Концептуальная секьюритологическая модель релевантных геоинформационных ресурсов в логистике

Conceptual model of security relevant geoinformation resources in logistics

Медведев / Medvedev V.
Владимир Арсентьевич
(krat29@rambler.ru)
кандидат экономических наук.
ФГБОУ ВПО «Национальный минерально-сырьевой университет «Горный», доцент.
г. Санкт-Петербург

Ключевые слова: геоинформатика – geoinformatics; логистика – logistics; релевантность – relevance; принципы безопасности – safety principles; концептуальная модель – conceptual model; эвристическая диаграмма – heuristic chart.

Рассматриваются общие принципы и требования обеспечения безопасности логистической фирмы. На уровне концептуального моделирования предложен трёхуровневый сценарий создания модели безопасности и зависимость ценности информации, получаемой принимающим решение лицом, от её объёма. Приводится концептуальная, укрупнённая модель защиты релевантных геоинформационных ресурсов в логистике.

The general principles and requirements of security logistics company are considered. Three-level script of the security model creation is proposed on the conceptual modeling level. Also the dependence of the value of information received by decision-makers person of its volume. Conceptual, bigger security model relevant geographic information resources in logistics is provided.

Геоинформационные ресурсы при принятии оптимизационных логистических решений играют важнейшую, порой главную, роль. Геоинформационные знания их актуализация и постоянное уточнение по сформированным неформальным информационным запросам (релевантность) необходимы для принятия логистических решений, оптимизирующих цепи поставок (ЦП), таких как:

· выбор оптимального маршрута и условий поставок;

· определение территориальных преимуществ у всех звеньев ЦП (поставщики, заказчики-грузополучатели, склады и терминалы, транспортные средства и инфраструктура);

· коррекция управления поставками при изменении климатических и временных условий и др.

Использование логистом в своей работе современных геоинформационных систем (ГИС), обеспечивающих выбор своевременных оптимизационных решений, даёт ему конкурентные преимущества на рынке посредников, управляющих ЦП. Следовательно, обеспечение должного уровня информационной безопасности становится важнейшим атрибутом успешности его профессиональной деятельности.

Организация и функционирование комплексной системы обеспечения безопасности логистической (предпринимательской) деятельности в целях максимальной эффективности должны основываться на принципах, приведённых на рис. 1 [1, с. 12–13].

Эффективность использования системы защиты геоинформации зависит от правильного осознания самого объекта защиты, выбора средств и режимов защиты, определение возможных угроз и своевременной оценки возможного урона, с учётом специфики снятия, модернизации и хранения геоданных. Эти данные можно разделить на статические (картографические) и динамические (состояние объектов учёта и инфраструктуры, климатические и временные изменения и др.), что обуславливает режим работы ГИС, а также различные методы и средства их защиты.

Так, во время Великой Отечественной войны пока театр сражений проходил на советской территории советские полевые офицеры предпочитали использовать трофейные немецкие карты, так как они были более точными. Картина кардинально изменилась, когда линия фронта отодвинулась на немецкую территорию – немецкие офицеры по той же причине старались пользоваться советскими картами. Этот парадокс объяснялся традиционными привычками картографов «секретить» географические данные, связанные с военными объектами, находившимися на территории в момент снятия или уточнения этих данных.

На уровне концептуального моделирования можно предложить трёхуровневый сценарий создания модели безопасности (рис. 2), когда объектом защиты является релевантная геоинформация, то есть необходимые для своевременного и эффективного принятия решения знания и оперативноценные данные.

Нетрадиционными в подходе к подобному моделированию являются такие современные аспекты как

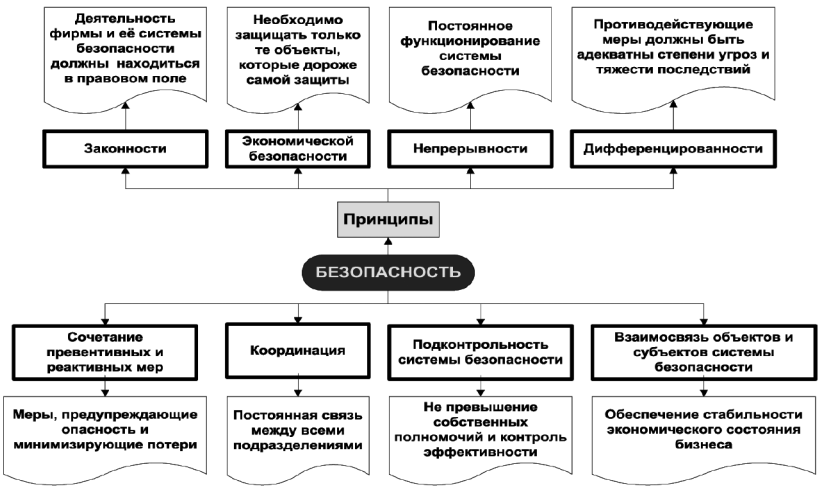

Рис. 1. Требования обеспечения безопасности логистической фирмы

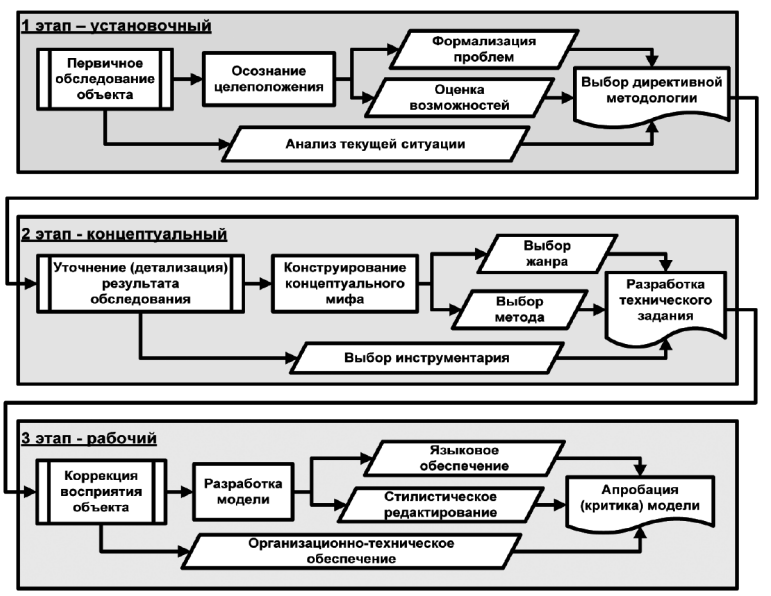

Рис. 2. Сценарий создания модели системы защиты

Рис. 3. Эвристическая диаграмма релевантности геоинформации

Рис. 4. Логистическое управление материальным потоком

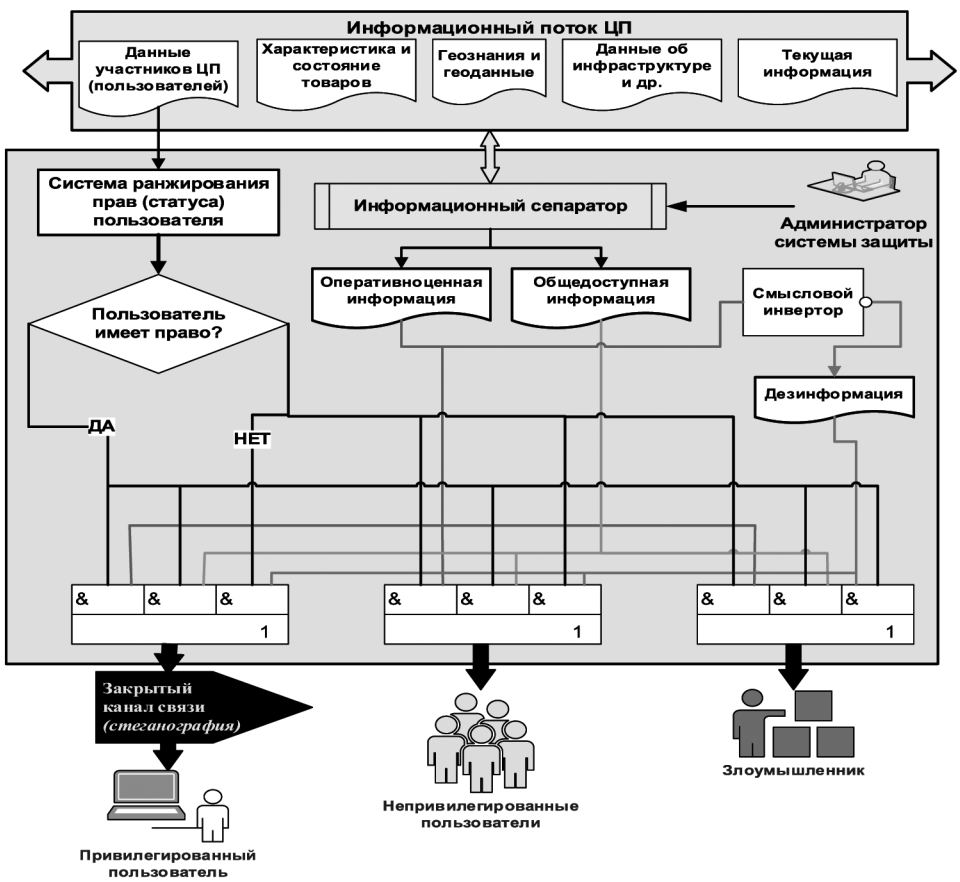

Рис. 5. Концептуальная секьюритологическая модель

конструирование концептуального мифа и выбор жанра для его апробирования [2, с. 55, 136].

Правильность выбранного концептуального мифа (информационного образа объекта управления и констатация поставленной цели его преобразования) подтверждается при опытном подтверждении основных его канонов и принципов модификации.

Выбор жанра при моделировании определяется компетентностью и традициями его создателей и потенциальных заказчиков (отчёт по ГОСТу, бизнес-план, сценарий, презентация и др.).

При конструировании концептуальной модели системы защиты геоинформации необходимо проанализировать содержательное значение геоинформационных ресурсов с целью из значимости для принятий эффективных логистических решений. Целесообразно разделить имеющиеся знания на 3 основные группы:

· оперативноценная (релевантная – то есть необходимая для достижения поставленной цели) информация – требует соблюдения принципов информационной безопасности;

· избыточная и неактуальная информация – не требует затрат на её защиту;

· дезинформация (иррелевантная информация – мешающая для достижения поставленной цели) – требует наиболее значимых затрат для её эффективного формирования и доведения до потенциальных злоумышленников.

На рис. 3 представлена эвристически сформулированная (не имеющая опытного подтверждения) зависимость ценности («вредности») информации, получаемой принимающим решение лицом, от её объёма *Q*. При этом следует учитывать, что получение информации в объёме сверхнеобходимом для уверенного принятия решения приводит к информационным «завалам», когда даже уже сформированное решение не может быть принято из-за возникших подозрений в их недостаточной релевантности. Своевременность принятия решения является в логистике основополагающим фактором успешного управления ЦП.

Исходя из изложенных положений, а также традиционной схемы логистического управления ЦП (материальным потоком), приведённой на рис. 4 [3, с. 220], можно предложить следующую (рис. 5) концептуальную, укрупнённую модель защиты (секьюритологическая модель) релевантных геоинформационных ресурсов в логистике.

Как видно из схемы, в соответствии с логикой информационной сепарации и определения прав пользователя, привилегированный пользователь получит всю информацию кроме дезинформации, обычные легитимные пользователи – только общедоступные информационные ресурсы, а злоумышленник будет приравнен к привилегированному пользователю, но вместо оперативноценной информации получит её «кривое отражение».

Смысловое инвертирование является высокоинтеллектуальной задачей, алгоритм решения которой зависит не только от имеющегося аппаратно-программного инструментария, но и от выбранного концептуального мифа, то есть от выбранных канонов определения ценности («вредности») содержания и форм представления информации. Важным звеном в этой модели играет канал связи для доведения информации привилегированным пользователям, находящимся на некотором удалении от системы защиты.

В этом случае необходимо использовать либо технически и организационно защищённые каналы, либо использование стеганографических методов, которые собственно скрывает само наличие связи. В отличие от криптографии, где злоумышленник точно может определить является ли передаваемое сообщение зашифрованным текстом, методы стеганографии позволяют встраивать секретные сообщения в безобидные послания так, чтобы невозможно было заподозрить существование встроенного тайного послания. Как вариант, можно упаковывать информацию, требующую защиты, в пачки-контейнеры, которые маскируются путём их скремблирования (перемешиванием с неким шумовым сигналом) с массивом общедоступной информации.

Обычно на практике средой сбора, хранения и распределения геоинформации является глобальная сеть – Интернет. Его влияние и распространение хорошо проиллюстрировано Министерством торговли США (U. S. Department of Commerce): так для достижения аудитории в 50 млн. человек для радио потребовалось 50 лет, для ТВ – 13 лет, а Интернету только 4 года [4, с. 224].

Глобальная популярность Интернета является причиной создания широкого спектра методов и аппаратно-программных средств, как для атак на чужие информационные ресурсы, так и для их защиты. Это необходимо учитывать при выборе инструментария, обеспечивающего реализацию выбранной концепции защиты геоданных.

Литература

1. Захаров, О.Ю. Практическая секьюритология: руководство по безопасности бизнеса / О.Ю. Захаров. – Ростов н/Д: Феникс, 2010. – 320 с.

2. Титц, С. Язык организаций. Интерпретация событий и создание значений / С. Титц, Л. Коэн, Д. Массон ; пер. с англ. А. Лысых. – Х.: Изд-во Гуманитарный центр, 2008. – 324 с.

3. Антикризисная логистика: методологические основы / В.М. Прохоров [и др.]. – СПб.: Изд-во Политехн. ун-та, 2014. – 238 с.

4. Фейд, Т. Кибершпионаж / Т. Фейд, М. Нордфелт, С. Ринг; пер. с англ. И.В. Багаутдиновой. – М.: НТ Пресс, 2008. – 384 с.