то сделанных затрат на их получение.

С учетом (1), (2) ценность $V(t)$ ЗИР можно определить как

$$V(t)=\max_{j\in J}\min_{i\in I}\left\{W_{2j}(t)-W_{1i}(t)-\sum_{r=1}^{N}a_r\times\right.$$
$$\left.\times(C_{2.1rj}(t)-C_{1ri}(t))-\sum_{r=1}^{N}a_r\cdot C_{2.2rj}(t)\right\}. \quad (3)$$

Проанализируем это выражение. В условиях, когда разница между затратами ресурсов на достижение $W_{1i}(t)$, $W_{2j}(t)$ сводится к затратам на приобретение ЗИР:

$$\sum_{r=1}^{N}a_r(C_{2.1rj}(t)-C_{1ri}(t))=0, \quad (4)$$

их ценность относительно потребителя равна

$$V(t)=\max_{j\in J}\min_{i\in I}\left\{W_{2j}(t)-W_{1i}(t)-\sum_{r=1}^{N}a_r\cdot C_{2.2rj}(t)\right\}. \quad (5)$$

Снижение ценности $V(t)$ ЗИР для потребителя возможно, например, за счет искажения или внедрения в них ложных данных или раскрытия конфиденциальности.

В ситуации, когда можно успешно восстановить утраченные ЗИР до момента их использования, ценность ЗИР определяется как минимум затрат на их восстановление:

$$V(t)=\min_{j\in J}\sum_{r=1}^{N}a_r\cdot C_{2.2rj}(t). \quad (6)$$

Таким образом, в самом простом случае ценность ЗИР можно оценивать согласно (6), а при учете отдаленных последствий — по формуле (3) или (5).

Метод обоснования мероприятий ИБ

Учитывая особенности исследуемого процесса, задачу обоснования мероприятий ИБ математически можно сформулировать в следующем виде. Требуется найти комплекс M_o целесообразных мероприятий ИБ, при котором на момент времени t достигается минимум суммарных потерь $L_o(M_o, t)$:

$$L_o(M_o,t)=\min_{k\in Q}\left\{B_k(M_k,t)+\sum_{z=1}^{Z}V_z(t)\times\right.$$
$$\left.\times\left(1-\prod_{s=1}^{S_{kz}}(1-P_{kzs}(PRG_{kzs}(M_k),t))\right)\right\} \quad (7)$$

и выполняются условия

$$P_{kzs}(PRG_{kzs}(M_k),\ t)\ge P_E; \quad (8)$$
$$PRG_{kzs}(M_k)\in R, \quad (9)$$
$$k=1,\ 2,\ \ldots,\ K;\ z=1,\ 2,\ \ldots,\ Z;\ s=1,\ 2,\ \ldots,\ S_z.$$

В формулах (7)–(9) приняты обозначения: Q — область допустимых мероприятий ИБ; $B_k(M_k, t)$ — суммарные затраты на реализацию комплекса M_k мероприятий ИБ; $V_z(t)$ — текущая ценность z-го ЗИР; K — число мероприятий ИБ; Z — число ЗИР; $P_{kzs}(PRG_{kzs}(M_k),\ t)$ — вероятность деструктивного воздействия на z-й ЗИР по возможной s-й программе $PRG_{kzs}(M_k)$ при реализации комплекса M_k мероприятий ИБ; S_{kz} — число возможных альтернативных программ деструктивных воздействий на z-й ЗИР при комплексе M_k мероприятий ИБ; P_E — вероятность, при превышении которой угроза принимается во внимание; R — область допустимых результативных программ деструктивного воздействия на ЗИР.

В правой части выражения (7) второе слагаемое — это ожидаемые потери ценности ЗИР (риски). Потеря ценности z-го ЗИР имеет место, если он подвергся деструктивному воздействию хотя бы по одной из s-х программ. Согласно (8), принимаются во внимание только деструктивные программы с эффектом не ниже заданного. В соответствии с (9) анализируются только результативные программы, приводящие к нарушениям ИБ за конечное число шагов.

Решение этой задачи предусматривает генерацию потенциально возможных программ деструктивного воздействия на ЗИР, которые злоумышленники могут разработать с учетом их осведомленности, технической оснащенности и мотивации.

Результаты потенциальной осведомленности возможных злоумышленников о системе ИБ относительно текущего момента времени с формальной точки зрения для каждого анализируемого комплекса мероприятий ИБ предлагается задавать вектором исходных данных $\mathbf{d}_b = (d_{b1}, d_{b2}, d_{b3}, \ldots, d_{bN})$ и вектором интересующих результатов (целей) $\mathbf{d}_w = (d_{w1}, d_{w2}, d_{w3}, \ldots, d_{wM})$, а также условиями

$$F_{zv}(d_{zv\_e},\ e=1,\ 2,\ \ldots,\ E_z)\to d_{zv\_a},$$
$$z=1,\ 2,\ \ldots,\ Z;\ v=1,\ 2,\ \ldots,\ V_z, \quad (10)$$

связывающими исходное состояние с конечным. Для упрощения изложения материала индекс k здесь опущен. В (10) могут входить, например, функции получения доступа к ресурсам сервера с преодолением средств защиты, открытия защищаемых файлов, копирования, изменения параметров средств защиты для облегчения последующего доступа и др. Каждой из них ставятся в соответствие временные затраты на их реализацию. В выполнении этих функций могут участвовать как аппаратно-программные средства, так и злоумышленники. Условия (10) могут быть заданы в следующем виде (таблица).

■ Формализованные условия задачи

№ пп.	Функциональное выражение	Логическая запись	Статус	Условия истинности
1	$d_5 = F_{11}(d_1, d_2, d_3)$	$F_{11}(.), d_1, d_2, d_3 \to d_5$	F	
2	$d_5 >= F_{21}(d_2, d_4)$	$F_{21}(.), d_2, d_4 \to d_5$	R	7,12
3	$d_8 = F_{41}(d_7)$	$F_{41}(.), d_7 \to d_8$	S	N
.	.	.	.	
n	$d_{37} = F_{zv}(d_8, d_5)$	$F_{zv}(.), d_8, d_5 \to d_{37}$	F	
.	.	.	.	
N	$d_{504} = F_{ZVz}(d_{92})$	$F_{ZVz}(.), d_{92} \to d_{504}$	F	

В таблице F — основное условие; R — предусловие; S — постусловие. В графе «Условия истинности» для предусловий определены номера основных условий, при которых они должны быть истинными, а для постусловий — номера основных условий, при которых они должны быть ложными.

Ищутся результативные программы, с применением которых за конечное число шагов, исходя из $\mathbf{d}_b$, может быть достигнут конечный результат $\mathbf{d}_w$.

Синтез программ на заданном множестве условий предлагается осуществлять, исходя из стремления найти программу с наибольшим числом интерпретаций исходных данных, при которых достигается положительный результат [10].

Для доказательства существования результативной программы необходимо установить выполнимость основных и разрешимость вспомогательных условий задачи. Основное условие (F) считается выполнимым, если все входящие в него переменные являются свободными, а аргументы определены. Переменные могут считаться свободными в двух случаях. Во-первых, если они не связаны вспомогательными условиями. Во-вторых, если они связаны, но используются совместно с вспомогательными условиями, причем эти условия являются разрешимыми, и переменные, входящие в них, свободны. Вспомогательные условия (предусловия и постусловия) разрешимы, если все входящие в них переменные определены.

Если поставить всем элементам в условиях (10) соответствующие им предикаты, $P_{zv0}(F_{zv}(.))$, $P_{zv1}(d_{zv1})$, ..., $P_{zva}(d_{zv\_a})$, принимающие значение 1, когда переменные определены (истинны), и 0 в противном случае, то условия задачи могут быть записаны в виде

$$\{P_{zv0} \wedge P_{zv1} \wedge, ..., P_{ZVEz} \to P_{zv\_a} \,|\, S_{zv}, M_{zv}, z = 1, 2, ..., Z; v = 1, 2, ..., V_z\},$$

где S_{zv} — статус zv-го условия; M_{zv} — множество номеров основных условий, при которых предусловия и постусловия, соответственно, истинны и ложны. Для основных условий $M_{zv} = \varnothing$.

С учетом этого основное условие со свободными переменными выполнимо, если

$$P_{zv0} \wedge P_{zv1} \wedge, ..., P_{ZVEz} = 1.$$

Вспомогательное условие разрешимо, если

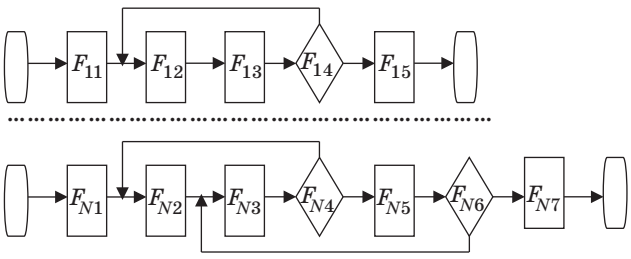
$$P_{zv0} \wedge P_{zv1} \wedge, ..., P_{ZVEz} \wedge P_{zv\_a} = 1.$$

Принимая это во внимание, синтез потенциально возможных деструктивных программ в интересах обоснования комплексов мероприятий ИБ предлагается осуществлять по следующему обобщенному алгоритму.

1. Ввод исходных данных и дополнительных условий.
2. Доказательство существования результативной программы.
3. Если доказательство не существует, то завершение синтеза.
4. Извлечение опорной программы из доказательства (вывода).
5. Если в опорной программе отсутствуют логические условия, то переход к п. 9.
6. «Сжатие» полученного вывода.
7. Обработка логических условий и получение подпрограмм.
8. Сведение подпрограмм в общую программу.
9. Выдача результативной программы.

Доказательство существования результативной программы выполняется от исходных данных к результату с использованием принципа резолюций [11]. Для выделения результативной программы из этого доказательства, если она существует, рекомендуется использовать идею обратного вывода. Этот вывод следует осуществлять по схеме зеркальной прямому выводу. При «сжатии» полученного вывода условия, взаимный порядок расположения которых в линейной программе не влияет на результат, прижимаются к условиям, использующим их. В интересах синтеза результативных программ с циклами на заданном множестве условий ищутся программы с наибольшим числом интерпретаций исходных данных, при которых достигается положительный результат.

При синтезе мы получаем схемы программ, подлежащих оцениванию. Простые примеры таких схем программ показаны на рис. 2, где F_{ij} —



■ ***Рис. 2.*** Примеры синтезированных схем программ

функции, которые потенциально могут реализовываться злоумышленниками при доступе и деструктивном воздействии на ЗИР. Если условиям (10) однозначно ставятся элементы программного кода на одном из известных языков программирования, то в результате такого синтеза получаем машинные программы.

Зная структуры таких программ и принимая во внимание случайный характер подлежащих анализу процессов, вероятности деструктивных воздействий можно рассчитать с применением математического аппарата полумарковских процессов [12]. Частным случаем его выступает аппарат марковских процессов. Предлагается по структурам синтезированных программ автоматически составлять системы интегральных (для полумарковских процессов) или дифференциальных (для марковских процессов) уравнений и разрешать их, получать искомые вероятности $P_{kzs}(PRG_{kzs}(M_k), t)$ деструктивных воздействий на z-е ЗИР по возможным s-м программам $PRG_{kzs}(M_k)$ при реализации комплекса M_k мероприятий ИБ. Технология автоматического составления таких систем уравнений известна. Методы разрешения их реализованы в ряде пакетов прикладных программ (MatLab, MathCad). В некоторых случаях могут быть использованы и другие методы оценки [13]. Особенностью такого анализа выступает необходимость учета неопределенности по разрешению логических условий в синтезированных программах. Эта неопределенность численно характеризуется числом и длительностью циклов в соответствующих программах, которые необходимо реализовать, чтобы ее преодолеть. Ее также можно определять через относительные частоты анализируемых переходов.

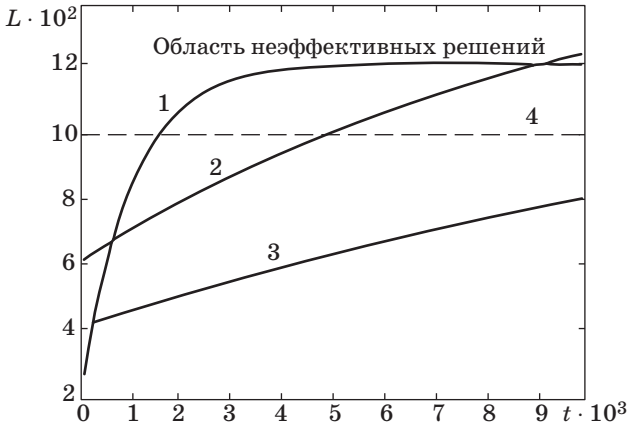
Суммарные затраты $B_k(M_k, t)$ на реализацию комплекса M_k мероприятий ИБ могут складываться из стоимости приобретаемых и устанавливаемых средств защиты, затрат на управление ими и восстановление ИР. Определение их может осуществляться простым суммированием затрат на реализацию отдельных мероприятий.

Заметим, что с течением времени исходные данные, защищаемые ресурсы, возможные мероприятия ИБ и условия (10) могут изменяться. С учетом этого обоснование мероприятий ИБ должно осуществляться для предварительно заданного интервала времени T. Период повторения $\Delta t << T$ такого обоснования и реализации найденных решений должен выбираться в зависимости от интенсивности угроз.

Результаты моделирования

Проверка работоспособности предлагаемого метода осуществлялась на простых примерах. Информация о защищаемых ресурсах и самой системе ИБ задавалась в виде правил (10). Защищались три вида информационных ресурсов и оценивались три различных комплекса мероприятий ИБ. Каждому комплексу мероприятий с формальной точки зрения ставилась своя система правил (10), с соответствующими им временными характеристиками и затратами со стороны системы ИБ. В качестве таких систем выступали совокупности из 18, 24 и 40 правил (10). Достаточно просто и легко синтезировались возможные линейные программы доступа к информационным ресурсам. Время t_c синтеза таких программ на скалярных процессорах прямо пропорционально квадрату числа n условий (10) задачи: $t_c = cn^2$. Синтез программ с логическими условиями (программ с циклами) требовал больше времени: $t_c \approx bn_1^2(1 + n_2)^2$, где b — постоянный коэффициент; n_1 — число основных условий задачи; n_2 — число логических условий. Для расчета вероятностей деструктивного воздействия на ЗИР по синтезированным программам использовался аппарат марковских процессов. При оценке ценности ЗИР применяли выражение (6). Установлено, что если с течением времени не тратить средства на поддержание требуемого уровня ИБ, существенных потерь ценности ЗИР не избежать. Затраты на обеспечение ИБ должны быть ниже ценности защищаемых информационных ресурсов, иначе мы всегда будем в минусе. На рис. 3 показаны результаты математического моделирования процессов обеспечения ИБ.

Из трех проанализированных вариантов предпочтение следует отдать третьему комплексу мероприятий ИБ. Затраты на его реализацию $B_3(M_3, t = 0) = 400$ усл. ед. больше, чем для первого, но меньше, чем для второго комплекса.



■ ***Рис. 3.*** Результаты обоснования комплексов мероприятий ИБ: *1*, *2*, *3* — зависимости основного показателя L суммарных потерь от времени t при реализации, соответственно, первого, второго и третьего комплексов мероприятий ИБ; *4* — линия, разделяющая области эффективных и неэффективных решений

При применении третьего комплекса мероприятий ИБ на всем анализируемом временном интервале суммарные потери не превышают ценности ЗИР. Она в данном случае составляет 1000 усл. ед. Однако заметим, что первый комплекс в связи с малыми затратами на его реализацию обладает временными преимуществами над третьим вариантом на незначительном интервале времени t = = 0...200. Следовательно, при принятии решений по обеспечению ИБ необходимо учитывать временной интервал безопасности. Принимая это во внимание, в качестве целевой функции задачи обоснования мероприятий ИБ вместо (7) в ряде случаев предлагается использовать минимальную площадь $S_o(M_o, T)$ под кривой суммарных потерь на заданном интервале времени T:

$$S_o(M_o, T) = \min_{k \in Q} \int_0^T L_k(M_k, t)\mathrm{d}t; \qquad (11)$$

$$L_k(M_k, t) = B_k(M_k, t) + \\ + \sum_{z=1}^{Z} V_z(t)\left(1 - \prod_{s=1}^{S_{kz}} (1 - P_{kzs}(PRG_{kzs}(M_k), t))\right). \qquad (12)$$

Параметры, входящие в (11), (12), раскрыты при пояснении (7)–(9).

Заключение

В результате выполненного исследования разработан новый метод обоснования мероприятий ИБ.

Обоснование мероприятий ИБ предлагается осуществлять, исходя из минимума общих потерь, среди которых ключевое место занимают потери из-за снижения ценности ЗИР. В интересах этого уточнена модель ценности ЗИР. В ряде случаев ценность ЗИР предлагается оценивать как минимум затрат на их восстановление. В общем случае рекомендуется учитывать отдаленные последствия из-за возможных деструктивных воздействий на ЗИР. Для этого целесообразно разработать математические модели систем — потребителей конкретной информации.

При обосновании мероприятий ИБ предлагается автоматически синтезировать на знаниях потенциально возможные для злоумышленников программы деструктивных воздействий на ЗИР и оценивать их. При этом возможен автоматический синтез не только линейных программ, но и программ с циклами.

Особенностью предлагаемого метода выступает его ориентированность на широкий круг возможных ситуаций обеспечения ИБ, учет ценности ЗИР и потенциальной информированности злоумышленников на текущий момент времени.

Отдельные положения метода могут быть применимы также при решении частных задач ИБ.

В целом предлагаемый метод расширяет взгляды и возможности по обоснованию мероприятий ИБ в различных условиях.

Литература

1. **Астахов М. А., Ростовцев Ю. Г., Яфраков М. Ф.** Информационная борьба. — М.: ТОМ, 2007. — 334 с.
2. **Осипов В. Ю., Юсупов Р. М.** Информационный вандализм, криминал и терроризм как современные угрозы обществу // Тр. СПИИРАН. 2009. Вып. 8. С. 34–45.
3. **Мальцев Г. Н., Теличко В. В.** Оптимизация состава средств защиты информации в информационно-управляющей системе с каналами беспроводного доступа на основе графа реализации угроз // Информационно-управляющие системы. 2008. № 4. С. 29–33.
4. **Миронов В. В., Носаль И.А.** Моделирование и оценка системы обеспечения информационной безопасности на примере ГОУ ВПО «СыктГУ» // Информация и безопасность. 2011. № 2. С. 209–211.
5. **Молдованин Т. В.** Решение задачи выбора оптимального варианта комплексной защиты информации с помощью метода экспертного оценивания // Информационно-управляющие системы. 2007. № 3. С. 39–44.
6. **Wang L., Yao C., Singhal A., Jajodia S.** Implementing interactive analysis of attack graphs using relational databases // J. of Computer Security. 2008. N 16. P. 419–437.
7. **Burgess M., Canright G., Engo-Monsen K.** A graph-theoretical model of computer security // Intern. J. of Information Security. 2004. N 3. P. 70–85.
8. **Dewri R., Ray I., Poolsappasit N., Whitley D.** Optimal security hardening on attack tree models of networks: a cost-benefit analysis // Intern. J. of Information Security. 2012. N 11. P. 167–188.
9. **Осипов В. Ю., Кондратюк А. П.** Оценка информации в интересах рефлексивного управления конкурентами // Программные продукты и системы. 2010. № 2. С. 64–68.
10. **Осипов В. Ю.** Синтез результативных программ управления информационно-вычислительными ресурсами // Приборы и системы управления. 1998. № 12. С. 24–27.
11. **Искусственный** интеллект. В 3 кн. Кн. 2. Модели и методы: справочник / под ред. Д. А. Поспелова — М.: Радио и связь, 1990. — 304 с.
12. **Новиков И. С.** Методы расчета количественных показателей надежности сложных программных комплексов на стадии проектирования и разработки // Тр. СПИИРАН. 2008. Вып. 6. С. 86–111.
13. **Осипов В. Ю.** Оценка защищенности информационно-вычислительных ресурсов от несанкционированного доступа // Приборы и системы управления. 1996. № 7. С. 16–19.