ISSN 2658-5014 (Print) СИИТ ISSN 2686-7044 (Online)
2020. Т. 2, № 2 (4). С. 43–50 СИСТЕМНАЯ ИНЖЕНЕРИЯ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ http://siit.ugatu.su

УДК 004.056

ПРИМЕНЕНИЕ МЕТОДОВ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ЗАДАЧАХ ЗАЩИТЫ ИНФОРМАЦИИ (ПО МАТЕРИАЛАМ НАУЧНОЙ ШКОЛЫ УГАТУ)

В. И. Васильев[1], В. М. Картак[2]

[1] vasilyev@ugatu.ac.ru, [2]kvmail@mail.ru

ФГБОУ ВО «Уфимский государственный авиационный технический университет» (УГАТУ)

Поступила в редакцию 19 октября 2020 г.

Аннотация. Проблема защиты информации сегодня приобретает особую остроту и актуальность в связи с активным внедрением все усложняющихся цифровых информационных технологий и методов искусственного интеллекта в сферу промышленного производства и оказания услуг и, как следствие, возрастанием интереса к этим информационным ресурсам со стороны всевозможных внешних и внутренних злоумышленников и ростом числа инцидентов и масштабов потерь в результате успешной реализации целенаправленных атак. В данной обзорной статье приведены результаты исследований в области информационной безопасности, выполненных в рамках научной школы УГАТУ с начала 2000-х годов. Подчеркивается особая роль и значимость применения для решения этих задач технологий интеллектуального анализа данных, показаны преимущества и перспективы их практического использования.

Ключевые слова: защита информации; информационная безопасность; интеллектуальный анализ данных; анализ рисков; аудит информационной безопасности.

ВВЕДЕНИЕ

Современный этап развития мировой экономики неразрывно связан с повсеместным внедрением цифровых информационных технологий во все отрасли народного хозяйства, комплексной автоматизацией систем контроля и управления сложными технологическими процессами, переходом к безлюдным роботизированным производствам, все более широким использованием методов искусственного интеллекта. Эти тенденции лежат в основе создания 4-го промышленного уклада (Industry 4.0), Промышленного Интернета вещей (Industrial Internet of Things), «умных» предприятий (Smart Factory) и городов (Smart City). В то же время специалисты отмечают резкий рост числа и масштабов организованных цифровых атак (targeted attacks), направленных на информационные ресурсы указанных объектов и приводящих к серьезным авариям, разрушениям, остановке производства и т.п. Этим объясняется повышенное внимание к необходимости надежной защиты данных объектов и в первую очередь, объектов, обладающих повышенной потенциальной опасностью для жизни и здоровья людей, состояния окружающей среды, по отношению к возможным внешним и внутренним угрозам. Сегодня активно разрабатывается законодательная и нормативно-методическая база обеспечения кибербезопасности (информационной безопасности) автоматизированных систем управления сложными технологическими процессами и производствами (АСУ ТП). Решение указанных вопросов находится в центре внимания руководителей и специалистов крупных предприятий, образовательных и научных учреждений, компаний-разработчиков программно-аппаратных комплексов и систем защиты информации.

Предпосылкой становления в УГАТУ новой научной школы в области информационной безопасности (ИБ) явилась созданная в 70 – 80-х гг. уфимская научная школа в области надежности и безопасности функционирования сложных организационно-технических систем (проф. Н. К. Зайнашев, проф. И. Ю. Юсупов, проф. И. М. Хомяков, проф. Ф. А. Шаймарданов, проф. Ю. М. Гусев, проф. Б. Г. Ильясов). В рамках этой школы установились тесные научные связи и контакты с ведущими вузами и академическими

Работа поддержана грантами РФФИ 20-08-00668 А, РФФИ- 19-07-00895 А

организациями, в первую очередь, с Ленинградской (позже – Санкт-Петербургской) научной школой в области надежности и безопасности (проф. Р. М. Юсупов, проф. А. М. Половко, проф. А. Г. Варжапетян, проф. Д. В. Гаскаров). По данной тематике, связанной с проектированием высоконадежных систем управления сложными техническими объектами, систем контроля, диагностики и поддержки принятия решений в критических ситуациях, в УГАТУ были успешно защищены докторские диссертации В. Г. Крымского, В. Н. Ефанова, В. В. Миронова, Н. И. Юсуповой, С. В. Павлова, В. Е. Гвоздева, Л. Р. Черняховской, К. Ф. Тагировой, И. У. Ямалова и др., а также большое количество кандидатских диссертаций.

Формально начало научной школы УГАТУ в области информационной безопасности связано с открытием в УГАТУ в 1995 г. на факультете информатики и робототехники (ФИРТ) кафедры вычислительной техники и защиты информации (ВТиЗИ, зав. кафедрой с 1995 г. по 2017 г. – д.т.н., проф. В.И. Васильев, с 2017 г. – д.ф.-м.н., проф. В.М. Картак), на которой на одной из первых в стране начали готовить дипломированных специалистов по защите информации. Начиная с 2000 г., на кафедре ВТиЗИ началась подготовка аспирантов в области ИБ из числа выпускников кафедры.

С первых лет существования кафедры ее коллектив принимает активное участие в проведении научных исследований в области разработки интеллектуальных методов и систем защиты информации, которые условно можно отнести к следующим трем направлениям:

- управление защитой информации (ЗИ) в корпоративных информационных системах (КИС) с использованием интеллектуальных технологий обработки данных;
- интеллектуальные системы обнаружения и предотвращения атак в компьютерных системах и сетях;
- интеллектуальные системы поддержки принятия решений (СППР) при проведении аудита информационной безопасности КИС на основе анализа и управления рисками.

МЕТОДЫ УПРАВЛЕНИЯ ЗИ В КИС

В качестве важного шага в рамках первого научного направления следует отметить защиту докторской диссертации И. В. Машкиной [1], посвященной разработке общей методологии проектирования интеллектуальных систем защиты информации (СЗИ) в КИС. В этой работе предложен системный подход к построению архитектуры системы управления ЗИ в сегменте КИС, включающей в себя подсистемы оперативного и организационно-технического управления, обеспечивающей формирование управляющих воздействий на основе использования интеллектуальных технологий. Предложена концепция построения модели угроз нарушения информационной безопасности, основанная на описании угроз с помощью пространственных графовых моделей и деревьев угроз, а также модель противодействия угрозам ИБ в сегменте КИС, основанная на выборе рационального варианта реагирования с использованием численной оценки вероятности реализации атак на основе нечеткой логики. Разработан метод формирования рационального модульного состава средств ЗИ на основе морфологического подхода и метода анализа иерархий. Предложен метод и алгоритм оценки уровня защищенности СЗИ на основе численной оценки вероятностей уязвимостей с учетом технических характеристик средств защиты и механизма нечеткого логического вывода. Разработаны инструментальные программные комплексы для интеллектуальной поддержки принятия решений в СЗИ, реализующие предложенные методы и алгоритмы управления ЗИ.

Особенности построения пространственных графовых моделей угроз как каналов несанкционированного доступа, утечки информации и деструктивного воздействия на информационную среду рассмотрены в [2]. Здесь же представлены методы поддержки принятия решений по организационно-техническому управлению ЗИ, включая задачу выбора состава средств ЗИ и его изменения в процессе эксплуатации, а также решений, связанных с выбором варианта оперативного управления в случае возникновения потенциально опасных ситуаций на основе правил нечеткой логики. Разработаны программные модули для подсистем, осуществляющих поддержку принятия соответствующих решений в составе интеллектуальной СЗИ.

В работе [3] рассмотрены возможные подходы к организации ЗИ в распределенных информационных системах предприятий. Предложена оригинальная концепция построения автоматизированной СЗИ виртуального предприятия. Разработаны методы оптимизации процессов ЗИ в информационной системе (ИС) виртуального предприятия (анализ рисков, выбор конфигурации СЗИ, принятие решений при оперативном управлении ЗИ). Предложена методика проектирования автоматизированной СЗИ

виртуального предприятия в классе многоагентных систем, включающая в себя в качестве основных этапов анализ рисков на основе метода анализа иерархий, оценку требуемого уровня защищенности информации с применением нечеткого логического вывода, применение разработанных автором инструментальных программных средств на всех этапах проектирования.

Задачи интеллектуальной поддержки принятия решений по управлению ЗИ в распределенных информационно-управляющих системах (ИУС) на примере региональной системы межведомственного электронного взаимодействия (РСМЭВ) Республики Башкортостан рассмотрены в работе [4]. Автором разработана онтология предметной области и функциональные модели SIEM-системы на основе SADT-методологии и IDEF-технологий, предложен метод и алгоритм оценки защищенности ИС на основе правил нечеткой логики с учетом возможной корреляции событий ИБ в ИС. Разработана методика и алгоритм оценки информационных рисков в РСМЭВ на основе аппарата нечетких когнитивных карт с целью анализа текущего уровня защищенности РСМЭВ и выбора необходимых контрмер по противодействию основным угрозам в РСМЭВ.

Особенности организации управления ЗИ в системе электронной торговой площадки (ЭТП) исследуются в работе [5]. Разработана модель угроз в ИС ЭТП. Предложен метод выбора комплекса средств ЗИ для ИС ЭТП, обеспечивающего нейтрализацию актуальных угроз ИБ в ИС ЭТП. Предложена методика формализации правил взаимодействия информационных субъектов и объектов в ИС ЭТП, предназначенных для используемой в ИС ЭТП конфигурации средств ЗИ. Разработана архитектура системой управления ЗИ в ИС ЭТП, а также программное обеспечение для автоматизации выбора модульного состава СЗИ и процесса формирования политики разграничения доступа.

МЕТОДЫ ОБНАРУЖЕНИЯ АТАК В КОМПЬЮТЕРНЫХ СИСТЕМАХ

Значительное количество работ посвящено вопросам повышения эффективности систем обнаружения атак (СОА) за счет применения современных методов и технологий интеллектуального анализа данных. Так, работа [6] посвящена разработке и исследованию СОА на ИС (www-сервер) с использованием нейросетевых технологий. Произведен выбор программно-аппаратной платформы для реализации исследовательского прототипа СОА. В качестве используемого метода обнаружения атак предложен комбинированный метод, основанный на объединении методов поиска сигнатур и обнаружения аномалий. В качестве базовой топологии нейронной сети (НС) используется гибридная НС встречного распространения Counter Propagation. Приведены рекомендации по выбору структуры нейросетевой СОА на базе www-сервера Apache. Представлены результаты экспериментальных исследований и оптимизации параметров обучения НС, выполненных с применением нейросетевого симулятора SNNS в ОС UNIX, подтверждающих более высокую эффективность предложенного способа реализации нейросетевой СОА по сравнению с существующими СОА.

В работе [7] исследуется способ построения интеллектуальной СОА на основе технологии искусственных иммунных систем с использованием принципа распознавания «свой-чужой». В отличие от классического метода обнаружения атак, основанного на использовании конечного множества сигнатур («шаблонов») атак, в данном случае обеспечивается возможность распознавания новых, ранее неизвестных системе атак. Предложен усовершенствованный алгоритм генерации детекторов СОА с помощью генетического алгоритма, позволяющий сократить время обучения и повысить эффективность организации активного аудита ИС.

Задача построения интеллектуальной системы обнаружения атак на основе имитационного моделирования с использованием нечетких когнитивных карт обсуждается в работе [8]. В основу выбора архитектуры СОА и алгоритмов принятия решений заложены принципы многоагентного подхода и прогнозирования рисков ИБ в режиме реального времени с помощью нечеткой когнитивной динамической модели ИС. Центральным элементом СОА при этом является глобальная база знаний, содержащая информацию об известных видах атак, методах противодействия вторжениям, архив событий системы, а также выступающая в качестве арбитра (супервизора) при организации взаимодействия между различными агентами, входящими в состав СОА (агенты-сенсоры, агенты-локальные СОА и т.д.). Приведены результаты тестирования разработанного исследовательского прототипа СОА, подтверждающие значительное уменьшение числа ошибок первого и второго рода по сравнению с существующими аналогами.

Работа [9] посвящена разработке многоуровневой многоагентной системы обнаружения и фильтрации нежелательных электронных сообщений (спама). Предложена оригинальная концепция построения архитектуры иерархической

многоуровневой системы защиты информации, обрабатываемой электронными почтовыми системами, от вредоносного воздействия спама в организации. Предложен эффективный алгоритм классификации электронных сообщений на основе когнитивного подхода и нейросетевого классификатора. Разработан программный прототип многоагентной системы противодействия распространению спама в организации, позволяющий посредством использования системы правил в базе знаний эффективно решать задачу классификации поступающих электронных сообщений на различных уровнях иерархии организации.

Актуальные вопросы, связанные с обнаружением возможных аномалий в поведении вычислительных процессов микроядерных операционных систем (МОС) реального времени, обсуждаются в работе [10]. Разработана модель вычислительных процессов в МОС на основе сбора статистики о штатном поведении вычислительных процессов. Предложен метод и нейросетевые алгоритмы обнаружения аномального поведения вычислительных процессов в МОС, включая выявление новых типов атак с неизвестными сигнатурами. Разработан исследовательский прототип нейросетевой системы обнаружения аномального поведения вычислительных процессов в МОС, реализующий функции сбора статистической информации о поведении вычислительных процессов и классификацию состояний на основе самообучаемой нейронной сети.

Задача обнаружения вредоносных интернет-страниц с использованием методов машинного обучения решается в работе [11]. Произведен анализ существующих экземпляров вредоносных интернет-приложений как программных артефактов на основе вычисления статистических показателей их элементов. Разработана модель интернет-страницы на основе формальных языков, отличающаяся представлением интернет-страницы в виде вектора в n-мерном пространстве признаков. Разработаны и исследованы алгоритмы обнаружения вредоносных интернет-страниц на основе технологий машинного обучения (метод логистической регрессии, нейронные сети, машина опорных векторов, искусственные иммунные системы). Проведено исследование модели иммунной сети для решения задачи обнаружения вредоносных интернет-страниц, показана эффективность применения вредоносных интернет-приложений в дополнение к существующим антивирусным сканерам.

Вопросы применения технологий интеллектуального анализа данных для решения задачи обнаружения атак в локальных беспроводных сетях обсуждаются в работе [12]. Рассмотрены особенности функционирования локальных беспроводных сетей организации с точки зрения их защищенности, возможных угроз и уязвимостей, методов ЗИ. Разработаны алгоритмы обнаружения атак в беспроводной сети на основе построения классификатора с использованием ансамбля методов машинного обучения (нейронные сети, машина опорных векторов, метод k-ближайших соседей, деревья решений). Предложена архитектура интеллектуальной СОА, разработано программное обеспечение, проведены вычислительные эксперименты по оценке эффективности предложенных алгоритмов обнаружения атак с использованием модифицированной базы сигнатур NSL-KDD 2009.

Работа [13] посвящена исследованию методов и алгоритмов обнаружения вредоносных программ в мобильных приложениях на примере ОС Android. Автором проведен анализ защищенности ОС Android, встроенных и внешних средств ЗИ, структуры прикладных программ, приведен перечень возможных угроз и уязвимостей ОС. Предложены алгоритмы обнаружения вредоносных программ в ОС, основанные на применении технологий интеллектуального анализа данных (нечеткая логика, нейронные сети, машина опорных векторов). Предложена архитектура интеллектуальной системы обнаружения вредоносных программ, разработано программное обеспечение исследовательского прототипа системы обнаружения вредоносных программ в ОС для мобильных устройств Android.

МЕТОДЫ ППР ПРИ ПРОВЕДЕНИИ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КИС

Третья группа работ связана с обеспечением автоматизированной интеллектуальной поддержки принятия решений (ППР) на этапе проведения аудита ИБ и анализа рисков КИС. Так, работа [14] посвящена разработке автоматизированной системы анализа защищенности корпоративной вычислительной сети (КВС) с использованием технологий многоагентных систем. Разработана модель представления знаний о КВС, средствах и системах анализа ее защищенности в виде онтологии предметной области. Предложена формализованная процедура анализа защищенности КВС, разработан метод повышения ее эффективности на основе оценок используемых средств анализа защищенности. Разработана динамическая модель процедуры анализа защищенности КВС на основе сетей Петри, предложен эффективный метод динамического

распределения вычислительных ресурсов узлов КВС в процессе проведения анализа ее защищенности на основе многоагентного подхода. Разработан программный прототип автоматизированной системы анализа защищенности КВС.

Исследованию процессов анализа и управления информационными рисками с использованием нечетких карт (НКК) на примере высшего учебного заведения посвящена работа [15]. В ней разработаны системные модели процесса оценки уровня ИБ вуза, показаны преимущества использования нечеткого когнитивного моделирования для целей анализа и управления рисками ИБ. Приведена формализованная методика анализа и управления информационными рисками вуза с применением НКК. Предложена программная реализация процедуры моделирования задачи оценки и управления информационными рисками, а также структура интеллектуальной системы поддержки принятия решений (СППР) по анализу и управлению рисками ИБ вуза.

Решение задачи управления информационными рисками организации с применением логико-вероятностного метода (ЛВМ) на примере страховой компании (СК) добровольного медицинского страхования (ДМС) рассматривается в работе [16]. На основе разработанной автором функциональной модели процесса управления информационными рисками СК ДМС предложена методика количественной оценки рисков, учитывающая различную степень детализации опасных состояний ИС в зависимости от их значимости на основе алгоритма нечеткой логики, карты рисков и логико-вероятностного подхода. Поставлена и решена задача определения структуры ущерба компании при нарушении конфиденциальности информации. Предложен метод формирования эффективного набора контрмер на основе ЛВМ с использованием иерархического перебора допустимых альтернатив. Разработано программное обеспечение системы управления информационными рисками, позволяющее осуществлять поддержку основных этапов риск-анализа в процессе управления рисками ИБ организации.

Вопросам применения нечетких когнитивных моделей для оценки рисков нарушения ИБ посвящена работа [17]. Автором разработана концептуальная модель преднамеренных угроз на основе построения НКК, предполагающая визуализацию путей распространения угроз в инфраструктуре ИС с помощью матриц угроз, устанавливающих взаимосвязь между каждым источником и объектом атаки. Предложен метод оценки рисков ИБ в локальных сегментах ИС и в ИС в целом с помощью НКК с учетом приведенных в открытых базах данных уязвимостей компонентов инфраструктуры и средств ЗИ, позволяющий оценить влияние архитектуры сети на значения рисков ИБ, сравнить эффективность различных наборов средств защиты на стадии эксплуатации и при проектировании СЗИ. Разработан метод количественной оценки ценности информационных активов локальных сетевых сегментов, а также программный комплекс автоматизированной оценки рисков нарушения ИБ, реализующий предложенные модели и методы.

В работе [18] предложен алгоритм контроля целостности результатов измерений технологических параметров промышленных объектов, основанный на использовании метода FDI (Fault Centric Security) и концепции DCS (Data Centric Security). Разработана нейросетевая модель оценки расхода жидкости в трубопроводе в процессе транспортировки нефти. Представлена методика и процедура оценки потенциального ущерба с использованием модели «осведомленность-эффективность». Предложены рекомендации по применению предложенных решений, позволяющих повысить уровень защищенности результатов измерений и уменьшить потенциальный ущерб от их возможной несанкционированной модификации.

Разработке моделей и алгоритмов анализа информационных рисков при проведении аудита ИБ в системе облачных вычислений (СОбВ) посвящена работа [19]. Автором проведен анализ возможных угроз нарушения ИБ в СОбВ; разработана модель преднамеренных целенаправленных угроз ИБ, основанная на построении НКК с учетом особенностей инфраструктуры СОбВ. Предложена модель политики ИБ и методика разработки частной политики безопасности СОбВ, основанной на использовании ролевой модели разграничения доступа. Разработан метод проведения экспертного аудита ИБ на основе оценки оперативного значения риска нарушения ИБ с использованием нейронной сети. Разработана модель программного средства проведения аудита ИБ СОбВ и программный модуль для автоматизации процесса проведения аудита ИБ с учетом результатов оценки показателей риска.

В работе [20] рассмотрена задача анализа и управления рисками ИБ при проведении аудита безопасности информационных систем персональных данных (ИСПДн). Разработана системная и онтологическая модель процесса аудита ИБ ИСПДн. Предложена методика комплексной оценки уровня защищенности ИСПДн на основе построения и анализа профиля защиты ИСПДн. Предложен алгоритм оценки рисков ИБ ИСПДн

на основе модульной нечеткой нейронной сети. Рассмотрен алгоритм оптимизации выбора средств защиты персональных данных с использованием модели Клементса-Хоффмана. Приведены результаты применения предложенной методики и алгоритмов анализа и управления рисками ИБ для ИС медицинского учреждения.

В работе [21] была предложена математическая модель построения системы безопасности помещений. На базе линейно-целочисленного программирования предложен метод нахождения оптимального размещения средств обеспечения безопасности.

Дополнительную информацию о результатах рассмотренных выше исследований можно найти в учебных пособиях [22, 23].

ЗАКЛЮЧЕНИЕ

Многообразие методов и технологий искусственного интеллекта открывает практически неограниченные возможности для расширения спектра решаемых задач ЗИ, создания новых поколений средств и систем ЗИ, обладающих повышенной эффективностью функционирования в условиях неопределенности (агрессивная внешняя среда, изменения конфигурации ИС и ее компонентов, наличие человеческого фактора и т.д.). Совместное применение (комплексирование) различных технологий искусственного интеллекта в рамках единой гибридной СЗИ (так называемая концепция «мягких вычислений») обеспечивает при этом дополнительный синергетический эффект, сохраняя положительные качества каждой из используемых технологий.

За 25 лет своего существования коллективу кафедры удалось создать прочный фундамент динамично развивающейся научной школы в области ИБ, результаты деятельности которой приобретают в наши дни особую актуальность в свете современных трендов создания в нашей стране успешной цифровой экономики.

СПИСОК ЛИТЕРАТУРЫ

1. **Машкина И. В.** Управление защитой информации в сегменте корпоративной информационной системы на основе интеллектуальных технологий / Дисс. … д.т.н. по спец-ти 05.13.19 (науч. конс. – Гузаиров М.Б.). Уфа: УГАТУ, 2009. **[** I. V.Mashkina Information security management in the segment of a corporate information system based on intelligent technologies / Diss. ... Doctor of Technical Sciences in the specialty 05.13.19. - Ufa: USATU, 2009. **]**

2. **Рахимов Е. А.** Модели и методы поддержки принятия решений в интеллектуальной системе защиты информации / Дисс. … к.т.н. по спец-ти 05.13.19 (науч. рук. – Машкина И.В.). Уфа: УГАТУ, 2006. **[** E. A. Rakhimov Models and methods of decision support in an intelligent information protection system / Diss. ... Ph.D. in the specialty 05.13.19. Ufa: USATU, 2006. **]**

3. **Погорелов Д. Н.** Защита информационных ресурсов предприятия на основе многоагентной технологии / Дисс. … к.т.н. по спец-ти 05.13.19 (науч. рук. – Валеев С.С.). Уфа: УГАТУ, 2006. **[** D. N. Pogorelov Protection of information resources of an enterprise based on multi-agent technology / Diss. ... Ph.D. in the specialty 05.13.19. Ufa: USATU, 2006. **]**

4. **Файзуллин Р. Р.** Интеллектуальная поддержка принятия решений по управлению защитой информации в распределенных информационно-управляющих системах (на примере региональной системы межведомственного электронного взаимодействия Республики Башкортостан) / Дисс. … к.т.н. по спец-ти 05.13.19 (науч. рук. – Васильев В.И.). Уфа: УГАТУ, 2013. **[** R. R. Fayzullin Intelligent decision support for managing information security in distributed information management systems (as an example of a regional system of interagency electronic interaction of the Republic of Bashkortostan) / Diss. ... Ph.D. in the specialty 05.13.19. Ufa: USATU, 2013. **]**

5. **Яндыбаева Э. Э.** Управление информационной безопасностью в системе электронной торговой площадки / Дисс. … к.т.н. по спец-ти 05.13.19 (науч. рук. – Машкина И.В.). Уфа: УГАТУ, 2016. **[** E. E. Yandybaeva Information Security Management in the Electronic Trading Platform System / Diss. ... Ph.D. in the specialty 05.13.19. Ufa: USATU, 2016. **]**

6. **Хафизов А. Ф.** Нейросетевая система обнаружения атак на WWW-сервер / Дисс. … к.т.н. по спец-ти 05.13.11 (науч. рук. – Васильев В.И.). Уфа: УГАТУ, 2004. **[** A. F. Khafizov Neural network system for detecting attacks on a WWW server / Diss. ... Ph.D. in the specialty 05.13.11. Ufa: USATU, 2004. **]**

7. **Кашаев Т. Р.** Алгоритмы активного аудита информационной системы на основе технологий искусственных иммунных систем / Дисс. … к.т.н. по спец-ти 05.13.19 (науч. рук. – Васильев В.И.). Уфа: УГАТУ, 2008. **[** T. R. Kashaev Algorithms for the active audit of an information system based on technologies of artificial immune systems / Diss. ... Ph.D. in the specialty 05.13.19. Ufa: USATU, 2008. **]**

8. **Свечников Л. А.** Интеллектуальная система обнаружения атак на основе имитационного моделирования с использованием нечетких когнитивных карт / Дисс. … к.т.н. по спец-ти 05.13.19 (науч. рук. – Васильев В.И.). Уфа: УГАТУ, 2010. **[** L. A. Svechnikov Intelligent attack detection system based on simulation using fuzzy cognitive maps / Diss. ... Ph.D. in the specialty 05.13.19. Ufa: USATU, 2010. **]**

9. **Никитин А. П.** Многоуровневая многоагентная система фильтрации спама в организации / Дисс. … к.т.н. по спец-ти 05.13.19 (науч. рук. – Валеев С.С.). Уфа: УГАТУ, 2009. **[** A. P. Nikitin Multilevel multi-agent spam filtering system in an organization / Diss. ... Ph.D. in the specialty 05.13.19. Ufa: USATU, 2009. **]**

10. **Дьяконов М. Ю.** Нейросетевая система обнаружения аномального поведения вычислительных процессов микроядерных операционных систем / Дисс. … к.т.н. по спец-ти 05.13.19 (науч. рук. – Валеев С.С.). Уфа: УГАТУ, 2011. **[** M. Yu. Dyakonov Neural network system for detecting abnormal behavior of computational processes of micronuclear operating systems / Diss. ... Ph.D. in the specialty 05.13.19. Ufa: USATU, 2011. **]**

11. **Котов В. Д.** Интеллектуальная система обнаружения вредоносных интернет-страниц на основе технологий машинного обучения / Дисс. … к.т.н. по спец-ти 05.13.19

(науч. рук. – Васильев В.И.). Уфа: УГАТУ, 2013. **[** V. D. Kotov Intelligent system for detecting malicious web pages based on machine learning technologies / Diss. ... Ph.D. in the specialty 05.13.19. Ufa: USATU, 2013. **]**

12. **Шарабыров И. В.** Система обнаружения атак в локальных беспроводных сетях на основе технологий интеллектуального анализа данных / Дисс. … к.т.н. по спец-ти 05.13.19 (науч. рук. – Васильев В.И.). Уфа: УГАТУ, 2016. **[** I. V. Sharabyrov System for detecting attacks in local wireless networks based on technologies of intellectual data analysis / Diss. ... Ph.D. in the specialty 05.13.19. Ufa: USATU, 2016. **]**

13. **Гаврилов Г. Н.** Система обнаружения вредоносных программ в операционной системе (ОС) для мобильных устройств (на примере Android) с применением интеллектуальных технологий / Дисс. … к.т.н. по спец-ти 05.13.19 (науч. рук. – Жернаков С.В.). Уфа: УГАТУ, 2017. **[** G. N. Gavrilov The system for detecting malicious programs in the operating system (OS) for mobile devices (using Android as an example) using intelligent technologies / Diss. ... Ph.D. in the specialty 05.13.19. Ufa: USATU, 2017. **]**

14. **Бакиров Т. К.** Автоматизированная система анализа защищенности корпоративной вычислительной сети на основе многоагентного подхода / Дисс. … к.т.н. по спец-ти 05.13.19 (науч. рук. – Валеев С.С.). **[** T. K. Bakirov An automated system for analyzing the security of a corporate computer network based on a multi-agent approach / Diss. ... Ph.D. in the specialty 05.13.19. **]**

15. **Кудрявцева Р. Т.** Управление информационными рисками с использованием технологий когнитивного моделирования (на примере высшего учебного заведения) / Дисс. … к.т.н. по спец-ти 05.13.19 (науч. рук. – Васильев В.И.). Уфа: УГАТУ, 2008. **[** R. T. Kudryavtseva Information risk management using cognitive modeling technologies (using the example of a higher educational institution) / Diss. ... Ph.D. in the specialty 05.13.19. Ufa: USATU, 2008. **]**

16. **Кустов Г. А.** Управление информационными рисками организации на основе логико-вероятностного метода (на примере компании добровольного медицинского страхования) / Дисс. … к.т.н. по спец-ти 05.13.19 (науч. рук. – Васильев В.И.). Уфа: УГАТУ, 2008. **[** G. A. Kustov Management of information risks of the organization based on the logical and probabilistic method (on the example of a voluntary medical insurance company) / Diss. ... Ph.D. in the specialty 05.13.19. Ufa: USATU, 2008. **]**

17. **Степанова Е. С.** Модели и методы оценки рисков нарушения информационной безопасности с использованием нечетких когнитивных карт / Дисс. … к.т.н. по спец-ти 05.13.19 (науч. рук. – Машкина И.В.). Уфа: УГАТУ, 2013. **[** E. S. Stepanova Models and methods for assessing the risks of information security breaches using fuzzy cognitive maps / Diss. ... Ph.D. in the specialty 05.13.19. Ufa: USATU, 2013. **]**

18. **Фазлиахметов Т. И.** Алгоритмы контроля целостности результатов измерений в базах данных на основе нейронных сетей (на примере информационной системы контроля транспорта нефти) / Дисс. … к.т.н. по спец-ти 05.13.19 (науч. рук. – Фрид А.И.). Уфа: УГАТУ, 2013. **[** T. I. Fazliakhmetov Algorithms for monitoring the integrity of measurement results in databases based on neural networks (using the example of an information system for monitoring oil transportation) / Diss. ... Ph.D. in the specialty 05.13.19. Ufa: USATU, 2013. **]**

19. **Сенцова А. Ю.** Модели и метод экспертного аудита информационной безопасности в системе облачных вычислений / Дисс. … к.т.н. по спец-ти 05.13.19 (науч. рук. – Машкина И.В.). Уфа: УГАТУ, 2016. **[** A. Yu. Sentsova Models and the method of expert audit of information security in a cloud computing system / Diss. ... Ph.D. in the specialty 05.13.19. Ufa: USATU, 2016. **]**

20. **Сагитова В. В.** Модели и алгоритмы анализа информационных рисков при проведении аудита безопасности информационной системы персональных данных / Дисс. … к.т.н. по спец-ти 05.13.19 (науч. рук. – Васильев В.И.). Уфа: УГАТУ, 2019. **[** V. V. Sagitova Models and algorithms for the analysis of information risks when conducting a security audit of an information system for personal data / Diss. ... Ph.D. in the specialty 05.13.19. Ufa: USATU, 2019.**]**

21. **Картак В. М., Башмаков Н.М.** Оптимизация размещения видеокамер /Вопросы защиты информации,Москва, 2019, №4, ст.54-58.[V.M. Kartak, N.M. Bashmakov Optimization of camcorder placement /Information security questions, 2019, №4 p/54-58]

22. **Васильев В. И.** Интеллектуальные системы защиты информации / Учеб. Пособие для вузов. 3-е изд. М.: Инновационное машиностроение, 2017. 201 с. (1-е изд. М.: Машиностроение, 2010; 2-е изд. М.: Машиностроение, 2012). **[** V. I. Vasilyev Intelligent systems of information security / Textbook. Manual for universities. 3rd ed. M.: Innovacionnoe mashinostroenie, 2017. 201 p. **]**

23. **Гузаиров М. Б., Машкина И. В.** Управление защитой информации на основе интеллектуальных технологий: учебное пособие для вузов. – М.: Машиностроение, 2013. 241 с. **[** M. B. Guzairov, I. V. Mashkina Information security management based on intellectual technologies: a textbook for universities. M.: Mashinostroenie, 2013.241 p. **]**

ОБ АВТОРАХ

ВАСИЛЬЕВ Владимир Иванович, проф. каф. ВТиЗИ УГАТУ. Дипл. инж. по пром. электронике (УАТ, 1970). Д-р техн. наук (ЦИАМ, 1990). Иссл. в обл. интеллектуальных систем управления и защиты информации.

КАРТАК Вадим Михайлович, зав. каф. ВТиЗИ. Дипл. инженер-программист (УГАТУ, 1995). Д-р физ.-мат. Наук (УГАТУ, 2012). Иссл. в обл. дискретной оптимизации.

METADATA

Title: Application of artificial intelligence technologies in the tasks of information protection (based on materials of USATU scientific school).

Authors: V. I. Vasilyev [1], V. M. Kartak[2]

Affiliation:

Ufa State Aviation Technical University (UGATU), Russia.

Email: [1]vasilyev@ugatu.ac.ru, [2]kvmail@mail.ru.

Language: Russian.

Source: SIIT, no. 2 (4), pp. 43-50, 2020. ISSN 2686-7044 (Online), ISSN 2658-5014 (Print).

Abstract: The problem of information protection acquires today a special acuity and topicality due to active implantation of all complicated digital information technologies and artificial intelligence methods in the sphere of industrial manufacturing and provision of services, and as a consequence, increasing interest to these information resources

from the side of all kinds of external and internal intruders and increase of the number of incidents and scale of losses as a result of successful implementation of targeted attacks. This paper presents the results of researches in the field of information security carried out in the framework of USATU scientific school since the beginning of 2000s. The particular role and significance of applying technologies of intelligent data analysis for solving these tasks is emphasized, the advantages and prospects for their practical use are shown.

Key words: information protection; information security; intelligent data analysis; risk analysis; audit of information security.

About authors:

VASILYEV, Vladimir Ivanovich, Prof. Dept. of Computer Engineering and Information Security. Dipl. Engineer in Industrial Electronics (USATU, 1970). Dr. of Tech. Sci. (CIAM, 1990). Invest. in intelligent systems of control and information security.

KARTAK, Vadim Mihailovich, Head of Dept. of. Computer Engineering and Information Security. Dipl. Software Engineer (USATU, 1995). Dr. of Phys.-Math. Sci. (USATU, 2012). Invest. in discrete optimization.