УДК 681.3

ОБ АКТУАЛЬНОСТИ ЗАДАЧ МАТЕМАТИЧЕСКОГО МОДЕЛИРОВАНИЯ МЕХАНИЗМОВ ЗАЩИТЫ ИНФОРМАЦИИ ОТ ИСКАЖЕНИЯ В СИСТЕМАХ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ

С. В. Скрыль*, А. М. Сычев, М. Ф. Сизинцев*****

* *Воронежский институт ФСИН России*
** *Московский государственный технический университет*
*** *Воронежский государственный технический университет*

Анализ ретроспектив развития информатики как объективного начала жизнедеятельности общества и перспектив ее влияния на современные общественные процессы позволяет выявить устойчивую тенденцию усиления роли технологий, связанных с обеспечением своевременности, полноты и достоверности результатов информационной деятельности [1]. Именно такие технологии, известные как высокие технологии (Hi-Tech), определяют эволюцию современной цивилизации.

Вместе с тем, применение этих технологий в различных сферах деятельности современного общества наряду с неоспоримыми преимуществами имеет ряд негативных последствий. Наиболее характерным отрицательным фактором выступает повышение уровня профессионализма криминальных структур, сопровождающего рост организованности современной преступности и дальнейшее совершенствование ее технической оснащенности, базирующееся на новейших достижениях научно-технического прогресса [2].

Первоочередным объектом противоправных действий криминальной среды является информационная деятельность так называемых критических инфраструктур – тех институтов государства, ущерб от нарушения деятельности которых приводит к особо значительным, а подчас к фатальным последствиям.

К таким структурам относится в первую очередь финансовая сфера.

Практика борьбы с противоправными действиями в отношении информационных ресурсов финансовой сферы на современном этапе ее развития дает основание считать, что одной из основных ее уязвимостей являются информационные процессы систем дистанционного банковского обслуживания (СДБО).

Практика эксплуатации СДБО дает основание считать, что целенаправленное изменение информации этих систем в процессе противоправных действий может нанести значительный ущерб деятельности основных ее элементов финансовой сферы.

Согласно терминологии информационной безопасности подобное изменение информации определяется как нарушение ее целостности [3].

Постоянное совершенствование методов несанкционированного доступа к информации СДБО с целью ее искажения обусловило целенаправленное и системное совершенствование технологий обеспечения целостности информации и способов применения соответствующих средств ее защиты от искажения.

Это в свою очередь ставит крайне актуальную проблему адекватной оценки эффективности таких технологий.

В условиях возрастания требований к уровню защищенности информационных процессов в СДБО, связанных с их постоянным совершенствованием на современном этапе развития финансовой системы, а также возрастанием потребности в методическом обеспечении мероприятий по противодействию искажению информации в СДБО вопросы оценки эффективности противодействия становятся в разряд наиболее актуальных.

При этом анализ содержания проблемы совершенствования способов оценки эффективности защиты информации в СДБО от искажения позволяет утверждать, что основным направлением ее решения является применение методов математического моделирования для количественной оценки разнородных характеристик механизмов защиты [4].

Следует отметить, что вопросы моделирования процессов защиты информации в финансовой сфере не являются новыми, их решению посвящен целый ряд основополагающих трудов [5, 6]. Вместе с тем незначительная глубина проработки в этих работах соответствий формализованного представления процессов искажения информации и формализованного представления процессов ее защиты от искажения не позволили достичь приемлемой адекватности математического представления исследуемых процессов и в полном объеме применить аппарат математического моделирования.

Это обусловило необходимость проработки вопросов формирования однозначных соответствий между формализованным представлением процессов искажения информации и формализованным представлением процессов ее защиты от такого рода угроз с целью адекватного математического представления исследуемых процессов и корректного использования существующего аппарата математического моделирования [7], а также обоснования показателя адекватности моделирования процессов защиты информации, от искажения учитывающего функциональные и информационные характеристики моделируемых процессов.

Несмотря на широкое использование методов теории моделирования в решении различных задач по исследованию проблем обеспечения целостности информации, специальные исследования, связанные с разработкой методов моделирования механизмов защиты информации от искажения в СДБО с целью адекватной оценки эффективности защиты носят крайне ограниченный характер.

С целью решения задачи математического моделирования механизмов защиты информации СДБО от искажения в интересах оценки эффективности этих механизмов определим соответствующий показатель как функциональный.

В качестве основания для определения такого показателя на основе множества $R = \{r_i \mid i = 1, 2, ..., |R|\}$ моделируемых функций механизмов защиты информации СДБО от искажения условимся использовать вероятность p оценки, как вероятность устранения неопределенности (энтропии) в функциональной интерпретации признаков искажения.

Исходя из этого адекватность оценки эффективности механизмов защиты информации СДБО от искажения соответствующими математическими моделями представим количеством информации, получаемой путем моделирования функций $\{r_i \mid i = 1, 2, ..., |R|\}$ защиты.

В зависимости от существующих в информатике теоретических направлений энтропия исследуемых процессов может быть определена через количество информации, получаемое от моделей этих процессов. Естественно, что более информативные модели будут иметь больший уровень адекватности. Из существующих в информатике вариантов интерпретации меры количества информации исследуемых процессов определим синтаксическую меру как меру, выраженную через энтропию [1].

Исходя из специфики информационных процессов в СДБО, реализуемых в условиях вероятностной интерпретации потока обслуживания клиентов, при решении сформулированной выше задачи диссертационного исследования будем пользоваться синтаксической мерой количества информации, представленной метрикой Шеннона [8].

Определение количества информации по Шеннону применительно к информационному процессу в СДБО формулируется следующим образом.

Для некоторого конечного множества функций $R = \{r_1, r_2, ..., r_{|R|}\}$ информационного процесса в СДБО, моделируемых с соответствующими вероятностями $p_1, p_2, ..., p_{|R|}$, $\sum_{i=1}^{|R|} p_i = 1$, количество информации, формируемой при моделировании одной функции $x_i \subset X$, , определяется изменением степени неопределенности при ее исследовании и равно:

$$q(R) = -\sum_{i=1}^{|R|} p_i \log_2 p_i.$$

Количество информации, формируемой при моделировании R функций, определяется согласно выражению:

$$q(R) = -R \cdot \sum_{i=1}^{|R|} p_i \log_2 p_i. \qquad (1)$$

Исходя из специфики механизмов защиты информации в СДБО от искажения, как объекта моделирования, задача математического моделирования такого рода механизмов в интересах оценки их эффективности в содержательном плане формулируется следующим образом.

Применительно к заданным условиям реализации информационных процессов в СДБО и используемом при этом оборудовании, способам несанкционированного доступа к информации СДБО с целью ее искажения и механизмам защиты информации от такого рода угроз, разработать совокупность математических моделей этих механизмов адекватно устанавливающих количественное значение показателя эффективности защиты информации в СДБО от искажения.

Формализовано задача математического моделирования механизмов защиты информации в СДБО от искажения в интересах оценки их эффективности представляется как задача выбора из множества вариантов $\{v_j, \mid v_j \in V\}$ моделирования рассматриваемых механизмов, варианта $v_{(м)}$, максимизирующего показатель (1).

Обозначив количество информации, формируемой при моделировании R параметров, как функцию v_j формально постановку задачи можно представить в виде:

$$q(R(v_{(м)})) = q(R(v_j)) \to \max. \qquad (2)$$
$$v_j \in V$$

Сформулированную задачу математического моделирования механизмов защиты информации в СДБО от искажения в интересах оценки эффективности рассматриваемых механизмов целесообразно решать путем представления в виде следующих последовательно решаемых задач:

– обоснование числа физически отражаемых параметров механизмов защиты информации в СДБО от искажения;

– разработка методики формирования множества моделируемых параметров рассматриваемых механизмов на основе физически отражаемых параметров;

– разработка математических моделей моделируемых параметров;

– численное доказательство критерия (2).

ЛИТЕРАТУРА

1. Информатика: учебник для высших учебных заведений МВД России. Том 1. Информатика: Концептуальные основы / В. А. Минаев, С. В. Скрыль, С. В. Дворянкин, Н. С. Хохлов [и др.]. – М.: Маросейка, 2008. – 464 с.

2. *Овчинский А. С.* Информационные воздействия и организованная преступность: курс лекций. – М.: ИНФРА-М, 2007. – 176 с.

3. Основы информационной безопасности: учебник для высших учебных заведений МВД России. / под ред. В. А. Минаева, С. В. Скрыля. – Воронеж: Воронежский институт МВД России, 2001. – 464 с.

4. Оценка защищенности компьютерной информации: пути решения проблемы / С. В. Скрыль, А. П. Курило [и др.]. // Интеллектуальные системы (INTELS' 2010): Труды Девятого международного симпозиума. – М.: МГТУ им. Н.Э. Баумана, 2010. – С. 564–566.

5. Обеспечение информационной безопасности бизнеса / А. П. Курило, С. Г. Антимонов, В. В. Андрианов [и др.]. – М.: БДЦ-пресс, 2005. — 512 с.

6. Аудит информационной безопасности. / А. П. Курило, С. Л. Зефиров, В. Б. Голованов. – М.: Издательская группа «БДЦ-пресс», 2006 – 304 с.

7. Моделирование систем: учебник для вузов – 3-е изд., перераб. и доп. / Б. Я. Советов, С. А. Яковлев. – М. : Высшая школа, 2001. – 343 с.

8. *Шеннон К.* Математическая теория связи // В сб.: Работы по теории информации и кибернетике. – М.: ИЛ, 1963.