Научная статья
УДК 004.8:33
ББК 32.813+65с51
Л 86
DOI: 10.53598/2410-3225-2024-4-351-46-57

Автоматизированный системно-когнитивный анализ состояния информационной безопасности фирмы

(*Рецензирована*)

Евгений Вениаминович Луценко[1], Валерий Евгеньевич Коржаков[2], Никита Сергеевич Головин[3]

[1] *Кубанский государственный аграрный университет имени И. Т. Трубилина, Краснодар, Россия, prof.lutsenko@gmail.com*
[2] *Адыгейский государственный университет, Майкоп, Россия, korve@yandex.ru*
[3] *Элитная частная экономическая школа, г. Нови-Сад, Сербия, nikitagolovin416@gmail.com*

Аннотация. *Работа посвящена созданию адаптивного инструмента решения задач прогнозирования и минимизации последствий уязвимостей в настройках безопасности компьютеров, работающих под управлением операционных систем MS Windows. Обоснован выбор автоматизированного системно-когнитивного анализа (АСК-анализа), позволяющего разрешить указанные проблемы, подчеркнута его способность обрабатывать фрагментированные и зашумленные данные различной природы. Интеллектуальная система «Эйдос» обеспечивает обработку и анализ больших объемов данных, связанных с конфигурацией системной безопасности, позволяет прогнозировать потенциальные риски и обеспечивает поддержку принятия решений по их минимизации. Работа включает описание этапов проведения АСК-анализа от когнитивной структуризации предметной области до синтеза моделей и поддержки принятия решений. Разработанная методика хорошо подходит для повышения информационной безопасности компьютерных систем малого и среднего бизнеса.*

Ключевые слова: *адаптивные модели, большие данные, прогнозирование рисков, когнитивная структуризация, автоматизированный системно-когнитивный анализ, АСК-анализ, информационная безопасность, MS Windows*

Для цитирования: *Луценко Е. В., Коржаков В. Е., Головин Н. С. Автоматизированный системно-когнитивный анализ состояния информационной безопасности фирмы // Вестник Адыгейского государственного университета. Сер.: Естественно-математические и технические науки. 2024. Вып. 4 (351). С. 46–57. DOI: 10.53598/2410-3225-2024-4-351-46-57*

Original Research Paper

Automated system-cognitive analysis of the company's information security status

Evgeny V. Lutsenko[1], Valery E. Korzhakov[2], Nikita S. Golovin[3]

[1] *Kuban State Agrarian University named after I. T. Trubilin, Krasnodar, Russia, prof.lutsenko@gmail.com*
[2] *Adyghe State University, Maykop, Russia, korve@yandex.ru*
[3] *Elite Private Economic School, Novi Sad, Serbia, nikitagolovin416@gmail.com*

Abstract. *The paper is devoted to the creation of an adaptive tool for solving the problems of predicting and minimising the consequences of vulnerabilities in the security settings of computers running under MS Windows operating systems. The choice of automated system-cognitive analysis (ASK-analysis), which allows solving the above problems, is justified, its ability to process fragmented and noisy data of different nature is emphasised. Intelligent system "Eidos" provides processing and analysis of large amounts of data related to the configuration of system security, allows to predict po-*

tential risks and provides support for decision-making on their minimisation. The paper includes a description of the stages of ASK-analysis from cognitive structuring of the subject area to model synthesis and decision support. The developed methodology is well suited for improving information security of small and medium-sized business computer systems.

Keywords: *adaptive models, big data, risk prediction, cognitive structuring, automated system-cognitive analysis, ASK-analysis, information security, MS Windows*

For citation: *Lutsenko E. V., Korzhakov V. E., Golovin N. S. Automated system-cognitive analysis of the company's information security status // The Bulletin of the Adyghe State University. Ser.: Natural-Mathematical and Technical Sciences. 2024. Iss. 4 (351). P. 46–57. DOI: 10.53598/2410-3225-2024-4-351-46-57*

1. Введение

Автоматизированный системно-когнитивный анализ демонстрирует широкие возможности для решения различных проблем в деятельности фирм [1–4]. Одной из таких актуальных проблем является обеспечение информационной безопасности. В последние годы исследованиям по данной проблематике уделяется все большее внимание [5–13].

Проблема обеспечения информационной безопасности является системной и далеко выходит за рамки чисто технической или инженерной проблемы. В частности, вся серьезность возможных последствий ошибок в обеспечении информационной безопасности часто не вполне осознается не только системным администратором, но и руководством фирмы. Одной из причин этого, по-видимому, является то, что примеры, приводящиеся в специальной литературе[*], редко бывают убедительными.

В то же время для обоснованного принятия решения о целевом финансировании работ по обеспечению информационной безопасности (ТЭО — технико-экономическом обосновании целесообразности этих работ) руководителю любой фирмы необходима информация как о стоимости этих работ, так и о возможных финансовых и иных последствиях отказа от их проведения. Проблема заключается в том, что получить подобную информацию в настоящее время весьма затруднительно, так как на российском рынке программного обеспечения (ПО) отсутствует доступное малым фирмам не проприетарное ПО, с понятной рядовому системному администратору и его руководителю методикой оценки последствий ошибок в конфигурировании системы безопасности их компьютеров.

В данной работе предлагается решение этой проблемы, чем и обусловлена ее актуальность.

2. Метод

К методу решения поставленной проблемы предъявляются определенные требования, в частности, метод должен:

– обеспечивать решение сформулированной проблемы на основе информации системного администратора об ошибках конфигурации системы безопасности компьютеров и фактических последствиях этого в данной конкретной фирме;

– быть недорогим в приобретении и использовании, то есть для этого должно быть достаточно недорогого лицензионного программного обеспечения и системного администратора, причем курс его дополнительного обучения должен быть несложным, то есть не предъявлять к нему каких-то сверхжестких нереалистичных требований;

– быть адаптивным, то есть оперативно учитывать изменения во всех компонентах моделируемой системы.

Для определенности ограничимся рассмотрением системы безопасности опера-

[*] http://ru.wikipedia.org/wiki/Information_security

ционной системы MS Windows. Однако данное средство не содержит какого-либо аппарата прогнозирования возможных последствий фактически имеющейся конфигурации системы безопасности.

Поэтому *целью данной работы* является решение поставленной проблемы путем разработки адаптивной методики прогнозирования последствий ошибок в настройках системы безопасности.

Для достижения поставленной цели выбран метод автоматизированного системно-когнитивного анализа (АСК-анализ) [1–4]. Этот выбор обусловлен тем, что данный метод является непараметрическим, позволяет корректно и сопоставимо обрабатывать тысячи градаций факторов и будущих состояний объекта управления при неполных (фрагментированных), зашумленных данных различной природы, то есть измеряемых в различных единицах измерения. Для метода АСК-анализа разработаны и методика численных расчетов, и соответствующий программный инструментарий, а также технология и методика их применения. Они прошли успешную апробацию при решении ряда задач в различных предметных областях [1–4]. Отметим, что первая статья о применении АСК-анализа для моделирования информационной безопасности написана в 2003 году.

Важной особенностью АСК-анализа является возможность единообразной числовой обработки разнотипных по смыслу и единицам измерения числовых и нечисловых данных. Это обеспечивается тем, что нечисловым величинам тем же методом, что и числовым, приписываются сопоставимые в пространстве и времени, а также между собой, количественные значения, позволяющие обрабатывать их как числовые: на первых двух этапах АСК-анализа числовые величины сводятся к интервальным оценкам, как и информация об объектах нечисловой природы (фактах, событиях) (этот этап реализуется и в методах интервальной статистики); на третьем этапе АСК-анализа всем этим величинам по единой методике, основанной на системном обобщении семантической теории информации А. Харкевича, сопоставляются количественные величины (имеющие смысл количества информации в признаке о принадлежности объекта к классу), с которыми в дальнейшем и производятся все операции моделирования (этот этап является уникальным для АСК-анализа).

Учитывая этапы АСК-анализа, выполним декомпозицию цели работы в последовательность задач и подзадач, являющихся этапами ее достижения (рисунок 1).

Для данной работы особое значение имеет решение подзадачи 8.1, так как она позволяет детально исследовать влияние каждого значения каждого фактора на риски, связанные с информационной безопасностью.

3. Результаты

В данном разделе кратко рассмотрим решение поставленных задач.

3.1. *Задача-1: Когнитивная структуризация предметной области*

Когнитивная структуризация предметной области — это 1-й единственный неавтоматизированный в системе «Эйдос» этап АСК-анализа, на котором решается, что является объектом моделирования, какие факторы на него влияют и каковы результаты влияния этих факторов.

3.2. *Задача-2: Формализация предметной области*

На этапе формализации предметной области, исходя из результатов когнитивной структуризации, осуществляется разработка классификационных и описательных шкал и градаций, а затем кодирование исходных данных с их помощью и получение в результате базы событий или обучающей выборки (датасет).

Исходные данные запланированного состава *были получены* в той форме, в которой они накапливаются в поставляющей их организации. В нашем случае этой органи-

зацией выступила фирма, название которой мы не приводим в связи с конфиденциальностью информации. В полученной базе данных представлены данные по настройкам системы безопасности компьютеров фирмы, полученные с применением системы MBSA, дополненные информацией о фактических последствиях различных настроек за календарный год; всего 323 записи по различным внутренним IP-адресам сетевых станций. Этого вполне достаточно для целей данной работы, за что авторы благодарны руководству данной фирмы.

В полном виде таблица исходных данных доступна по ссылке:

https://lc.kubagro.ru/Source_data_applications/Applications-000007/Inp_data.xlsx

При вводе исходных данных в API-2.3.2.2 системы «Эйдос» сокращено количество классификационных и описательных шкал и градаций, которое было в работе [1–4]. Это сделано с целью обеспечения лучшей обозримости моделей и ускорения расчетов.

В результате работы данного автоматизированного программного интерфейса *автоматически* получаются исходный справочник классов распознавания, справочник признаков, а также обучающая выборка (датасет), представляющая собой закодированные с помощью этих справочников исходные данные.

3.3. *Задача-3: Синтез статистических и системно-когнитивных моделей. Многопараметрическая типизация и математическая модель частных критериев знаний*

3.3.1. В результате синтеза семантической информационной модели решена *задача: Многокритериальная типизация* различных вариантов финансовых и иных последствий ошибок в настройках системы безопасности операционной системы MS Windows. Решение этой задачи осуществлялось в 3 этапа:

Этап-1. Расчет матрицы сопряженности (матрицы абсолютных частот), связывающей частоты *фактов* совместного наблюдения в исходной выборке интервальных значений классов и факторов. Всего этих фактов исследовано *18088*, что и составляет объем выборки.

Этап-2. На основе базы данных абсолютных частот рассчитываются информационные базы условных и безусловных процентных распределений или относительных частот, которые при увеличении объема исходной выборки асимптотически стремятся к предельным значениям – вероятностям, никогда не достигая точного равенства им. Имея это в виду, несколько упрощая, считается допустимым, как это принято в литературе, называть их условными и безусловными вероятностями.

Этап-3. На основе матриц условных и безусловных вероятностей рассчитываются матрицы системно-когнитивных моделей.

3.3.2. *Данные, информация, знания*

Исходные данные об объекте управления обычно представлены в форме баз данных, чаще всего временных рядов, то есть данных, привязанных ко времени. В соответствии с методологией и технологией АСК-анализа для управления и принятия решений использовать непосредственно исходные данные не представляется возможным. Точнее сделать это можно, но результат управления при таком подходе оказывается мало чем отличающимся от случайного. Для реального же решения задачи управления необходимо предварительно преобразовать данные в информацию, а ее — в знания. Для этого необходимо выполнить два этапа:

1. Выявление событий в данных (разработка классификационных и описательных шкал и градаций и кодирование исходных данных с их использованием, преобразование их в обучающую выборку, то есть в базу событий — эвентологическую базу).

2. Выявление причинно-следственных зависимостей между событиями в базе событий. В АСК-анализе предлагается 7 взаимосвязанных друг с другом количествен-

ных мер причинно-следственных связей, основанных на мере взаимосвязей критерия хи-квадрат Пирсона, известного в экономике коэффициента возврата инвестиций ROI, а также на семантической мере целесообразности информации по А. Харкевичу.

3.4. *Задача-4: Верификация моделей*

Для оценки достоверности моделей в системе «Эйдос» используется F-мера Ван Ризбергена и две ее модификации, предложенные авторами [1–4]:

– нечеткое мультиклассовое обобщение F-меры Ван Ризбергена;

– нечеткое мультиклассовое обобщение F-меры Ван Ризбергена, инвариантное относительно объема выборки.

Получены следующие результаты оценки достоверности созданных моделей:

– истинных отрицательных решений почти всегда больше, чем ложных;

– при низких уровнях сходства до 30 % больше доля ложных положительных решений, а при повышении уровня сходства до 40 % и выше возрастает и доля истинных положительных решений.

Это означает, что *уровень сходства* (*интегральный критерий*) *является адекватной мерой степени истинности решения*.

На этом основании можно сделать важный вывод: *система* «*Эйдос*» *сама без обращения к внешним верифицированным* (*гарантированно истинным*) *данным может оценивать степень истинности своих решений, то есть проводить адекватный внутренний аудит достоверности моделей и их применения для решения задач.*

3.5. *Задача-5: Выбор наиболее достоверной модели*

В системе «Эйдос» реализовано несколько различных методов повышения адекватности модели:

– исключение из модели статистически малопредставленных классов и факторов (артефактов);

– исключение незначимых факторов, то есть факторов, имеющих низкую селективную силу или дифференцирующую способность;

– ремонт (взвешивание) данных, что обеспечивает не только классическую, но и структурную репрезентативность исследуемой выборки по отношению к генеральной совокупности;

– итерационное разделение классов на типичную и нетипичную части (дивизивная, то есть разделяющая, в отличие от агломеративной, древовидная кластеризация);

– генерация сочетанных признаков, дополнение справочников классов и признаков и перекодирование исходной выборки.

Выводы:

– при прогнозировании и принятии решений целесообразно учитывать дифференциальную достоверность идентификации по классам, связанную со степенью их детерминированности;

– применение модели чаще всего обеспечивает во много раз более высокую достоверность, чем случайное угадывание или неиспользование модели, однако по слабодетерминированным классам это не так, и их нецелесообразно учитывать при прогнозировании и рассматривать при анализе модели.

3.6. *Задача-6: Системная идентификация и прогнозирование*

Если решать задачу прогнозирования в полном виде, то нужно организовать следующие вложенные циклы:

– по всем моделям;

– по всем объектам распознаваемой выборки;

– по всем классам;

– по всем признакам.

В системе «Эйдос» 10 моделей (3 статистических и 7 системно-когнитивных). Объектов распознаваемой выборки столько, сколько сетевых станций в фирме, в нашем примере их 343, но их может быть и меньше, и значительно больше — до нескольких десятков миллионов. Классов в нашем примере 23 (может быть до 2000), а признаков 28 (может быть до нескольких сотен тысяч и даже миллионов). При больших размерностях этих данных решение задачи прогнозирования может потребовать огромных затрат вычислительных ресурсов и длительного времени.

Кроме того, для ускорения расчетов в системе «Эйдос» по решению пользователя могут быть использованы графические процессоры (GPU), а также сжатые векторы (только со значащими координатами) на центральном процессоре (CPU).

Итак, в системе «Эйдос» для каждого состояния системы информационной безопасности фирмы, представленного в распознаваемой выборке, рассчитывается суммарное количество информации, содержащееся в градациях факторов, отражающих настройки системы безопасности, о принадлежности данного состояния к каждому из классов.

Иначе говоря, системой «Эйдос» каждое прогнозируемое состояние системы безопасности относится к тому классу, о принадлежности к которому в его системе признаков содержится *максимальное количество информации* (это и есть один из интегральных критериев сходства, используемых в системе «Эйдос»).

3.7. ***Задача-7: Поддержка принятия решений*** **(*упрощенный вариант принятия решений как обратная задача прогнозирования, позитивный и негативный информационные портреты классов, SWOT-анализ; развитый алгоритм принятия решений в АСК-анализе*)** [1–4]

Задача принятия решений является обратной по отношению к задаче прогнозирования. Если при прогнозировании по факторам, действующим на объект моделирования, определяется его будущее состояние, то при принятии решений, наоборот, по заданному будущему состоянию объекта моделирования (целевому или нежелательному) определяются факторы, обуславливающие это состояние.

Если при прогнозировании по заданным настройкам системы безопасности операционной системы определяется, какие проблемы с информационной безопасностью ими обусловливаются, то в задаче принятия решений, наоборот: по заданному виду проблемы с информационной безопасностью или по ее отсутствию определяется, какие настройки системы безопасности способствуют возникновению этой ситуации, а какие препятствуют этому.

Необходимо отметить, что задача выявления фактически имеющихся зависимостей и задача содержательного объяснения причин существования именно данных конкретных обнаруженных зависимостей, а не каких-либо других, то есть задача содержательной интерпретации обнаруженных зависимостей, – это совершенно разные задачи. По мнению авторов, задача интерпретации должна решаться специалистами в моделируемой предметной области, однако сама возможность применения обнаруженных зависимостей в практике прогнозирования и принятия решений не связана с наличием или отсутствием такой содержательной интерпретации или со степенью ее адекватности.

3.8. ***Задача-8: Исследование объекта моделирования путем исследования его модели включает ряд подзадач***

Кратко рассмотрим основные подпункты задачи 8 (рис. 1).

Подзадача-8.1: Инвертированные SWOT-диаграммы значений описательных шкал (семантические потенциалы). Пользователь может выбрать любое значение фактора и затем в нижней части экранной формы задать модель.

Подзадача-8.2: Кластерно-конструктивный анализ классов (градаций классификационных шкал). Данный режим имеет две реализации: на языках xBase++ и на Питоне. Реализация на Питоне лучше и быстрее работает на больших размерностях данных.

Подзадача-8.3: Кластерно-конструктивный анализ значений факторов (градаций описательных шкал). Данный режим имеет две реализации: на языках xBase++ и на Питоне. На этом этапе факторы разделяются на два противоположных по смыслу кластера, которые представляют собой смысловые полюса конструкта.

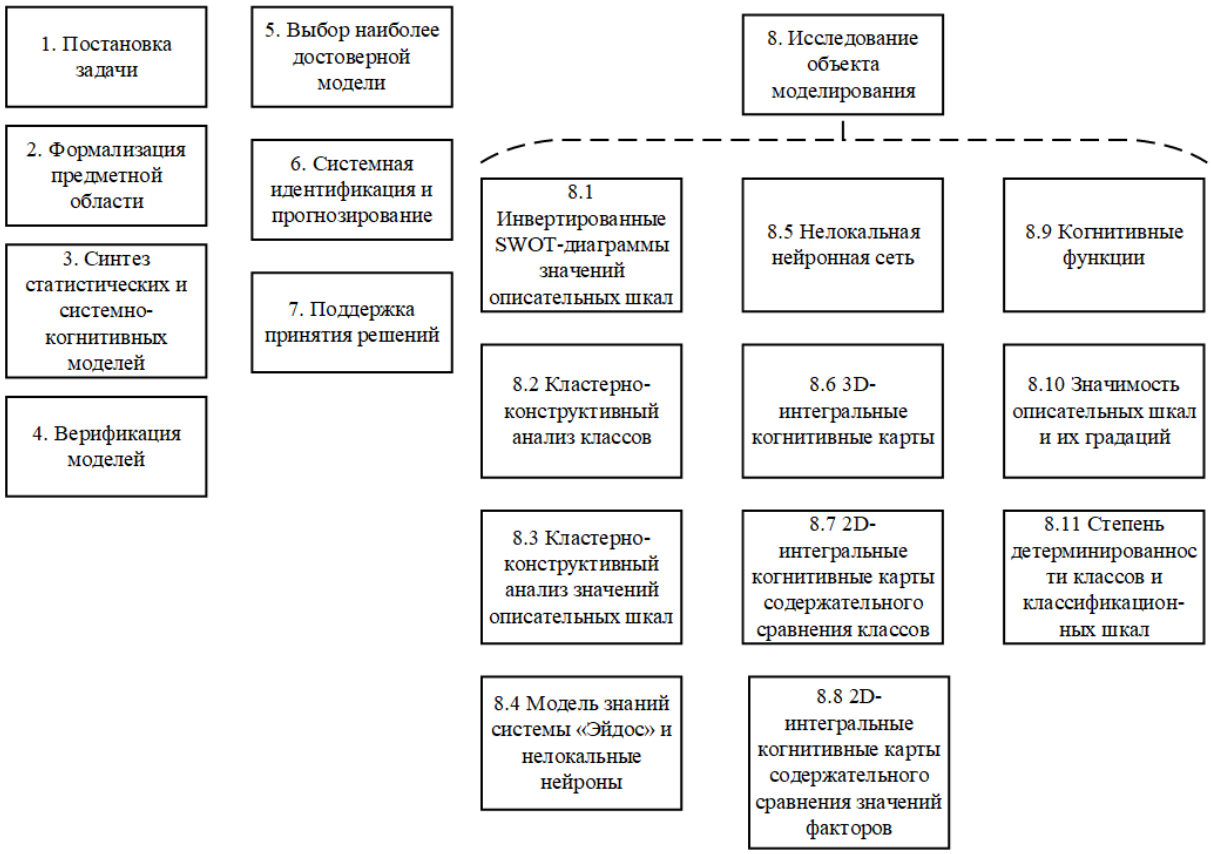

Рис. 1. Декомпозиция цели работы в последовательность задач и подзадач

Fig. 1. Decomposition of the purpose of the work in sequence of problems and subtasks

Подзадача-8.4: Модель знаний системы «Эйдос» и нелокальные нейроны.

Несмотря на огромное и быстро возрастающее количество различных интеллектуальных систем, количество различных *моделей знаний*, на которых они основаны, остается довольно ограниченным. Более того, можно обоснованно утверждать, что все известные на данный момент формализованные модели знаний, применяемые в базах знаний интеллектуальных систем, являются не более чем вариациями одной-единственной базовой модели знаний

В таблице 1 приведены практически все основные типы баз знаний, известные в настоящее время, а также дано соотношение содержания основных терминов, используемых в этих базах знаний.

Основной вывод, который можно обоснованно сделать на основе этой таблицы, состоит в том, что все эти модели представления знаний отличаются друг от друга в значительно меньшей степени, чем обычно принято думать. По сути, все известные модели представления знаний являются вариациями представления одной и той же модели знаний в разных по звучанию, но очень сходных по смысловому содержанию терминах.

Системно-когнитивные модели системы «Эйдос» представляют собой гибридные декларативные нечеткие модели, основанные на теории информации, сочетающие

в себе достоинства фреймовых и нейросетевых моделей. Поэтому они допускают нейросетевую интерпретацию [1–4].

Таблица 1

Известные типы баз знаний и соотношение смыслового содержания их основных терминов

Table 1. Known types of knowledge bases and correlation of semantic content of their main terms

Модель автоматизированного системно-когнитивного анализа и интеллектуальной системы «Эйдос» (Евгений Луценко, 1979)	Классификационные шкалы и градации	Описательные шкалы и градации	Конкретный образ объекта исследуемой выборки	База знаний (декларативное и процедурное представление знаний), прямые и обратные правдоподобные рассуждения	Обобщенный образ класса	Кластеры, могут отображаться в форме дерева и семантической сети	Конструкт как система наиболее непохожих классов с спектром промежуточных по уровню сходства классов
Логическая модель – классическая детерминистская логика (Аристотель, 350 году до н. э.)	Бинарные (дихотомические) справочники классов	Бинарные (дихотомические) справочники признаков	Бинарный вектор объекта	Правила логического вывода	–	–	–
Логическая модель (нечеткая логика Лотфи Заде, 1965)	Номинальные, порядковые и числовые справочники классов	Номинальные, порядковые и числовые справочники признаков	Вектор объекта с указанием степени выраженности у него признаков	Нечеткие правила логического вывода	–	–	–
Фреймовая модель (Марвин Мински, 1974)	Имена фреймов	Слоты и шпации	Фреймы-экземпляры	Процедуры формирования фреймов-прототипов на основе фреймов-экземпляров	Фреймы-образцы, или прототипы	–	–
Продукционная модель экспертных систем (Аллен Ньюэлл и Герберт Саймон, 1972)	–	–	–	Продукционное представление правил вывода	–	–	–
Семантические сети (Джон Сэрелл, 1968)	–	Свойства и их значения	Элемент класса	Отношения между классами	Класс	Граф результатов кластерного анализа	–
Нейронные сети (Фрэнк Розенблатт, 1957)	Множество нейронов	Множество рецепторов	Объект обучающей выборки	Матрица весовых коэффициентов	Нейрон с весовыми коэффициентами	Нейрон 2-го слоя сети	–

Подзадача-8.5: Нелокальная нейронная сеть. Представляет собой Парето-подмножество одного слоя полносвязной нейросети системно-когнитивной модели. Показано три четверти наиболее сильных положительных и отрицательных связей в слое.

Подзадача-8.6: 3d-интегральные когнитивные карты. 3d-интегральная когнитивная карта объединяет в одном изображении:

1. Вверху: фрагмент семантической 2d сети нейронов;
2. Внизу: фрагмент семантической 2d сети рецепторов;

3. Нейроны и рецепторы соединены линиями связи слоя нейросети.

Подзадача-8.7: 2d-интегральные когнитивные карты содержательного сравнения классов (опосредованные нечеткие правдоподобные рассуждения). Представлено Парето-подмножество 2d-интегральной когнитивной карты содержательного сравнения классов (опосредованные нечеткие правдоподобные рассуждения) в системно-когнитивной модели.

Подзадача-8.8: 2d-интегральные когнитивные карты содержательного сравнения значений факторов (опосредованные нечеткие правдоподобные рассуждения). Представлено Парето-подмножество 2d-интегральной когнитивной карты содержательного сравнения значений факторов по их смыслу (опосредованные нечеткие правдоподобные рассуждения) системно-когнитивной модели.

Подзадача-8.9: Когнитивные функции. Системно-когнитивные модели системы «Эйдос» представляют собой матричные передаточные функции [1–4], конформно отображающие когнитивное пространство факторов на когнитивное пространство классов, то есть результатов их влияния на объект моделирования [1–4].

Когнитивное пространство факторов — это многомерное не ортонормированное абстрактное фазовое пространство, построенное как на координатных осях на описательных шкалах, представляющих собой формализованное описание свойств объекта моделирования или влияющих на него факторов. Эти оси могут быть текстового или числового типа. Шкалы текстового типа могут быть номинальными, порядковыми и дихотомическими (бинарными или логическими). Градациями этих координатных осей являются значения свойств или значения факторов (признаки).

Когнитивное пространство классов — это многомерное не ортонормированное абстрактное фазовое пространство, построенное как на координатных осях на классификационных шкалах, представляющих собой формализованное описание обобщающих категорий, к которым относится объект моделирования или будущих состояний, в которые он может перейти под действием влияющих на него факторов. Эти оси могут быть текстового или числового типа. Шкалы текстового типа могут быть номинальными, порядковыми и дихотомическими (бинарными или логическими). Градациями этих координатных осей являются классы.

Каждому объекту обучающей выборки соответствуют определенные многомерные трубки (интервалы, траектории) как в когнитивном пространстве факторов, так и в когнитивном пространстве классов.

Если в качестве осей когнитивного пространства факторов и классов выбрать пространственные координаты, то построенные в системе «Эйдос» системно-когнитивные модели будут отражать статику объекта моделирования, и на этом пространстве может решаться задача идентификации.

Если к пространственным осям добавить время, то получится пространство Минковского, то есть пространство-время, используемое в специальной и общей теории относительности Эйнштейна. Построенные в системе «Эйдос» на этом пространстве-времени системно-когнитивные модели будут отражать динамику объекта моделирования, и на этом пространстве-времени может решаться задача прогнозирования и принятия решений.

Когнитивные функции представляют собой проекции в виде тепловой диаграммы на экранную плоскость модулей и знаков линий связи подматрицы модели, соответствующей одной описательной шкале и одной классификационной шкале.

Подзадача-8.10: Значимость описательных шкал и их градаций. Значимость фактора (описательной шкалы) информационной безопасности является средним от значимости его градаций.

Подзадача-8.11: Степень детерминированности классов и классификационных шкал. По результатам кластеризации можно сделать вывод о том, что различные классы обладают различной степенью вариабельности обусловливающих их факторов, то есть одни классы являются жестко детерминированными, тогда как другие вызываются различными сочетаниями действующих факторов, что затрудняет и делает менее достоверным их прогнозирование и осуществление.

4. Обсуждение

При планировании данного исследования авторы ставили цель лишь оценить возможность применения технологии АСК-анализа для прогнозирования последствий ошибочного конфигурирования системы безопасности MS Windows. Данное исследование показало, что это возможно и перспективно. Представленный в работе вариант исследования имеет ряд ограничений и недостатков, в преодолении которых и состоит перспектива его развития. В частности, можно было бы увеличить объем исследуемой выборки за счет увеличения количества компьютеров и периода времени, за который исследуется деятельность фирмы. Выявленные на основе опыта эксплуатации и системного администрирования сетевых станций знания о последствиях ошибок в конфигурировании системы безопасности MS Windows были верифицированы с помощью ChatGPT с моделью 4o, что показало высокую степень их соответствия и согласованности. При этом ChatGPT-4o еще и давал и более-менее обстоятельные объяснения причин возникновения проблем в области информационной безопасности.

Из этого результата можно сделать обоснованные выводы о том, что:

– выявленные в данной работе из реального опыта знания о влиянии настроек безопасности на возникновение проблем с информационной безопасностью MS Windows являются вполне адекватными;

– эти знания облают высокой степенью конкретности и именно для той фирмы, на основе опыта которой они выявлены, а значит, они обладают для этой фирмы более высокой адекватностью, чем общие знания ChatGPT.

Иначе говоря, система «Эйдос» не просто выявляет адекватные знания из опыта, но и делает это конкретно для данной фирмы в данное время, то есть выявленные с ее помощью знания являются локализованными с учетом места и адаптированными с учетом времени, в отличие от знаний общего характера, хранящихся в базах знаний ChatGPT.

При верификации использовались знания, содержащиеся в результатах решения задачи-7: Поддержка принятия решений (упрощенный вариант принятия решений как обратная задача прогнозирования, позитивный и негативный информационные портреты классов, SWOT-анализ; развитый алгоритм принятия решений в АСК-анализе) и подзадачи-8.1: Инвертированные SWOT-диаграммы значений описательных шкал (семантические потенциалы).

5. Выводы

Таким образом, в работе описана технология, методика и некоторые результаты применения автоматизированного системно-когнитивного анализа и его программного инструментария в целях обеспечения безопасности компьютерных систем. Основным элементом для выявления знаний о последствиях ошибок в конфигурировании системы безопасности в операционной системе Microsoft Windows и использования этих знаний для прогнозирования последствий, то есть вида проблем с информационной безопасностью, способа, стоимости и трудоемкости их устранения, выступает интеллектуальная система «Эйдос».

Примечания[**]

1. Луценко Е. В., Коржаков В. Е., Лаптев В. Н. Теоретические основы и технология применения системно-когнитивного анализа в автоматизированных системах обработки информации и управления (АСОИУ) (на примере АСУ вузом) / под науч. ред. Е. В. Луценко. Майкоп : АГУ, 2009. 536 с.

2. Луценко Е. В., Коржаков В. Е., Ермоленко В В. Интеллектуальные системы в контроллинге и менеджменте средних и малых фирм / под науч. ред. Е. В. Луценко. Майкоп : АГУ, 2011. 392 с.

3. Луценко Е. В., Коржаков В. Е., Дубянский А. А. Интеллектуальная система прогнозирования последствий ошибочного конфигурирования системы безопасности MS Windows // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. 2010. № 05 (059). С. 53–78. URL: http://ej.kubagro.ru/2010/05/pdf/06.pdf (дата обращения: 13.09.2024).

4. Луценко Е. В., Головин Н. С. Автоматизированный системно-когнитивный анализ состояния информационной безопасности фирмы на примере компьютеров с MS Windows // 2024. November. DOI: 10.13140/RG.2.2.35422.86088/1

5. Mughal A. A. Artificial Intelligence in Information Security: Exploring the Advantages, Challenges, and Future Directions // Journal of Artificial Intelligence and Machine Learning in Management. 2018. Vol. 2, No. 1. P. 22–34.

6. Li J. Cybersecurity meets artificial intelligence: a survey // Frontiers of Information Technology & Electronic Engineering. 2018. Vol. 19, No. 12. P. 1462–1474.

7. Artificial intelligence in cyber security: research advances, challenges, and opportunities / Z. Zhang, H. Ning, F. Shi [et al.] // Artificial Intelligence Review. 2022. Vol. 55. P. 1029–1055.

8. Dhingra M., Jain M., Jadon R. S. Role of artificial intelligence in enterprise information security: A review // Fourth International Conference on Parallel, Distributed and Grid Computing (PDGC). Waknaghat, 2016. P. 188–191.

9. Effectiveness of artificial intelligence techniques against cyber security risks apply of IT industry / B. Alhayani, H. J. Mohammed, I. Z. Chaloob // Materials Today: Proceedings. 2021. Vol. 531, No. 10. P.1016.

10. Increasing the level of network and information security using artificial intelligence / G. Pavlova, R. Dakov, G. Tsochev, R. Trifonov // Fifth International Conference on Advances in Computing, Communication and Information Technology. 2017. P. 83–88.

11. Kisimova Z. I., Begishev I., Sidorenko E. L. Artificial Intelligence and Problems of Ensuring Cyber Security // International Journal of Cyber Criminology. 2019. Vol. 13, No. 2. P. 564–577.

12. Das R., Sandhane R. Artificial intelligence in cyber security // Journal of Physics: Conference Series. IOP Publishing, 2021. Vol. 1964, No. 4. P. 042072.

13. Hashmi E., Yamin M. M., Yayilgan S. Y. Securing tomorrow: a comprehensive survey on the synergy of Artificial Intelligence and information security // AI and Ethics. 2024. July. P. 1–19.

References

1. Lutsenko E. V., Korzhakov V. E., Laptev V. N. Theoretical bases and technology of application it is system-kognitivnogo the analysis in the automated systems of processing of the information and management (ASPIM) (on an example of the automated control systems of high school) / under scient. ed. E. V. Lutsenko. Maykop : ASU, 2009. 536 c.

2. Lutsenko E. V., Korzhakov V. E., Ermolenko V. V. Intellectual systems in controlling and management of averages and small firms / under scient. ed. E. V. Lutsenko. Maykop : ASU, 2011. 392 c.

3. Lutsenko E. V., Korzhakov V. E., Dubyansky A. A. Intellectual system of forecasting of consequences erroneous configuration bf the systems of safety MS Windows // Polythematic network electronic scientific magazine of the Kuban State Agrarian University. 2010. No. 05 (059). P. 53–78. URL: http://ej.kubagro.ru/2010/05/pdf/06.pdf (access date: 13/09/2024).

4. Lutsenko E. V., Golovin N. S. The automated it is system-kognitivnyj the analysis of a

[**] Для удобства читателей другие работы авторов размещены на его сайтах: http://lc.kubagro.ru и https://www.researchgate.net/profile/Eugene-Lutsenko/research

[**] For the convenience of readers, the author's other works are posted on his websites: http://lc.kubagro.ru и https://www.researchgate.net/profile/Eugene-Lutsenko/research

condition of information safety of firm on an example of computers with MS Windows // 2024. November. DOI: 10.13140/RG.2.2.35422.86088/1

5. Mughal A. A. Artificial Intelligence in Information Security: Exploring the Advantages, Challenges, and Future Directions // Journal of Artificial Intelligence and Machine Learning in Management. 2018. Vol. 2, No. 1. P. 22–34.

6. Li J. Cybersecurity meets artificial intelligence: a survey // Frontiers of Information Technology & Electronic Engineering. 2018. Vol. 19, No. 12. P. 1462–1474.

7. Artificial intelligence in cyber security: research advances, challenges, and opportunities / Z. Zhang, H. Ning, F. Shi [et al.] // Artificial Intelligence Review. 2022. Vol. 55. P. 1029–1055.

8. Dhingra M., Jain M., Jadon R. S. Role of artificial intelligence in enterprise information security: A review // Fourth International Conference on Parallel, Distributed and Grid Computing (PDGC). Waknaghat, 2016. P. 188–191.

9. Effectiveness of artificial intelligence techniques against cyber security risks apply of IT industry / B. Alhayani, H. J. Mohammed, I. Z. Chaloob // Materials Today: Proceedings. 2021. Vol. 531, No. 10. P.1016.

10. Increasing the level of network and information security using artificial intelligence / G. Pavlova, R. Dakov, G. Tsochev, R. Trifonov // Fifth International Conference on Advances in Computing, Communication and Information Technology. 2017. P. 83–88.

11. Kisimova Z. I., Begishev I., Sidorenko E. L. Artificial Intelligence and Problems of Ensuring Cyber Security // International Journal of Cyber Criminology. 2019. Vol. 13, No. 2. P. 564–577.

12. Das R., Sandhane R. Artificial intelligence in cyber security // Journal of Physics: Conference Series. IOP Publishing, 2021. Vol. 1964, No. 4. P. 042072.

13. Hashmi E., Yamin M. M., Yayilgan S. Y. Securing tomorrow: a comprehensive survey on the synergy of Artificial Intelligence and information security // AI and Ethics. 2024. July. P. 1–19.

Авторы заявляют об отсутствии конфликта интересов.

Статья поступила в редакцию 18.11.2024; *одобрена после рецензирования 25.11.2024*; *принята к публикации 26.11.2024*.

The authors declare no conflicts of interests.

The article was submitted 18.11.2024; *approved after reviewing 25.11.2024*; *accepted for publication 26.11.2024*.