Концептуальная модель многомерного представления эмпирических данных о состоянии объектов критической информационной инфраструктуры

Д.Г. Зыбин[1], К.О. Буркова[1], А.В. Калач[1,2]

[1]Воронежский институт Федеральной службы исполнения наказаний, Иркутская 1-а, Воронеж, Россия, 394072
[2]Воронежский государственный технический университет, Московский проспект 14, Воронеж, Россия, 394026

Аннотация. Представлена **к**онцептуальная модель, построенная на основании синтеза обобщенных представлений об отдельных составляющих их процессах и явлениях, описывающих поведение исследуемой системы (объекта) критической информационной инфраструктуры. Концептуальная модель обеспечения киберустойчивости объектов критической информационной инфраструктуры ведомственной информационной сети, интегрированных посредством информационно-телекоммуникационной сети общего пользования в киберпространство, отражающей стохастическую динамику деструктивных информационных воздействий на объекты представлена в виде общей схемы и процессов (функционирования, воздействий и обеспечения киберустойчивости) выражающей их наиболее существенные связи.

1. Введение

Разнообразное проникновение в системы безопасности свойственно российской сфере информационной безопасности в различных отраслях. Предприятия, чья деятельность связана с обработкой платежной информации, традиционно считаются лидерами в использовании решений обеспечения информационной безопасности.

Сведения о состоянии компаний, которые не обрабатывают платежные данные (например, организации, хранящие данные о клиентах и партнерах) еще не говорят о защищенности информации в этой сфере.

По сравнению с общемировой картиной Россия занимает лидирующее место по утечкам информации в такой сфере, как государственные органы и силовые структуры.

Данная отрасль занимает до 39% от всех случаев компрометации информации, зафиксированных в России (таблица) [1–7].

2. Описание модели

Проблема безопасности данных стоит на первом месте и в России, и в мире, которую пытаются решить за счет применения технических средств защиты. В рамках решения комплексной задачи обеспечения кибербезопасности пользователей информационной системы особое значение приобретает предварительная оценка таких систем с точки зрения их безопасности.

Таблица 1. Классификация утечек информации по источникам происхождения.

Отрасль	*Мир, %*	*Россия, %*
Банки и финансы	8,9	12,2
Медицина	19,0	8,5
Торговля	6,8	5,6
Высокие технологии	20,2	10,4
Промышленность и транспорт	4,9	3,0
Госорганы и силовые структуры	13,9	23,3
Образование	9,9	7,4
Муниципальные учреждения	6,7	15,9
Другое/не определено	9,8	13,7

При оценке состояния обеспечения киберустойчивого функционирования в условиях деструктивных информационных воздействий (ДИВ) необходимо исследовать информационной инфраструктуры ведомственной информационной сети (КИИ ВИС) как сложный активный динамический объект. Обеспечение фактическими параметрами о состоянии КИИ в непрерывной динамике и с учетом всей совокупности влияющих факторов представляет собой поток данных.

Данный поток содержит наборы управляющих сигналов и информации, представляющие собой достаточно разнородные и несогласованные данные, характеризующие работу технических средств обработки информации, программного обеспечения, сервисов, служб, коммутационного оборудования и т.д., входящих в состав объекта КИИ [8–14].

Под концептуальной моделью обеспечения киберустойчивости объектов КИИ ВИС, интегрированных посредством информационно-телекоммуникационной сети общего пользования в государственную ИС (ГИС) и киберпространство, отражающей стохастическую динамику (ДИВ) на объекты КИИ понимаются общие схемы исследуемых в теории киберустойчивости объектов КИИ (АСУ ВИС, ИТКС) и процессов (функционирования, воздействий и обеспечения киберустойчивости) выражая их наиболее существенные связи (рисунок 1) [7, 15].

При накоплении статистических данных получаются большие массивы разнородной информации о процессах, явлениях, событиях, объектах, субъектах и т.п., пополняемые непрерывно в режиме реального времени (по статистике, соотношение неструктурированной информации к структурированной три к двум) [16, 17].

На данный момент, существует достаточно большое количество различных подходов к анализу данных, начиная от традиционных, использующих методы математической статистики и заканчивая методами интеллектуальной обработки данных.

Каждый из существующих методов предполагает представление собранных данных в определенном формате для возможности их дальнейшей обработки и получения результатов в виде, понятном для человека.

Для применения методов математической статистики информация должна быть представлена в виде однородных данных, а методы интеллектуальной обработки данных позволяют обрабатывать достаточно разнородные и несогласованные данные [15, 17].

Анализ опыта применения технологий интеллектуального анализа данных [18] позволяет утверждать, что для представления разнородной несбалансированной информации в сбалансированном виде для дальнейшего анализа используются специально спроектированные информационные хранилища для хранения данных. Отличительной чертой этих хранилищ является то, что структурированная и неструктурированная информация могут обрабатываться совместно, как единое целое.

Качество представляемой информации после аналитической обработки СППР будет определяться, прежде всего, объемом накопленных эмпирических данных и применяемым методом интеллектуального анализа данных [15].

Необходимость накопление эмпирических данных в специально спроектированном информационном хранилище способствует формированию ведомственного электронного, постоянно пополняющегося архива поведенческой активности самых различных объектов, от технических средств обработки информации отдельных объектов КИИ, до КИИ ВИС в целом, для чего предлагается построить соответствующую многомерную базу данных, рисунок 2.

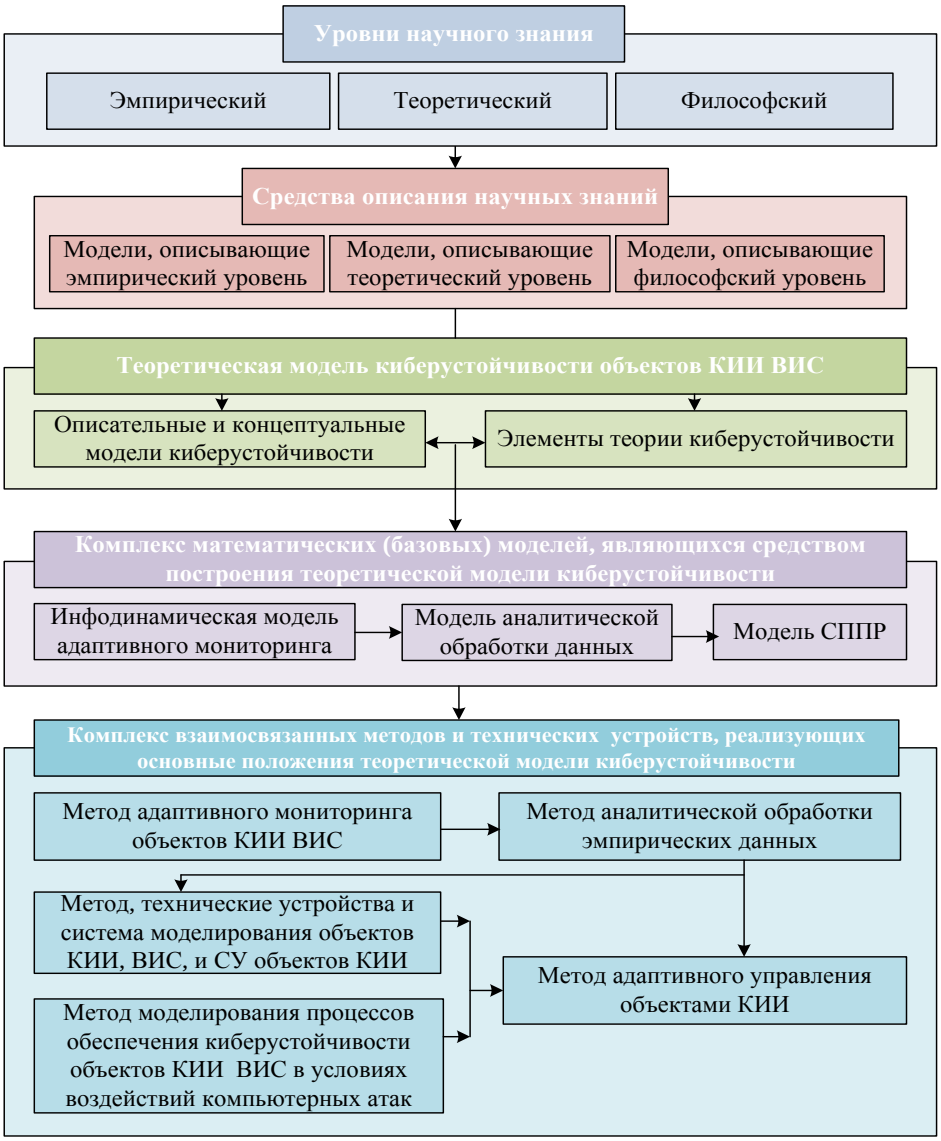

Рисунок 1. Концептуальная модель как средство описания научных знаний о киберустойчивости объектов КИИ ВИС.

Таким образом, использование технологии информационного хранилища с аналитической обработкой информации на базе многомерной базы данных позволяет [15, 16]:

– проводить самые различные и сколь угодно подробные классификации той или иной совокупности внешних и внутренних, конструктивных и деструктивных информационных воздействий, фактических выходных данных и параметров, описывающих систему и действия человеческой составляющей по самым разнообразным признакам. Такие классификации обеспечивают точное понимание взаимосвязи тех или иных характеристик любого объекта КИИ, тем самым обеспечив анализ как эмерджентных, так и синергетических свойств;

– осуществлять многомерный статистический математический анализ. Этот анализ

позволяет находить корреляции между самыми различными параметрами, характеристиками, событиями и т.п. Теоретические модели отвечает на вопрос – почему, а затем, выявив причинно-следственные закономерности, позволяют формировать рекомендации о порядке действий;

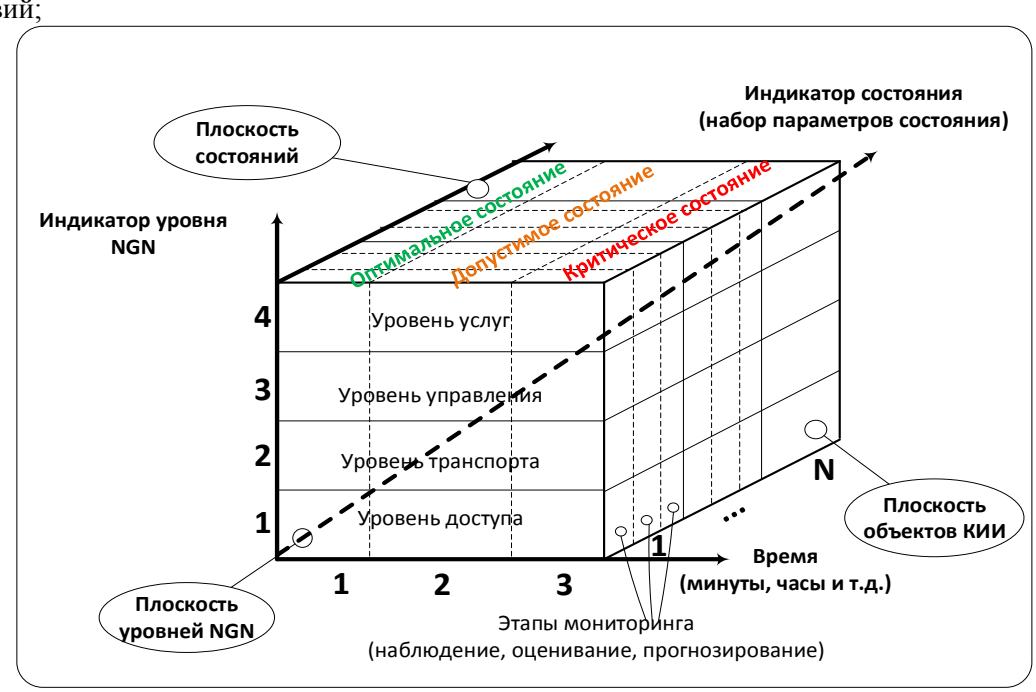

Рисунок 2. Модель многомерного представления информации о состоянии объектов КИИ.

– выполнять прогнозирование на основе классификаций и выявленной корреляционной связи факторов, определять наиболее целесообразный способ воздействия для того, чтобы один набор факторов, характеризующий текущее состояние того или иного объекта КИИ (параметры состояния, должностное лицо его использующее, разные события и т.п.) было преобразовано в заданное с прогнозированием необходимого времени;

– обеспечить СППР необходимой информацией для обеспечения адекватного управления устойчивостью функционирования КИИ ВИС, осуществив полный охват всех решаемых ей задач, включая традиционно трудные для автоматизации задачи планирования и прогнозирования.

3. Литература

[1] Утечки данных. Россия. 2018 год [Электронный ресурс]. – Режим доступа: https://www.infowatch.ru/resources/analytics/reports (01.11.2019).

[2] Смирнов, А.И. Глобальная безопасность в цифровую эпоху: стратагемы для России / А.И. Смирнов – М.: ВНИИ Геосистем, 2014. – 394 с.

[3] Макаренко, С.И. Информационное оружие в технической сфере: терминология, классификация, примеры / С. И. Макаренко // Системы управления, связи и безопасности. – 2016. – № 3. – С. 292-376.

[4] Щеглов, А.Ю. Защита компьютерной информации от несанкционированного доступа / А.Ю. Щеглов – СПб.: Наука и техника, 2004. – 384 с.

[5] Лукацкий, А.В. Обнаружение атак / А.В. Лукацкий – СПб.: БХВ-Петербург, 2001.

[6] Макаренко, С.И. Терминологический базис в области информационного противоборства / С.И. Макаренко, И.И. Чукляев // Вопросы кибербезопасности. – 2014, Т. 1, № 2. – С. 13-21.

[7] Захарченко, Р.И. Противоборство в киберпространстве: концептуальные основы и терминологический базис / Р.И. Захарченко, И.Д Королев, Е.Л. Мирошниченко // Труды V Международной НПК – КубГТУ, 2017.

[8] Баженов, Л.Б. Строение и функции естественнонаучной теории / Л.Б. Баженов – М.: Наука, 1978. – 225 с.
[9] Раджабов, У.А. Динамика естественнонаучного знания (системно-методологический анализ) / У.А. Раджабов – М.: Наука, 1982. – 336 с.
[10] Зиновьев, А.А. Основы логической теории научных знаний / А.А. Зиновьев – М.: Наука, 1967. – 261с.
[11] Печенкин, А.А. Обоснование научной теории / А.А. Печенкин – М.: Наука, 1991. – 184 с.
[12] Гриняев, С.Н. Поле битвы – киберпространство. Теория, приемы, средства, методы и системы ведения информационной войны / С.Н. Гриняев – М.: Харвест, 2004. – 426 с.
[13] Волкова, В.Н. Теория систем и системный анализ в управлении организациями: справочник / В.Н. Волкова, А.А. Емельянов – М.: Финансы и статистика, 2006. – 848 с.
[14] Волкова, В.Н. Основы теории систем и системного анализа / В.Н. Волкова, А.А. Денисов – СПб.: Изд-во СПбГТУ, 1977. – 512 с.
[15] Бочков, М.В. Модель адаптивной защиты информации от НСД в условиях информационного противоборства / М.В. Бочков, В.Ф. Комарович, И.Б. Саенко // Научно-технический сборник. – 2002. – № 4. – С. 21-25.
[16] Симанков, В.С Адаптивное управление сложными системами на основе теории распознавания образов / В.С. Симанков, Е.В. Луценко – Краснодар: Издательство Кубанского государственно технологического университета, 1999. – 318 с.
[17] Антонов, В.Н. Адаптивное управление в технических системах / В.Н. Антонов, В.А. Терехов, И.Ю. Тюкин – СПб.: Издательство Санкт-Петербургского университета, 2001. – 244 с.
[18] Срагович, В.Г. Теория адаптивных систем / В.Г. Срагович – М.: Наука, 1976. – 319 с.

Conceptual model for multidimensional presentation of empirical data on the state of critical information infrastructure facilities

D.G. Zybin[1], K.O. Burkova[1], A.V. Kalach[1,2]

[1]VRI of the FPS of Russia, Irkutskaya 1-a, Voronezh, Russia, 394072
[2]VSTU, 20-letya Oktyabry str. 84, Voronezh, Russia, 394026

Abstract. A conceptual model presented, built based on synthesis of generalized perceptions of their individual processes and phenomena, describing the behavior of the investigated system (object) of the critical information infrastructure. The conceptual model of ensuring cyber stability of objects of the critical information infrastructure of the departmental information network, integrated through the public information and telecommunication network into cyberspace, reflecting the stochastic dynamics of destructive information effects on objects in the form of a general scheme and processes (functioning, impacts and ensuring cyber stability) expressing their most significant connections presented.