Ю. В. Гуляев, А. С. Багдасарян, Г. А. Кащенко, Р. В. Семенов

ОЦЕНКА РИСКА НЕСАНКЦИОНИРОВАННОГО ДОСТУПА ПРИ ИСПОЛЬЗОВАНИИ СИСТЕМ РАДИОЧАСТОТНОЙ ИДЕНТИФИКАЦИИ

Задача обеспечения безопасности телекоммуникационных систем (ТКС) с целью минимизации ущерба от реализации потенциальных угроз, в том числе террористических, относится к числу приоритетных направлений научных исследований в области информационной безопасности Российской Федерации [1]. Это связано с увеличением удельного веса информационных потоков, используемых для процессов управления и принятия решений в государственных органах и коммерческих структурах. Решение задачи обеспечения безопасности ТКС, в свою очередь, обусловливает необходимость решения задачи оценки риска НСД при использовании средств защиты, в частности средств радиочастотной идентификации для контроля доступа, входящих в состав систем защиты (СЗ) рассматриваемых объектов.

Для решения данной задачи широко применяется технология радиочастотной идентификации (РЧИ) [2]. Известны полупроводниковые системы и устройства, использующие эту технологию: смарт-карты, магнитные карты, электронные замки, бесконтактные электронные идентификаторы и др. [2, 3]. Однако они обладают существенными недостатками, такими, как: зависимостью от электромагнитных помех, необходимостью наличия источника питания, ограниченным рабочим диапазоном температур, невозможностью работать в агрессивных средах и на территории с повышенным радиационным уровнем. В этой связи обращают на себя внимание системы и устройства РЧИ, созданные на основе акустоэлектронных технологий (АЭТ). Система, использующая эту технологию, состоит из следующих основных компонентов: устройства считывания, акустоэлектронных меток (АЭМ) и программного обеспечения для обработки данных в компьютерной системе. АЭМ, в отличие от аналогичных устройств на основе полупроводниковых технологий, обладают следующими отличительными особенностями: имеют малые массогабаритные характеристики, работают на частотах УВЧ и СВЧ, невосприимчивы к электромагнитным помехам, имеют расширенный температурный режим работы, устойчивы к жесткой радиации, пассивные.

Целью работы является оценка риска НСД при использовании средств и систем РЧИ.

Рассмотрим эффективность применения средств контроля доступа на основе РЧИ для защиты от НСД пункта управления ТКС. Для этого оценим риск НСД, который определяется как [6]:

$$R_{НСД} = P_{угрозы} \cdot P_{уязв.} \cdot C, \qquad (1)$$

где $P_{угрозы}$ — вероятность реализации угрозы, $P_{уязв.}$ — вероятность уязвимости, C — предполагаемый ущерб от реализации угрозы. Информационные и программные ресурсы считаются достаточно защищенными, если с учетом возможности потенциального преодоления преград СЗ риск НСД меньше допустимого значения.

Структурная схема системы защиты пункта управления ТКС с применением подсистемы РЧИ на основе АЭТ приведена на рис. 1.

Нарушитель получает доступ к информации и/или программным ресурсам пункта управления ТКС, если он успешно преодолевает последовательность преград, определяемых СЗ. Для защиты пункта управления автоматизированной ТКС существует свой набор преград $P_r, r = \overline{1, N}$, где N —количество преград, которое необходимо преодолеть нарушителю, чтобы получить доступ к пункту управления; P_r — вероятность преодоления нарушителем r-й преграды пункта управления. Здесь $P_r = P_{угрозы} \cdot P_{уязв.}$.

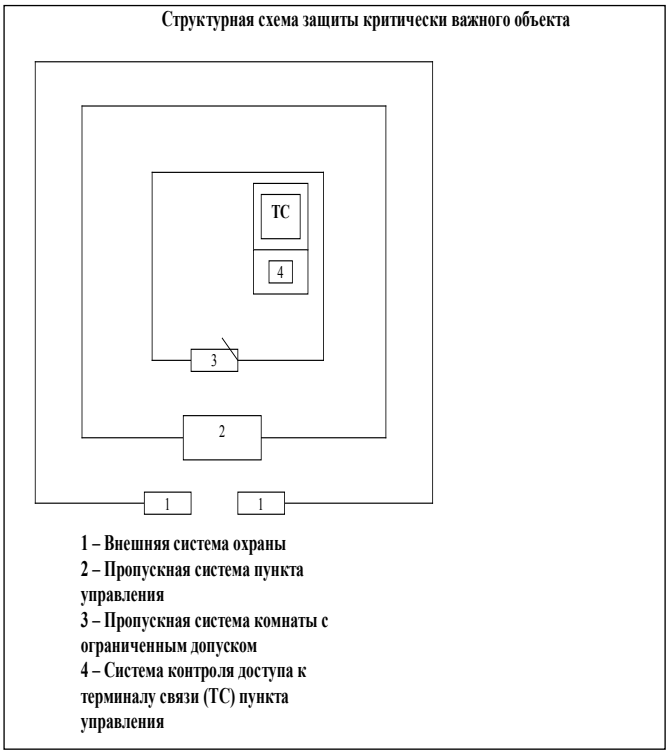

Рис. 1. Структурная схема защиты пункта управления ТКС

Зависимость вероятности подбора кода средства контроля доступа от времени можно определять как:

$$P(t) = 1 - e^{-\frac{t \cdot M}{S}}, \quad (2)$$

где S — мощность пространства кодов, M — скорость подбора кодов.

Мощность пространства кодов вычисляется следующим образом [7]:

$$S = A^L, \quad (3)$$

где L — длина кода, A — мощность алфавита кода.

Кодирование определяется топологией АЭМ. Для формирования кодов с заданными свойствами в системе может использоваться фазовая и амплитудная модуляция. В простейшем случае амплитудного позиционного кодирования (ASK – amplitude shift keying) каждый символ в определенной позиции сигнала связан с наличием (бит – есть, «1») или отсутствием отражателя (бит – нет, «0») в соответствующем месте в топологии АЭМ. Общее число возможных отражателей определяют длину кода и возможное число АЭМ с различными кодами. Например, при числе отражателей 16, длина кода равна 16 битам, а число различных кодов равно 2^{16}=65536. При фазовой модуляции PSK (phase shift keying) в ответном сигнале АЭМ меняются фазы сигнала, при неизменных амплитудах. Бинарная фазовая модуляция дает меньше ошибок с уровнем сигнала на 6 дБ меньшем, чем при амплитудной модуляции. Это позволяет увеличить расстояние между устройством считывания и АЭМ. Фазовая модуляция более высокого порядка, использующая несколько символов (отражателей), уменьшает длину подложки метки, немного уменьшая вносимые потери, но требует для обработки более высокое отношение сигнал/шум. Требования к АЭМ, использующим фазовую модуляцию, являются более жесткими, смещения электродов, формирующих фазовые сдвиги, невелики и поэтому требуют при их изготовлении большей точности, т.е. они менее технологичны (длина волны λ=4 мкм, а смещения электродов при бинарной модуляции $\Delta L = \lambda/4$=1 мкм, отсюда точность должна быть 0.1 мкм). В связи с этим

чаще отдают предпочтение позиционной амплитудной модуляции, с помощью которой достигается большая длина кодов и меньшая чувствительность при изготовлении АЭМ.

При проектировании АЭМ на основе отражателей применяются различные варианты конструкций (Рис. 2, а-г). На рис. 2 а) представлена конструкция АЭМ на основе приемопередающего однонаправленного ВШП с набором отражательных ВШП с малым числом электродов. На рис. 2 б) представлена многоканальная конструкция АЭМ, на рис. 2 в) – конструкция АЭМ на основе временного разделения слотов, на рис. 2 г) - конструкция АЭМ на основе одновременного фазового кодирования и временного разделения слотов.

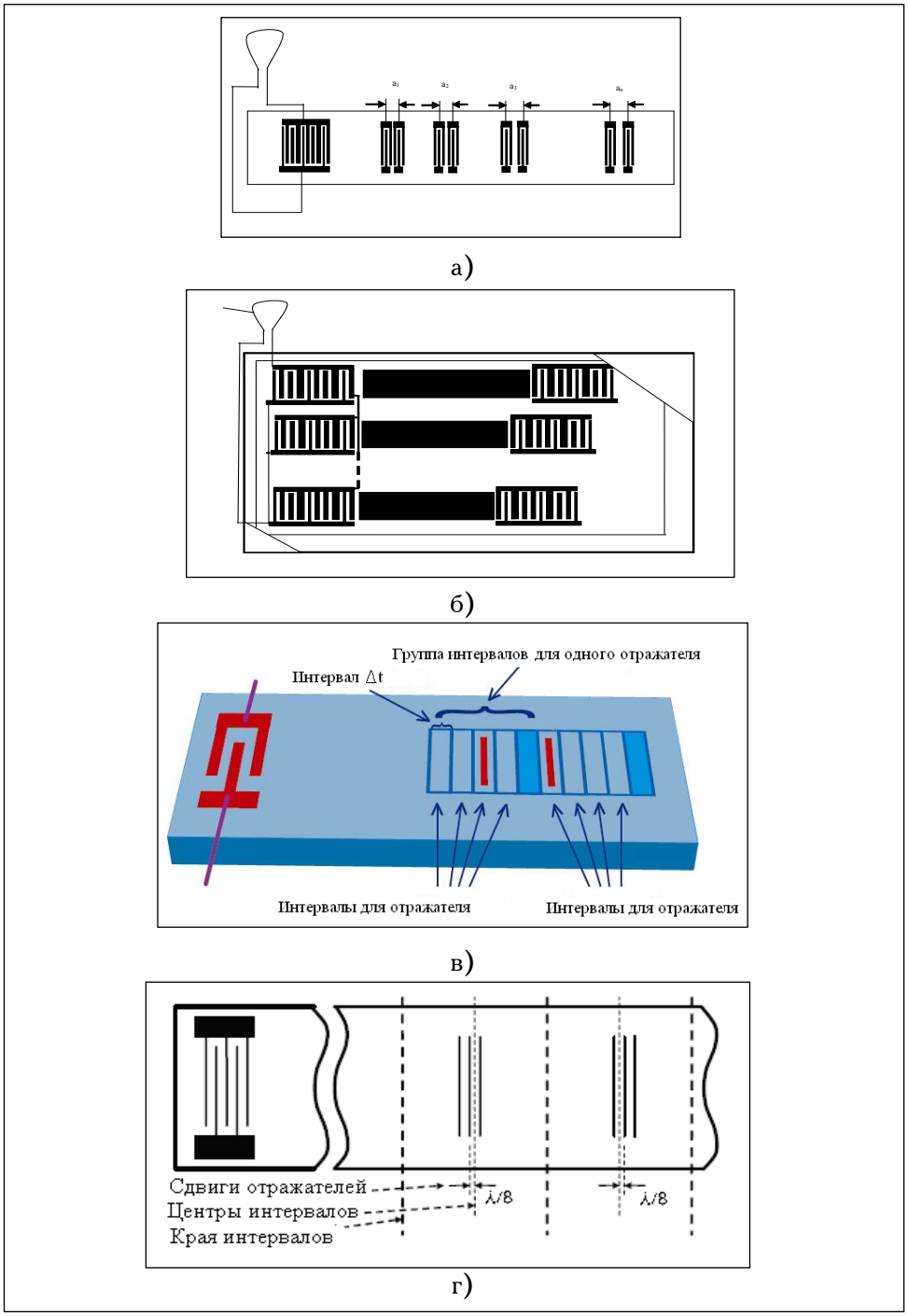

Рис. 2. Основные типы конструкций АЭМ

На рис. 3 а) и 3 б) приведены временные диаграммы АЭМ для способов кодирования временных позиций и одновременных фазовых и временных позиций соответственно. Величина интервала $\Delta t = 1/\Delta F$, где ΔF — ширина полосы пропускания системы.

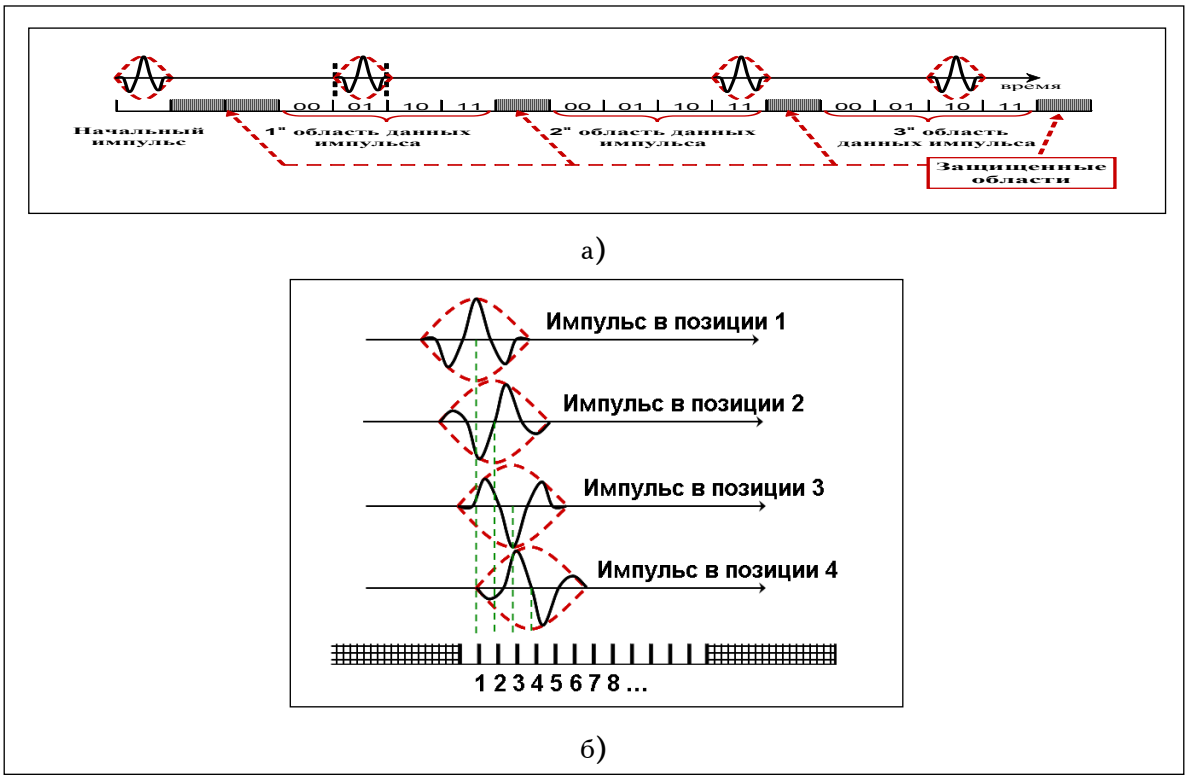

Рис. 3. Основные способы кодирования данных в АЭМ

Рассмотрим более подробно способ кодирования данных АЭМ, основанный на одновременной модуляции фазовых и временных позиций. Здесь число состояний N, которые возможны в пределах одной пачки информационных импульсов определяется как [8]:

$$N = \frac{(L-(M-1)\cdot K)!}{(L-(M-1)\cdot K-M)!\cdot M!}, \tag{4}$$

где L — число временных интервалов в пачке импульсов; M — число импульсов в пачке; K — минимальное число пустых промежутков, которые должны присутствовать между импульсами, чтобы удовлетворять критерию Найквиста.

АЭМ характеризуется следующими параметрами: B — число битов данных; D — плотность записи; E — эффективность импульсов; S — коэффициент разделения импульсов; H — показатель качества, характеризующий производительность системы.

$$B=\text{int}(\log 2\ (N)), \tag{5}$$

$$D = \frac{B}{\Delta t \cdot \Delta F \cdot (L+K)}, \tag{6}$$

$$E = B/M\ , \tag{7}$$

$$S = \Delta F \cdot \Delta t \cdot (1+K), S \geq 1, \tag{8}$$

$$H = D \cdot E\ . \tag{9}$$

В выражениях (5)-(9) Δt — длительность временного интервала, ΔF — ширина полосы пропускания системы, $\Delta T = \Delta t \cdot (L+K)$ — общая длительность пачки, $\Delta t \cdot (1+K)$ — минимальное разрешенное расстояние между двумя импульсами.

Значение коэффициента разделения импульсов S важно для расшифровки данных. Хорошая расшифровка сигналов АЭМ требует, чтобы около пика любого информационного импульса, фаза этого импульса не была подвержена помехам от соседних импульсов. В идеальной системе соседние импульсы с минимальным разделением начинают перекрывать пик данного импульса при $S = 1$. На практике S больше 1, так как системы функционируют в реальной помеховой обстановке и требуют приемлемый диапазон погрешности для успешной демодуляции.

При использовании АЭМ для защиты от НСД, вероятность реализации угрозы несанкционированного преодоления преграды определяется вероятностью подбора кода АЭМ. В случае непрерывных попыток подобрать код вероятность подбора определяется как:

$$P(t) = \frac{M \cdot t}{A^L}, \tag{10}$$

для АЭМ $A = 2$ [8]. График зависимости вероятности подбора кода АЭМ от времени для различных L представлен на рис. 4.

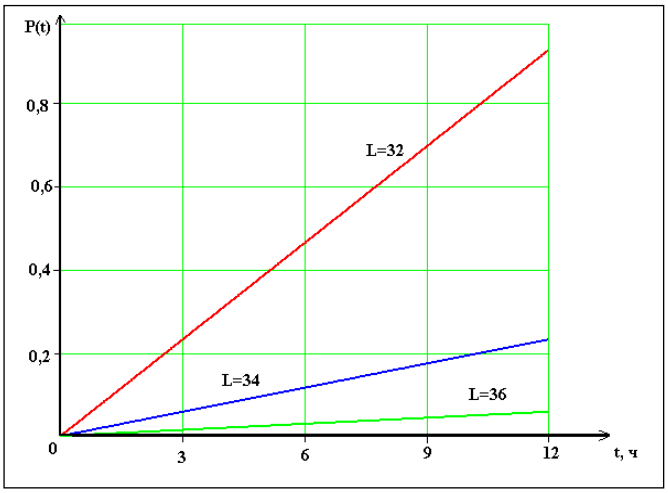

Рис. 4. Зависимость вероятности подбора кода АЭМ от времени

Тогда длину кодовой последовательности АЭМ для СЗ от НСД необходимо выбирать согласно следующему правилу:

$$2^L \geq \frac{M \cdot t}{P}, \tag{11}$$

где L — требуемая разработчику длина кодовой последовательности АЭМ, M — число опробованных нарушителем кодов АЭМ в единицу времени, P — заданная разработчиком СЗ вероятность подбора правильного кода АЭМ нарушителем в течение времени t.

В качестве примера рассмотрим СЗ, в состав которой входят четыре преграды (см. табл. 1): 1) внешняя система охраны; 2) пропускная система пункта управления; 3) пропускная система комнаты с ограниченным допуском; 4) система контроля доступа к терминалу связи. Различные системы идентификации имеют различные значения $P_{уязв.}$, которые зависят от защищенности самих систем, причем, чем выше защищенность, тем ниже $P_{уязв.}$

В табл. 1 отражены характеристики преград на основе используемых средств контроля доступа. Для определения защищенности средств контроля доступа используется экспертная процедура оценки на основе метода анализа иерархий [9]. В качестве параметров для оценки защищенности используются: помехозащищенность, надежность, криптостойкость. Иерархическая система для относительной оценки защищенности приведена на рис. 5.

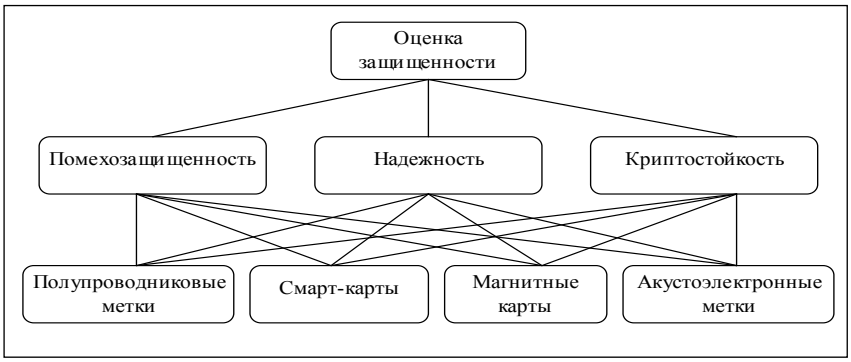

Рис. 5.

Попарным сравнением критериев определяется степень их важности по универсальной шкале Саати [10]. Так как все средства контроля доступа имеют одно и то же назначение, то $A_1 = A_2 = A_3$, а значит, равны и коэффициенты значимости одних и тех же параметров для каждого средства. По результатам экспертных оценок сформирована матрица

$$A = \begin{Vmatrix} 1 & 1/4 & 1/7 \\ 4 & 1 & 1/5 \\ 7 & 5 & 1 \end{Vmatrix}.$$

Собственный вектор матрицы $\omega_1 = \omega_2 = \omega_3 = \{0{,}073; 0{,}205; 0{,}722\}$. Для матрицы A $\lambda_{max} = 3{,}128$; индекс согласованности экспертов ИС = 0,064, отношение согласованности ОС = 0,11.

Согласно расчету средства контроля доступа имеют следующие коэффициенты защищенности $K_{защ.}$: полупроводниковые метки — 0.167, смарт-карты — 0,117, магнитные карты — 0,073, акустоэлектронные метки — 0,643. Вероятность уязвимости определяется как: $P_{уязв.} = 1 - K_{защ.}$.

Данные о вероятности реализации угрозы НСД при использовании средств контроля доступа получены на основе формулы (10), при значениях М = 10^5 кодов/с, $t = 6$ ч.

Таблица 1.

Преграда	Вероятность преодоления преграды
Внешняя система охраны с использованием а) АЭМ с длиной кода равной 32 битам	0,32
б) на основе полупроводниковых меток с длиной кода равной 32 битам	0,75
Пропускная система пункта управления на основе а) электронных карт со встроенными АЭМ с длиной кода равной 32 битам	0,32
б) на основе смарт-карт с длиной кода равной 32 битам	0,795
Пропускная система комнаты с ограниченным допуском на основе а) пропуска с АЭМ с длиной кода равной 40 битам	0,027

б) магнитных карт с длиной кода равной 40 битам	0,07
Система контроля доступа к терминалу связи на основе а) электронного ключа со встроенной АЭМ (длина кода равна 48 бит)	0,0032
б) электронного ключа доступа со встроенной полупроводниковой меткой (длина кода равна 48 бит)	0,0075

Вероятность сохранения защищенности пункта управления автоматизированной ТКС определяется как [3]:

$$P_{\text{ПУ}} = 1 - \prod_{r=1}^{N} P_r \,. \qquad (12)$$

Сравним эффективность защиты пункта управления автоматизированной ТКС от НСД с применением средств контроля доступа на основе АЭТ и на основе полупроводниковых технологий. Для определенности примем предполагаемый ущерб C от реализации НСД равный 10000000 руб., который в общем случае определяется ценностью информации, обрабатываемой в ТКС. Для оценки риска НСД к пункту управления ТКС используем формулы (1), (12).

Результаты оценки риска НСД при использовании систем РЧИ представлены в табл. 2.

Таблица 2.

	СЗ на основе полупроводниковых технологий	СЗ на основе АЭТ
Вероятность сохранения защищенности пункта управления	0,99969	0,99999
Риск безопасности пункта управления	3100	100

Снижение риска НСД пункта управления ТКС определим исходя из данных табл. 2 по следующей формуле:

$$\Delta R = \frac{3100 - 100}{3100} \cdot 100\% = 96\% \,.$$

Таким образом, применение средств и систем РЧИ на основе АЭТ для СЗ позволяет повысить эффективность защиты почти в 2 раза.

СПИСОК ЛИТЕРАТУРЫ:

1. Протокол № 1 от 28.03.2001 заседания секции по информационной безопасности научного совета при Совете Безопасности Российской Федерации.

2. *Дшхунян В. Л., Шаньгин В. Ф.* Электронная идентификация. Бесконтактные электронные идентификаторы и смарт-карты. М.: ООО «Издательство АСТ»: Издательство «НТ-Пресс», 2004. – 695 с.: ил.

3. *Гарсиа М.* Проектирование и оценка систем физической защиты. М.: Мир: ООО «Издательство АСТ», 2002. – 386 с., ил.

4. *Гуляев Ю. В., Багдасарян А. С., Кащенко Г. А., Багдасарян С. А., Семенов Р. В.* Аутентификация в беспроводных локальных сетях на основе устройств радиочастотной идентификации // Информация и безопасность: регион. науч.-техн. журнал. Воронеж, 2007. Вып. 4. С. 75–82.
5. *Гуляев Ю. В., Багдасарян А. С., Кащенко Г. А., Семенов Р. В.* Автоматизация процессов обработки и защиты информации в информационно-телекоммуникационных системах на основе радиочастотной идентификации // Информация и безопасность: регион. науч.-техн. журнал. Воронеж, 2008. Вып. 1. С. 31–38.
6. *Петренко С. А., Симонов С. В.* Управление информационными рисками. М.: ДМК Пресс, 2004. – 384 с.
7. *Девянин П. Н.* Модели безопасности компьютерных систем. М.: Академия, 2005. – 144 с.
8. *Hartman C. S.* A Global SAW ID Tag with Large Data Capacity // Proc. IEEE Ultrasonics Symposium, Munich, 2002. С. 63–67.
9. *Гуляев Ю. В., Багдасарян А. С., Кащенко Г. А., Семенов Р. В.* Интеллектуальные системы мониторинга безопасности на основе ПАВ-технологий // Информация и безопасность: регион. науч.-техн. журнал. Воронеж, 2008. Вып. 3. С. 349–354.
10. *Саати Т.* Принятие решений. Метод анализа иерархий: пер. с англ. М.: Радио и связь, 1993. – 316 с.