УДК 001.2

А.В. Поляков
(МГТУ "Станкин"; e-mail: okcom@li.ru)

О НАУЧНЫХ НАПРАВЛЕНИЯХ РЕШЕНИЯ ПРОБЛЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Дан краткий обзор научных направлений, используемых при решении проблем информационной безопасности.
Ключевые слова: информационная безопасность, научные направления.

A.V. Polyakov

ABOUT SCIENCE DIRECTIONS OF SOLVING PROBLEMS OF INFORMATION SECURITY

Short review of science directions used in the solution problems of information security.
Key words: information security, science directions.

Статья поступила в редакцию Интернет-журнала 23 июня 2011 г.

По мнению исследователей [1], научные направления решения проблем информационной безопасности включают в себя такие ***математические методы,*** как теория линейного и целочисленного программирования, математическая логика, теория математической статистики и теория множеств, теория вычислительной сложности, теория графов и теория вероятностей, включая теорию случайных процессов, теория игр, разработка математических алгоритмов, теория нейронных сетей и проведение численных экспериментов.

Среди ***общенаучных методов*** специалисты выделяют системный подход, методы системного анализа и экспертных оценок, синтез [2]. При проведении исследования используются различные способы и методы моделирования: имитационное моделирование, построение математических моделей объектов информационной безопасности, методы объектно-ориентированного моделирования и теория моделирования дискретных систем.

При проведении исследований проблем информационной безопасности специалистами используются также технологии искусственного интеллекта и теория многоагентных систем, методология структурного анализа и проектирования, теория принятия решений и инженерия программного обеспечения [3].

Среди общих проблем обеспечения информационной безопасности исследователи выделяют повышение доступности, целостности и конфиденциальности информационных систем; совершенствование систем информационной безопасности; повышение эффективности функционирования информационных систем и защищённости информации; формулирование единых принципов построения системы информационной безопасности организации [4, 5].

Исследователи проблем информационной безопасности используют математические модели для оценки информационных рисков, информационных систем, угроз информационным системам, моделирование атак на информаци-

онную систему организации, построение моделей несанкционированного доступа [6]. Также используются линейные математические модели процессов, происходящих при нарушении правил обеспечения информационной безопасности; модели для выбора оптимальных систем защиты информации, анализа влияния внешних воздействий на информационную систему организации.

Большое внимание специалистов уделяется исследованию информационных рисков и угроз, включая управление информационными рисками, классификацию типов злоумышленников и шаблонов угроз, определение возможных угроз для информационной системы, управление рисками, анализ потенциальных уязвимостей, ошибок и угроз, аудит информационной безопасности для оценки вероятностей угроз [7].

Исследования технических аспектов информационной безопасности помогают находить уязвимости в системе и средствах защиты безопасности, выявлять недостатки политики безопасности организации.

Среди исследований, имеющих прикладное значение, специалисты выделяют методы оценки ущерба для организаций при нарушении конфиденциальности, целостности и доступности информации; разработку программных прототипов систем защиты информации и оценку существующих систем защиты информации; разработку систем фильтрации спама и учёт семантики сообщений электронной почты; разработку экспертных систем поддержки принятия решений. Также приводятся описания структур ресурсов и множества опасных состояний информационной системы; проводится оценка риска ресурсов и всей системы информационной безопасности; оцениваются вероятности отказов аппаратных средств и ошибок в программном обеспечении [8, 9]. Специалисты также предупреждают о возможностях использования программного обеспечения в преступных целях, получения несанкционированного доступа к ресурсам, а также путях обхода средств защиты информации; проводят анализ структур систем информационной безопасности и исследуют проблемы создания и поддержания автоматизированных систем информационной безопасности (функционирующих с меньшей долей участия человека) [10].

Существуют различные классификации ресурсов информационной системы организации. Отдельные исследователи разделяют ресурсы информационной системы на следующие категории, при взаимодействии которых формируется информационная система организации [11]:

- информационные ресурсы;
- физические ресурсы;
- программные ресурсы.

Информационные ресурсы включают в себя собственно информацию, хранящуюся в различном виде в организации. К ***физическим ресурсам*** относятся оборудование и аппаратные средства хранения, создания и передачи информации.

Исследователи выделяют различные примеры угроз информационной безопасности, среди которых: нарушение конфиденциальности, целостности, доступности информации; блокирование работы веб-серверов, рабочих станций и другого оборудования и программного обеспечения; уничтожение, кража

и внесение изменений в информацию; раскрытие или уничтожение информации. Также выделяют раскрытие, модификацию или уничтожение персональной или коммерческой информации; отказ и временную недоступность ресурса информационной системы; отсутствие или потерю резервной копии ресурса информационной системы [12].

Как считают специалисты [13], к проблемам информационной безопасности относится защищённость информации о сфере деятельности организации, информация об отделах и их количестве, данные о количестве сотрудников организации, данные о количестве и составе рабочих станций, локальных вычислительных сетях, серверах, коммутаторах и программном обеспечении.

Литература

1. ***Арьков П.А.*** Комплекс моделей для поиска оптимального проекта системы защиты информации // Известия ЮФУ. Технические науки. Тематический выпуск: "Информационная безопасность". Таганрог: Изд-во ТТИ ЮФУЮ, 2008, № 8 (85). С. 30-36.

2. ***Кустов Г.А., Зотова О.Ф.*** Управление рисками в добровольном медицинском страховании // Принятие решений в условиях неопределенности. Вопросы моделирования. Межвузовский научный сборник. Уфа: УГАТУ, 2007. С. 91-98.

3. ***Валеев С.С., Никитин А.П.*** Многоуровневая система фильтрации спама на основе технологий искусственного интеллекта // Вестник УГАТУ, т. 11, № 1 (28), 2008. С.215-219.

4. ***Шахов В.Г., Фофанов А.В.*** Идентификация пользователей в защищённой системе хранения информации // Автоматика, связь, информатика, 2002, № 1.

5. ***Кустов Г.А.*** Задача управления информационными рисками компании добровольного медицинского страхования // Вестник УГАТУ, серия "Управление, вычислительная техника и информатика", т. 9, № 4 (22), 2007. Уфа: УГАТУ. С. 77-84.

6. ***Фофанов А.В.*** Анализ безопасности корпоративных сетей с использованием алгоритма перебора L-классов // Сборник научных трудов "Проблемы информационной безопасности в системе высшей школы". М.: МИФИ, 2005.

7. ***Зотова О.Ф., Зиборов Г.С., Кустов Г.А.*** Методы принятия решений в задачах управления риском на примере исследования риска неэффективного лечения в лечебно-профилактическом учреждении // Управление риском, № 4 (44), 2007. М.: Изд-во "Анкил". С. 62-66.

8. ***Никитин А.П.*** Интеллектуальная система автоматической классификации // Материалы Всероссийской молодёжной научной конференции, посвящённой 75-летию УГАТУ, т. 3. Уфа: УГАТУ, 2007. С. 18-19.

9. ***Королева Н.А., Тютюнник В.М.*** Экспертная система поддержки принятия решений по обеспечению информационной безопасности организации. Тамбов, М., С.-Пб., Баку, Вена: Изд-во "Нобелистика", 2006.

10. ***Шахов В.Г., Фофанов А.В.*** Алгоритм приближенного решения задачи целочисленного квадратичного программирования, связанный с оценкой безопасности информационного комплекса // Безопасность информационных технологий. Вып. 1. М.: МИФИ, 2004.

11. ***Кустов Г.А., Зотова О.Ф.*** Организация и защита данных в системах аналитической поддержки деятельности компании добровольного медицинского страхования // "Принятие решений в условиях неопределенности", "Вопросы моделирования". Межвузовский научный сборник. Уфа: УГАТУ, 2006. С. 56-61.

12. ***Арьков П.А.*** Построение модели процесса реализации угрозы в информационной системе на основе сетей Петри // Обозрение прикладной и промышленной математики, 2008, т. 15. Вып. 4. М.: Редакция журнала "ОПиПМ", 2008. С. 655-656.

13. ***Шахов В.Г., Фофанов А.В.*** Экспериментальный анализ алгоритмов решения задачи целочисленного линейного программирования при оценке безопасности информационного комплекса // Безопасность информационных технологий. Вып. 3. М.: МИФИ, 2003.