



ДЛЯ ВУЗОВ

В.И. Васильев

ИНТЕЛЛЕКТУАЛЬНЫЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Издание третье, стереотипное

Допущено Учебно-методическим объединением по образованию в области информационной безопасности в качестве учебного пособия для студентов высших учебных заведений, обучающихся по специализациям специальности «Комплексное обеспечение информационной безопасности автоматизированных систем»

**МОСКВА
«ИННОВАЦИОННОЕ МАШИНОСТРОЕНИЕ»
2021**

УДК 681.5:004(07)
ББК 32.81:32.97я7
В19

Рецензенты:

кафедра программирования и вычислительной техники
(Башкирский государственный педагогический университет им. М. Акмуллы),
зав. кафедрой, д-р физ.-мат. наук, профессор *Р.М. Асадуллин*;
д-р техн. наук, профессор *С.С. Валеев*,
д-р техн. наук, профессор *А.В. Мельников*

Васильев В.И.

В19 Интеллектуальные системы защиты информации: учебное
пособие. 3-е изд., стереотип. М.: Инновационное машинострое-
ние, 2021. 172 с.

ISBN 978-5-907104-99-0

Рассмотрены основы построения интеллектуальных систем защиты информа-
ции в корпоративных информационных системах. Особое внимание уделено по-
строению биометрических систем идентификации личности, систем обнаруже-
ния и предотвращения вторжений, анализа и управления информационными рис-
ками. Изложены современные подходы к созданию данного класса систем с ис-
пользованием методов теории нейронных сетей, искусственных иммунных систем,
нечетких когнитивных моделей.

Предназначено для студентов высших учебных заведений, обучающихся по
специализациям специальности «Комплексное обеспечение информационной
безопасности автоматизированных систем».

УДК 681.5:004(07)
ББК 32.81:32.97я7

ISBN 978-5-907104-99-0

© Издательство "Инновационное
машиностроение", 2021
© Васильев В.И., 2021

Перепечатка, все виды копирования и воспроизведения материалов,
опубликованных в данной книге, допускаются только с разрешения
издательства и со ссылкой на источник информации

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ	5
ГЛАВА 1. ОСНОВЫ ПОСТРОЕНИЯ ИНТЕЛЛЕКТУАЛЬ- НЫХ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ	9
1.1. Системные принципы защиты информации.....	9
1.2. Интегрированные системы защиты информации.....	12
1.3. Интеллектуализация систем защиты информации.....	20
Контрольные вопросы	33
ГЛАВА 2. БИОМЕТРИЧЕСКИЕ СИСТЕМЫ ИДЕНТИФИКАЦИИ ЛИЧНОСТИ.....	34
2.1. Биометрические технологии: классификация, сравнительные характеристики	34
2.2. Постановка задачи распознавания образов. Построение решающего правила.....	45
2.3. Нейросетевые алгоритмы биометрической идентификации	52
2.4. Нейросетевая реализация биометрических систем идентификации с криптозащитой	61
2.5. Биометрические системы идентификации на основе нечетких экстракторов	67
Контрольные вопросы	73
ГЛАВА 3. НЕЙРОСЕТЕВЫЕ СИСТЕМЫ ОБНАРУЖЕНИЯ АТАК	74
3.1. Актуальность проблемы, пути ее решения	74
3.2. Нейросетевые СОА на основе сигнатурного анализа ...	81
3.2.1. Обнаружение атаки <i>SYN Flood</i>	82
3.2.2. Построение нейронечеткого классификатора.	89
3.2.3. Обнаружение сетевых атак с помощью модулярной НС	94
3.3. Обнаружение аномалий с помощью НС. Интегрированные системы обнаружения атак.....	99
Контрольные вопросы	111

ГЛАВА 4. ИНТЕЛЛЕКТУАЛЬНЫЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ МЕХАНИЗМОВ ИСКУССТВЕННЫХ ИММУННЫХ СИСТЕМ	112
4.1. Роль и место искусственных иммунных систем в задачах защиты информации	112
4.2. Естественная иммунная система: механизмы функционирования	115
4.3. Обнаружение аномалий процесса на основе механизмов иммунной системы	119
4.4. Практические примеры реализации систем обнаружения аномалий на основе технологий искусственных иммунных систем	126
4.5. Системы антивирусной защиты на основе искусственных иммунных систем	133
Контрольные вопросы	137
ГЛАВА 5. АНАЛИЗ И УПРАВЛЕНИЕ ИНФОРМАЦИОН- НЫМИ РИСКАМИ НА ОСНОВЕ НЕЧЕТКИХ КОГНИТИВНЫХ МОДЕЛЕЙ	138
5.1. Состояние вопроса	138
5.2. Методика когнитивного моделирования сложных систем	141
5.3. Анализ информационных рисков с помощью нечетких когнитивных карт	145
5.4. Инструментальное средство анализа и управления информационными рисками	152
Контрольные вопросы	157
ЗАКЛЮЧЕНИЕ	158
СПИСОК СОКРАЩЕНИЙ	160
СПИСОК ЛИТЕРАТУРЫ	161

*Миссия обеспечения
информационной безопасности
трудна, во многих случаях
невыполнима, но всегда
благородна
В. А. Галатенко*

*Я пришел к выводу, что наилучшими
экспертами в области безопасности
являются люди, исследующие
несовершенство защитных мер
Б. Шнайер «Секреты и ложь»*

ВВЕДЕНИЕ

Современный мир – мир информационных технологий. Информация сегодня является самым ценным и востребованным товаром. Жизнь практически любой организации (предприятия, государственного учреждения, учебного заведения, банка и т.д.) в значительной степени зависит от того, насколько эффективно и устойчиво функционирует ее информационная система, насколько надежно защищены ее информационные ресурсы по отношению к действию возможных внешних и внутренних угроз.

Спектр угроз информационной безопасности сегодня значительно расширился – это не только возможность получения несанкционированного доступа к секретной или конфиденциальной информации, хакерские атаки или вирусы, но и тщательно спланированные компьютерные преступления с целью материальной наживы или нанесения материального и морального ущерба частным лицам и организациям, кибертерроризм, подготовка к широкомасштабным информационным войнам. Все больший удельный вес (по различным оценкам, до 60 – 70 %) приобретают внутренние угрозы, связанные с действиями так называемых «инсайдеров» – штатных сотрудников организации, умышленно или ошибочно превышающих свои полномочия при работе с информацией, следствием чего является ее утечка, несанкционированная модификация или уничтожение. Повсеместное использование Интернета в качестве глобальной сети, объединяющей сотни

миллионов компьютеров и пользователей по всему миру, лишь усугубляет ситуацию, поскольку получить доступ к ресурсам любого (даже защищенного) компьютера, подключенного к Интернету, теоретически можно с любого другого компьютера, расположенного в сети.

Сложность решения проблемы информационной безопасности состоит и в том, что лица, принимающие решения (руководители высшего звена, специалисты по защите информации, системные администраторы, рядовые пользователи), вынуждены действовать в условиях наличия факторов неопределенности, связанных с неточностью и недостоверностью исходных данных, неполнотой знаний о рассматриваемом объекте, неоднозначностью принимаемых решений (известный специалист в области искусственного интеллекта А. С. Нариньяни назвал эти факторы НЕ-факторами [1]). Попытки автоматизации отдельных функций защиты информации с помощью соответствующих программно-аппаратных средств (системы обнаружения атак, межсетевые экраны, сканеры уязвимости и т.п.) в целом являются довольно ограниченными и, в силу указанных выше причин, не позволяют решать поставленные задачи в полном объеме.

Возможный выход из сложившейся ситуации состоит в применении известного в кибернетике принципа «необходимого разнообразия» У. Р. Эшби [2], суть которого заключается в том, что для успешного функционирования системы сложность ее управляющей части (т.е. многообразие выполняемых ею функций и методов их реализации) должна соответствовать сложности управляемого объекта и той среды, в которой он функционирует. Применительно к сфере информационной безопасности, это означает, что защита должна быть адекватна нападению, т.е. используемые средства защиты информации должны обеспечить своевременное обнаружение и достоверное распознавание различных видов угроз с учетом возможного места и характера их проявления, квалификации злоумышленника, потенциальных уязвимостей информационной системы и т.д., а также предотвращение или локализацию воздействия этих угроз на защищаемую информацию в условиях действия указанных выше факторов неопределенности.

В последние годы большое внимание специалистов привлекает направление, связанное с интеллектуализацией систем защиты ин-

формации, т.е. с надделением их такими функциями, которые обычно выполняет высококвалифицированный оператор (эксперт), привлекая для этого свои профессиональные знания и опыт. Решаемые им задачи в процессе выполнения этих функций относятся к классу плохо-формализуемых (неструктурированных) задач, составляющих предмет изучения и применения методов искусственного интеллекта.

Существуют различные определения искусственного интеллекта (ИИ). По мнению профессора Массачусетского технологического института (США) Марвина Мински, одного из пионеров ИИ, *искусственный интеллект* (англ. – *Artificial Intelligence*) – это «наука, которая позволяет машинам делать такие вещи, которые при их выполнении людьми требуют интеллекта». Известный французский ученый Жан Луи Лорьер в своей книге [3] дает более развернутое определение: *искусственный интеллект* – это «область исследований, в которой главным желанием исследователей является стремление понять, как система обработки информации, будь то человек или машина – способна воспринимать, анализировать, передавать и обобщать то, чему ее обучают, и с помощью этих данных исследовать конкретные ситуации и находить решения задач».

Область исследований искусственного интеллекта чрезвычайно широка и охватывает такие направления /методы, как:

- искусственные нейронные сети (НС);
- системы на основе нечеткой логики (НЛ);
- генетические алгоритмы (ГА);
- экспертные системы (ЭС);
- мультиагентные системы (МАС);
- искусственные иммунные системы (ИИС).

Не останавливаясь подробно на содержании указанных направлений (более детальную информацию читатель может найти, например, в [3 – 10]), рассмотрим ниже лишь те из задач, относящиеся к области защиты информации (естественно, это далеко не полный их перечень!), которые эффективно решаются с помощью указанных методов для обеспечения эффективной защиты информации в условиях неопределенности. Поскольку затронутая проблема является очень обширной, авторы были вынуждены ограничиться рассмотрением лишь некоторых «узловых точек» этой проблемы, с целью привлечь

внимание читателя к данной проблематике и пробудить в нем интерес к более глубокому ее изучению. В основу пособия положен анализ большого числа источников, на которые по тексту сделаны ссылки, включая труды общепризнанных авторов в области ИИ, а также современные научные публикации, в том числе принадлежащие автору. Изложение сопровождается большим числом примеров (часть из которых носит оригинальный характер), иллюстрирующих особенности реализации соответствующих методов ИИ в системах защиты информации.

Для того чтобы не перегружать основной текст множеством определений, автор рекомендует читателям обратиться к ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения» (см. также [11]).

Учебное пособие предназначено для слушателей и студентов, обучающихся по специализации специальности «Комплексное обеспечение информационной безопасности автоматизированных систем», а также преподавателям при проведении лекционных и индивидуальных занятий по курсу «Искусственный интеллект в системах защиты информации». Материалы, изложенные в пособии, могут быть также полезны аспирантам, научным работникам и специалистам при проведении научных исследований и в практической работе.