УДК 004.056.53

И.В. Котенко, И.Б. Саенко, А.В. Чернов, М.А. Бутакова

ПОСТРОЕНИЕ МНОГОУРОВНЕВОЙ ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Котенко И.В., Саенко И.Б., Чернов А.В., Бутакова М.А. **Построение многоуровневой интеллектуальной системы обеспечения информационной безопасности для автоматизированных систем железнодорожного транспорта.**

Аннотация. В статье рассматриваются особенности построения и функционирования автоматизированных систем железнодорожного транспорта. В качестве основных отличительных факторов выделены достаточно большое многообразие и разнородность таких систем, их взаимная связность и связность с сетями общего пользования и сильная разнородность внутренних пользователей. Представлена и рассмотрена архитектура многоуровневой системы обеспечения информационной безопасности, которая предложена для защиты информации в автоматизированных системах железнодорожного транспорта. Для хранения данных о безопасности в многоуровневой интеллектуальной системе защиты предложено использование гибридного онтологического репозитория. Для интеллектуальных сервисов анализа данных, находящихся на верхнем уровне рассматриваемой системы защиты, предложены формальные постановки задачи. Анализ этих постановок показал, что разработка интеллектуальных сервисов управления корреляцией, анализа защищенности и моделирования атак следует относить к задачам анализа. Интеллектуальные сервисы поддержки принятия решений и визуального анализа данных относятся к задачам синтеза.

Ключевые слова: автоматизированная система, железнодорожный транспорт, информационная безопасность, концепция, формальная постановка задачи.

Kotenko I.V., Saenko I.B., Chernov A.V., Butakova M.A. **The construction of a multi-level intelligent information security system for automated systems of railway transport**.

Abstract. The paper discusses features of construction and operation of automated systems of railway transport. As main distinguishing factors, the great variety and diversity of such systems, their mutual co-relationships and links with public networks, and strong heterogeneity of internal user are highlighted. The architecture of a multi-level intelligent information security system that proposed to protect information in automated systems of railway transport is suggested and discussed. To store data about security in a multilevel intelligent system of protection it is proposed to use a hybrid ontology repository. Formal task statements for intelligent services of data analysis at the top level of the reviewed protection systems are offered. Analysis of these statements showed that development of intelligent services for correlation management, security analysis and attack modeling should be assigned to analysis tasks. Intelligent services for decision support and visual data analysis are among the synthesis tasks.

Keywords: automated system, railway transport, information security, концепция, formal task statement.

1. Введение. Железнодорожный транспорт (ЖТ) является основным звеном транспортного комплекса России, так как его доля в об-

щем грузообороте страны превышает 40 процентов, а в пассажиропотоке — 30 процентов. Тем самым ЖТ имеет ключевое значение для функционирования и развития социальной, экономической, финансовой, а также оборонной и других сфер общественной жизни. При этом наблюдается устойчивая тенденция повышения грузооборота (не менее чем на 3 процента в год) и, соответственно, значимости ЖТ [1]. Для поддержания этой тенденции на ЖТ внедряются автоматизированные информационные и управляющие системы, позволяющие осуществлять оперативный сбор достоверной информации обо всех показателях деятельности в ОАО «РЖД». Они объединяются в корпоративную АСУ ЖТ, являющуюся основным средством эффективного управления ресурсами и направлениями производственно-технологической и административно-хозяйственной деятельности ЖТ. По имеющимся оценкам, общее количество автоматизированных систем (АС) в составе АСУ ЖТ, обслуживающих различные направления и виды деятельности компании, превышает 6000 [2].

Однако широкое внедрение АС на ЖТ неизбежно поднимает вопрос обеспечения защиты информации. Появление в АСУ ЖТ новых продуктов современных телекоммуникационных технологий влечет появление новых видов угроз информационной безопасности (компьютерных атак), с которыми традиционно имеющиеся средства защиты информации (к их числу относятся криптографические средства, включая сети VPN, антивирусные средства, системы обнаружения атак, системы дискреционного, мандатного и ролевого доступа и пр.) справляются недостаточно эффективно.

Традиционные средства защиты информации относятся к группе «априорных» средств, которые действуют до попытки нарушения безопасности информации (атаки). В критических инфраструктурах, к числу которых относится и ЖТ, необходимо активно развивать и внедрять группу средств «апостериорной» защиты информации, которые, как правило, действуют после обнаружения атак (вторжения), однако способны, анализируя данные о произошедших событиях безопасности, осуществлять прогностический анализ защищенности, оказывать поддержку в выработке адекватных контрмер и, тем самым, реализовывать принцип «проактивной» защиты информации [3]. К числу таких систем можно отнести системы мониторинга и управления безопасностью нового поколения, обладающие широкими интеллектуальными возможностями в области представления, хранения, обработки и отображения информации о безопасности [4]. Системы такого рода обладают высокой масштабируемостью, возможностями

обнаружения «редких» атак и совместного анализа событий безопасности на различных уровнях (сетевом уровне, уровне физических управляющих элементов/датчиков и бизнес–уровне) [5]. Поэтому вопросы, связанные с построением такой многоуровневой интеллектуальной системы обеспечения безопасности информации для АС ЖТ, являются целью настоящей работы.

2. Особенности построения и функционирования АСУ ЖТ. АСУ ЖТ имеет трехуровневую структуру, как показано на рис. 1.

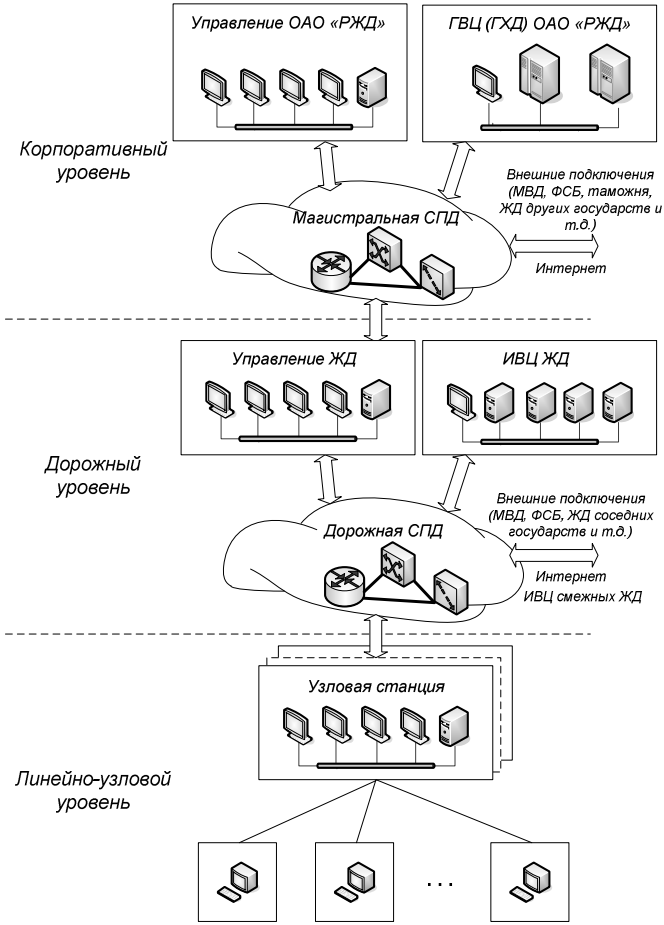

Рис. 1. Структура корпоративной АСУ ЖТ.

Топология АСУ ЖТ имеет радиально–узловую структуру и выраженное деление на подсистемы по Железным дорогам (ЖД) с узлами в Информационно–вычислительных центрах (ИВЦ) ЖД и центром в Главном вычислительном центре (ГВЦ) ОАО «РЖД». На верхнем (корпоративном) уровне располагаются Центральный аппарат (Управление), ГВЦ и Главное хранилище данных (ГХД) ОАО «РЖД». Здесь решаются задачи корпоративного управления ЖТ. Через магистральную сеть передачи данных (СПД) объекты корпоративного уровня связываются с объектами ЖД, с сетью Интернет, а также с внешними объектами — подразделениями МВД России, ФСБ России, таможни, организациями, входящими в состав железных дорог других государств и т.д.

На среднем (дорожном) уровне располагаются управления и ИВЦ Дорог. Каждая ЖД имеет свою сложную информационно–вычислительную инфраструктуру. Через дорожную СПД они связываются с подчиненными объектами нижнего, линейно–узлового уровня — узловыми станциями, станциями и линейными предприятиями, а также с внешними объектами, смежными дорогами и сетью Интернет.

Автоматизированные системы, входящие в состав корпоративной АСУ ЖТ, обеспечивают автоматизированное решение задач в следующих областях:

- грузовые перевозки;
- пассажирские перевозки;
- перевозочный процесс в целом;
- управление финансами и ресурсами;
- управление инфраструктурой.

Перечень ключевых АС ЖТ, отвечающих за решение этих задач, приведен в табл. 1–5. В таблицах указаны следующие уровни: 1 — корпоративный; 2 — дорожный; 3 — линейно–узловой.

Комплекс АСУ грузовыми перевозками (ГП) (табл. 1) насчитывает несколько десятков крупных взаимодействующих автоматизированных систем и является сложнейшим информационным комплексом. В качестве ядра комплекса выступает система АСОУП–2. Также АСУ ГП осуществляет взаимодействие по целевому ориентированию для решения следующих задач:

- взаимодействия с грузоотправителями в условиях электронного документооборота;
- управления и контроля выполнения грузовых перевозок;
- хранения и анализа информации о выполненных перевозках;

- моделирования оптимального управления вагонопотоками на различных уровнях иерархии.

Таблица 1. **Автоматизированные системы для грузовых перевозок**

Название	Назначение	Уровень
АСОУП–2	Оперативное управление перевозками верхнего уровня. Ядро комплекса для грузовых перевозок.	1, 2
АКСФТО	Фирменное транспортное обслуживания. Взаимодействие с грузоотправителями в условиях электронного документооборота.	1, 2
ЭТРАН	Работа с электронной транспортной накладной. Взаимодействие с грузоотправителями в условиях электронного документооборота.	2, 3
ЕК ИОДВ	Интегрированная обработка дорожных ведомостей. Взаимодействие с грузоотправителями в условиях электронного документооборота.	2, 3
АСОУП	Оперативное управление перевозками нижнего уровня. Управление и контроль выполнения грузовых перевозок.	1, 2
ДИСПАРК	Пономерной учет, контроль дислокации, анализ работы и регулирования вагонного парка	2, 3
ДИСКОН	Управление контейнерными перевозками	2, 3
ДИСЛОК	Управление тяговыми ресурсами	2, 3
ЕМПП	Работа с единой моделью перевозочного процесса	1, 2, 3
КИХ	Хранение и анализ информации о выполненных перевозках (корпоративное хранилище)	1, 2
ЦУП РЖД	Моделирование оптимального управления вагонопотоками	1
РЦУП	Моделирование оптимального управления вагонопотоками	2
ЕДЦУ	Диспетчерское управление железнодорожными перевозками	3

Базовой АСУ пассажирскими перевозками является система «Экспресс–3». Одной из приоритетных задач, решаемых на основе АСУ «Экспресс–3», является автоматизация бизнес-процессов в части пригородных и дальних пассажирских перевозок с использованием сети Интернет, при этом учитывается их лояльность и доходность. Внедрение данной системы привело, с одной стороны, к сокращению эксплуатационных расходов, а с другой — к улучшению обслуживания пассажиров [6].

АСУ «Экспресс–3», в свою очередь, взаимодействует с рядом других АС, наименование и назначение которых представлены в табл. 2.

Таблица 2. **Автоматизированные системы для пассажирских перевозок**

Название	Назначение	Уровень
Экспресс–3	Сбыт и учет электронных билетов с использованием сети Интернет	1, 2, 3
ДУТИСС	Динамическое управление тарифами	1, 2
АБД	Аналитическая база данных АСУ «Экспресс»	1, 2, 3
АСУПВ	Анализ надежности и качества выполненных ремонтов.	2, 3

Комплекс АСУ перевозочным процессом (табл. 3) базируется на следующих системах: Центр управления перевозками (ЦУП), Дорожный центр управления перевозками (ДЦУП) и диспетчерский центр управления местной работой (ЦУМР). В совокупности эти системы представляют собой главный орган оперативного диспетчерского управления движением поездов, который обеспечивает бесперебойные перевозки пассажиров и грузов на железнодорожном транспорте общего пользования. Этими АС также решаются задачи оптимизации использования пропускной способности инфраструктуры железных дорог, тяговых и погрузочных ресурсов, организации движения поездов в соответствии с графиком движения и планом формирования поездов при безусловном обеспечении безопасности движения поездов. В перспективе планируется развивать новое направление — интеллектуальное управление движением поездов, включая грузовые и пассажирские высокоскоростные поезда.

Таблица 3. **Автоматизированные системы для перевозочного процесса**

Название	Назначение	Уровень
ЦУП	Управление перевозками на высшем уровне	1
ДЦУП	Управление перевозками на уровне Дороги	2
ЦУМР	Диспетчерское управление местной работой	3

Комплекс АС управления финансами и ресурсами обеспечивает реализацию единой маркетинговой, финансовой и ресурсной политики отрасли. В его состав входят следующие системы (табл. 4):

- единая корпоративная автоматизированная система управления финансами и ресурсами (ЕКАСУФР);

- единая корпоративная автоматизированная система управления трудовыми ресурсами (ЕКАСУТР);

- автоматизированная система мониторинга показателей социальной сферы (АС ОАО «РЖД»).

Таблица 4. **Автоматизированные системы управления финансами и ресурсами**

Название	Назначение	Уровень
ЕКАСУФР	Единое корпоративное управления финансами и ресурсами	1, 2
ЕКАСУТР	Единое корпоративное управления трудовыми ресурсами	1, 2
АС ОАО «РЖД»С	Мониторинг показателей социальной сферы	1, 2

ЕКАСУФР состоит из подсистемы анализа доходов от грузовых перевозок, подсистемы анализа заключаемых договоров и подсистемы анализа наличности. Она взаимодействует с рядом других подсистем, которые передают в нее результаты финансово–экономической деятельности, доходную и расходную части бюджета. Частота поступления этих данных — один раз в сутки. В обратном направлении передается планово–экономическая, нормативная и другая информация.

Система ЕКАСУТР осуществляет учет персонала (более 1,3 млн. человек) и обеспечивает функции нормирования труда, учета рабочего времени, расчета заработной платы и т.д.

Основу комплекса АС управления инфраструктурой (табл. 5) представляет Единая корпоративная автоматизированная система управления инфраструктурой (ЕКАСУИ), решающая следующие задачи: создание единой базы объектов инфраструктуры; эффективное планирование и реализация текущей деятельности на основе оперативных данных.

ЕКАСУИ является основным инструментом работы дорожных центров управления содержанием инфраструктуры (ЦУСИ). Основными задачами ЦУСИ являются: обеспечение содержания инфраструктуры в соответствии с нормативными требованиями; повышение эффективности и качества деятельности; диагностика и мониторинг хозяйства автоматики и телемеханики.

Таблица 5. **Автоматизированные системы управления финансами и ресурсами**

Название	Назначение	Уровень
ЕКАСУИ	Ведение базы данных об объектах инфраструктуры. Планирование и реализация текущей деятельности на основе оперативных данных.	1, 2, 3
ЦУСИ	Обеспечение содержания инфраструктуры в соответствии с нормативами. Диагностика и мониторинг хозяйства автоматики и телемеханики.	1, 2, 3

Анализ построения и функционирования рассмотренных АС ЖТ позволил сформулировать следующие выводы, имеющие непосредственное отношение к обеспечению их информационной безопасности:

1) все АС ЖТ являются неоднородными по применяемым в них средствам и технологиям;

2) все АС ЖТ взаимоувязаны между собой посредством магистральной и дорожных СПД, а также каналов удаленного доступа;

3) пользователи АС ЖТ представляют собой достаточно многочисленный контингент сотрудников, отличающийся уровнем подготовки и полномочиями.

Рассмотрим теперь возможности существующей системы защиты информации в АСУ ЖТ.

3. Возможности существующей системы защиты информации. Существующая в АСУ ЖТ система защиты информации представляет собой достаточно сложную организационно–техническую систему, к основным целям функционирования которой относятся: обеспечение защиты информации, не относящейся к категории "государственная тайна"; внедрение и эксплуатация технических подсистем комплексов и средств обеспечения информационной безопасности; обеспечение доступности соответствующих категорий информации для пользователей ОАО "РЖД", других организаций и частных лиц; управление информационной инфраструктурой; аудит уровня информационной безопасности. В ее составе выделяются следующие подсистемы [7]:

- система антивирусной защиты (САЗ);
- автоматизированная система "Технологический электронный документооборот с применением электронной цифровой подписи" (АС ЭТД);
- реестр автоматизированных систем и архитектурных моделей ОАО «РЖД» (АСУ «Реестр АС и АМ»);

- система защиты информации от несанкционированного доступа (СЗИ НСД) и другие.

Важнейшим принципом обеспечения безопасности информации в АС ЖТ является функциональная интеграция специализированных программно–технических комплексов защиты с программно–техническими комплексами передачи и обработки информации, имеющими собственные встроенные средства защиты с мощной функциональностью — операционными системами рабочих станций и серверов, активным сетевым оборудованием [8]. Активное совместное использование специализированных и встроенных средств защиты в совокупности с подсистемой антивирусной защиты способствует предотвращению угроз распространения разрушающих программных средств (вирусов) и «троянских» программ.

В то же время рост количества возможных типов кибератак определяет необходимость реализации ряда дополнительных мер обеспечения информационной безопасности, включая использование только проверенных средств мониторинга и управления безопасностью и мониторинг кибератак [9]. В силу того, что РЖД, как любая критическая инфраструктура, требует повышенного внимания к информационной безопасности, в систему защиты АС ЖТ необходимо внедрять интеллектуальные механизмы, которые делают эту систему многоуровневой интеллектуальной и наделяют принципиально новыми функциональными возможностями. Рассмотрим подробнее концепцию построения такой системы защиты.

4. Концепция построения многоуровневой интеллектуальной системы обеспечения защиты информации для АС ЖТ. Создание многоуровневой интеллектуальной системы обеспечения информационной безопасности является перспективным направлением обеспечения безопасности информации для автоматизированных систем критических инфраструктур, к числу которых относятся и АС ЖТ.

В основу построения такой системы предлагается положить технологию мониторинга и управления информационной безопасностью, которая в мировой литературе получила название «управление информацией и событиями безопасности» (Security Information and Event Management, SIEM) [10]. SIEM–система нового поколения отличается наличием ряда интеллектуальных сервисов и функциональных возможностей, таких как гибридное онтологическое информационное хранилище (репозиторий), логический вывод, межуровневая корреляция, моделирование поведения, анализ защищенности системы, визуальный анализ и другие [11]. Как показали последние исследования,

SIEM–системы нового поколения обладают высокой масштабируемостью, способностью вырабатывать адекватные контрмеры в условиях неполноты и противоречивости поступающих данных, способностью обнаруживать угрозы и нарушения безопасности не только на информационном уровне, но и на других уровнях защищаемой инфраструктуры [12, 13]. Предполагается, что реализация многоуровневой интеллектуальной системы обеспечения информационной безопасности позволит значительно повысить транспортную безопасность и безопасность населения на железнодорожном транспорте.

Архитектура предлагаемой для АС ЖТ многоуровневой интеллектуальной системы обеспечения информационной безопасности представлена на рис. 2.

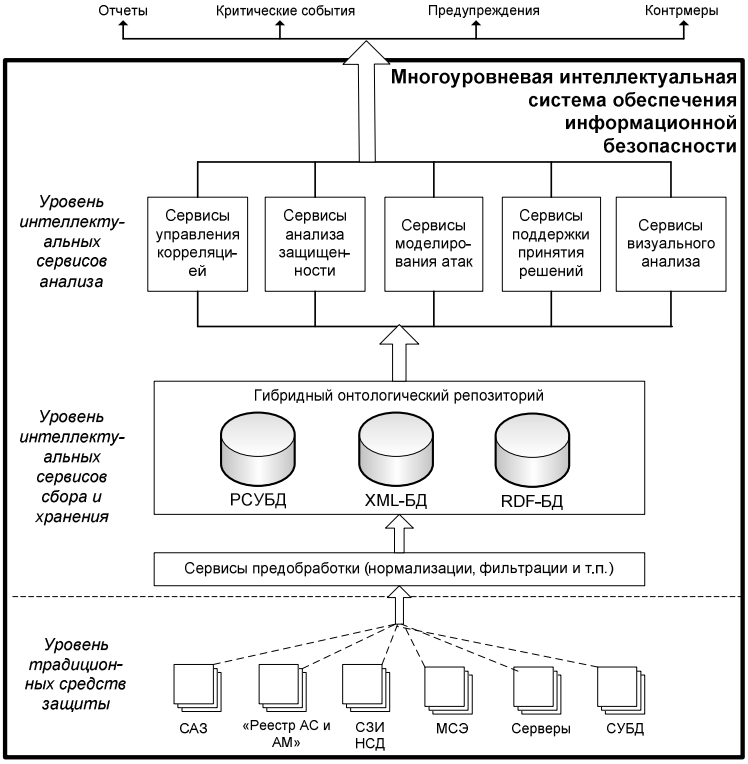

Рис. 2. Архитектура многоуровневой интеллектуальной системы обеспечения информационной безопасности для АС ЖТ.

Как видно из приведенного рисунка, в данной системе можно выделить следующие три уровня:

- уровень традиционных средств защиты (нижний);
- уровень интеллектуальных сервисов сбора и хранения данных (средний);
- уровень интеллектуальных сервисов анализа данных (высший).

На нижнем уровне данной системы находятся традиционные средства защиты информации, используемые в настоящее время в АС ЖТ. Они в подавляющем своем большинстве выполняют функцию «априорной» защиты информации. Однако, помимо этого, они еще являются источниками данных о событиях безопасности, т.е. о событиях, происходящих в различных элементах АС ЖТ и способных привести к нарушению безопасности. Помимо традиционных средств защиты, информация о событиях безопасности вырабатывается рядом других средств, которые номинально не являются средствами защиты. К их числу можно отнести, например, операционные системы, установленные на серверах и рабочих станциях (OS/390, Windows и другие), а также системы управления базами данных (СУБД), такие как DB2 для мэйнфреймов zSeries 900, установленных в ГВЦ. Они также включены в состав элементов нижнего уровня, так как являются источниками необходимой для анализа информации.

На среднем уровне осуществляется сбор, предварительная обработка и хранение информации о событиях безопасности. Для сбора данных используются два основных метода: «выталкивание» и «втягивание». Суть метода «выталкивания» заключается в том, что источник сам посылает данные о событиях безопасности в систему. В методе «втягивания» система сама осуществляет процесс получения данных о событиях безопасности.

Предварительная обработка информации включает в себя нормализацию, фильтрацию, корреляцию, агрегацию и классификацию. Нормализация сводится к преобразованию собираемых данных к единому формату. В ходе фильтрации отбрасываются избыточные данные. Корреляция в ходе предобработки позволяет оперативно находить в поступающем потоке событий безопасности те из них, которые являются критическими. Агрегация, или обобщение, позволяет объединять события, принадлежащие к одному и тому же виду. Классификация разделяет события на заранее выбранные классы.

Предварительно обработанные данные помещаются затем на хранение в системный репозиторий. Для реализации системного репози-

тория очень важным моментом является то, какой вид модели представления данных поддерживает лежащая в его основе СУБД.

Практически во всех известных коммерческих системах мониторинга и управления безопасностью для этих целей используются реляционные СУБД (РСУБД), такие как MS SQL, MySQL, PostgreSQL и другие. Однако, как показали исследования [14], представление хранимых данных в реляционном виде для интеллектуальной системы является недостаточным. Для нее необходимо использовать такую модель (формат) представления данных, которая позволяет реализовать логический вывод и другие интеллектуальные возможности. К таковым моделям в настоящее время относят XML–ориентированные записи данных и записи данных в формате RDF, т.е. в виде триплетов «субъект — предикат — объект» [15]. Эти форматы позволяют представлять и хранить данные в виде онтологической модели. В результате системный репозиторий становится гибридным онтологическим хранилищем. Он должен поддерживать три вида моделей данных: реляционную, XML и триплетную. Возможным инструментарием для такого решения могут служить системы, относящиеся к классу «хранилищ триплетов», например, система Virtuozo [16].

На верхнем системном уровне располагаются подсистемы, реализующие различные интеллектуальные сервисы анализа информации о безопасности. К их числу относятся:

- сервисы управления корреляцией данных о событиях безопасности;
- сервисы анализа защищенности АС ЖТ и СПД, соединяющих их между собой;
- сервисы моделирования атак на АС ЖТ и СПД;
- сервисы поддержки принятия решений;
- сервисы визуального анализа информации о безопасности.

В силу того, что интеллектуальные сервисы анализа информации для АС ЖТ еще подлежат своей реализации, подробно рассмотреть их в настоящей статье не представляется возможным. Однако, учитывая концептуальный характер настоящего материала, предложим вариант формализованных постановок задач для их разработки.

5. Формальные постановки задач. Исходными данными для всех интеллектуальных сервисов анализа информации являются данные, содержащиеся в гибридном онтологическом репозитории GOR. В общем виде всех их можно разделить на следующие классы:

Sys — данные о защищаемой инфраструктуре (ее топологии, составе элементов, пользователях, ресурсах и т.д.);

Events — данные о событиях безопасности, прошедшие предобработку и находящиеся в репозитории на хранении;

Pattr — данные о шаблонах атак, инцидентах безопасности, возможных контрмерах и прочих образцах, которые загружаются из внешних баз данных и/или формируются в ходе функционирования системы;

Pol — данные о принятых в защищаемой инфраструктуре политиках безопасности.

В результате состав исходных данных, используемых практически всеми интеллектуальными сервисами анализа, можно представить в следующем виде:

$$GOR = \langle Sys, Events, Pattr, Pol \rangle . \quad (1)$$

Рассмотрим теперь задачи, решаемые каждым из аналитических сервисов.

В сервисе управления корреляцией решается следующая задача:

$$e_{critical} = Corr(\{e_i\}), \quad (2)$$

где $e_{critical}$ — критическое событие безопасности; $e_i \subset Events$ — отдельное событие безопасности; $Corr$ — функция корреляции, позволяющая на основе анализа событий безопасности, хранящихся в репозитории, выявлять критические события. Определение функции $Corr$ является основной задачей разработки данного сервиса.

В сервисе анализа защищенности решается следующая задача:

$$Var(metr_j) = Eval(Sys, Att, Pattr, Pol), \quad (3)$$

где $Var(metr_j)$ — значение j –ой метрики (показателя) защищенности; $Att = \{e_{critical,k}\}$ — события безопасности, отражающие атаку (атаки) на защищаемую систему; $Eval$ — функция, позволяющая вычислить значение метрики защищенности на основе данных Sys, Att, $Pattr$ и Pol. Как и в предыдущем случае, определение функции $Eval$ является основной задачей разработки сервиса анализа защищенности.

В сервисе моделирования атак решается следующая задача:

$$El_{critical} = Mod(Sys, Att, Pattr, Pol, t), \quad (4)$$

где $El_{critical} \subset Sys$ — критический системный элемент, подверженный атаке к наступлению времени t; Mod — модель атаки, прогнозирующая ее поведение во времени. Определение Mod является основной задачей разработки сервиса моделирования атак.

В сервисе поддержки принятия решений решается следующая задача:

$$CntrMrsh^* = \arg\min\left|Var - Var^*\right|, \tag{5}$$

где $CntrMrsh^* \subset Pol$ — это наилучшая контрмера (мера противодействия), являющаяся элементом Pol; Var и Var^* — текущее и требуемое значения метрики защищенности, соответственно, а $\left|Var - Var^*\right|$ показывает отклонение текущего значения метрики защищенности от требуемого. Как видно из (3) и (5), формальная постановка задачи для сервиса поддержки принятия решений является задачей синтеза. Этим она принципиально отличается от всех предыдущих, которые являются задачами анализа.

Наконец, в сервисе визуального анализа решается задача выбора формы визуального представления данных $Form_{viz}^*$, которая в конечном итоге приводит к принятию меры противодействия $CntrMrsh^*$:

$$Form_{viz}^* = Viz^{-1}\left(CntrMrsh^*\right), \tag{6}$$

где под функцией визуализации понимается функция

$$CntrMrsh = Viz\left(Form_{viz}\left(Sys, Events, Pol\right)\right), \tag{7}$$

позволяющая администратору безопасности принимать контрмеру $CntrMrsh$ на основании использования формы $Form_{viz}$ визуального представления информации о системе, событиях и политиках безопасности. Как и в случае предыдущей задачи, данную задачу можно отнести к задачам синтеза.

Заключение. Автоматизированные информационные и управляющие системы ЖТ представляют собой достаточно многочисленное и разнородное множество систем, тесно взаимосвязанных друг с другом и имеющих выход в сети общего назначения. Учитывая чрезвычайно большое разнообразие видов возможных атак на АС ЖТ и критичность возможных последствий их реализация для безопасности ЖТ, необходима разработка и внедрение в АСУ ЖТ многоуровневой интеллектуальной системы обеспечения информационной безопасности.

Традиционные средства защиты в архитектуре такой системы занимают нижний уровень и отвечают, помимо реализации функций априорной защиты, за формирование и предоставление данных о со-

бытиях безопасности. На втором уровне такой системы с помощью интеллектуальных сервисов сбора и хранения осуществляется ведение гибридного онтологического репозитория данных о безопасности. На высшем уровне такой системы функционируют интеллектуальные сервисы управления корреляцией, анализа защищенности, моделирования атак, поддержки принятия решений и визуального анализа данных.

Анализ приведенных формальных постановок задач показал, что первые три аналитических сервиса можно отнести к задачам анализа, а последние два — к задачам синтеза. Разработка моделей, методов и алгоритмов, направленных на решение поставленных задач, является направлением дальнейших научных исследований.

Литература

1. Год на год не приходится // «Транспорт», № 01–02, Издательская группа «Индустрия», 2012. С 11.
2. *Санькова Г.В., Одуденко Т.А.* Информационные технологии в перевозочном процессе: учебное пособие. — Хабаровск: Изд-во ДВГУПС, 2012. 111 с.
3. *Котенко И.В., Воронцов В.В., Чечулин А.А., Уланов А.В.* Проактивные механизмы защиты от сетевых червей: подход, реализация и результаты экспериментов // Информационные технологии, № 1, 2009. С. 37–42.
4. *Котенко И.В., Саенко И.Б., Полубелова О.В., Чечулин А.А.* Технологии управления информацией и событиями безопасности для защиты компьютерных сетей // Проблемы информационной безопасности. Компьютерные системы. № 2, 2012. С. 57–68.
5. *Котенко И.В., Саенко И.Б., Полубелова О.В., Чечулин А.А.* Применение технологии управления информацией и событиями безопасности для защиты информации в критически важных инфраструктурах // Труды СПИИРАН. Вып. 1(20). СПб.: Наука, 2012. С. 27–56.
6. Информационный бюллетень «Вестник АСУ «Экспресс–3», № 1 (3), Изд. ОАО "ВНИИЖТ", 2012. С. 5.
7. *Глухов А.П.* ОАО "РЖД": о приоритетах и перспективах // Журнал Information Security / Информационная безопасность. № 2, 2007. С. 4–5.
8. *Ададуров С.* Современное состояние системы обеспечения информационной безопасности ОАО «РЖД»// Журнал «Connect! Мир Связи», № 3, 2007.
9. *Розенберг Е.Н.* Современные технологии в перевозочном процессе. Электронная презентация. НП «Гильдия экспедиторов». http://www.myshared.ru/slide/274952/#
10. *Mille D.R., Harris Sh., Harper A.A., VanDyke S., Black Ch.* Security Information and Event Management (SIEM) Implementation. — McGraw–Hill Companies, 2011. 430 p.
11. *Котенко И.В., Саенко И.Б.* Архитектура системы интеллектуальных сервисов защиты информации в критически важных инфраструктурах // Труды СПИИРАН. Вып. 1(24). 2013. С. 21–40.
12. *Котенко И.В., Саенко И.Б.* Построение системы интеллектуальных сервисов для защиты информации в условиях кибернетического противоборства // Труды СПИИРАН. Вып. 3(22). 2012. С. 84–100.
13. Magic Quadrant for Security Information and Event Management. Gartner, 2013.
14. *Котенко И.В., Полубелова О.В., Саенко И.Б., Чечулин А.А.* Применение онтологий и логического вывода для управления информацией и событиями безопасности // Системы высокой доступности. № 2, т.8, 2012. С. 100–108.

15. *Котенко И.В., Саенко И.Б., Полубелова О.В.* Перспективные системы хранения данных для мониторинга и управления безопасностью информации // Труды СПИИРАН. Вып. 2(25). 2013. С. 113–134.
16. Virtuoso Universal Server. http://virtuoso.openlinksw.com/

Котенко Игорь Витальевич — д.т.н., проф.; заведующий лабораторией проблем компьютерной безопасности СПИИРАН. Область научных интересов: безопасность компьютерных сетей, в том числе управление политиками безопасности, разграничение доступа, аутентификация, анализ защищенности, обнаружение компьютерных атак, межсетевые экраны, защита от вирусов и сетевых червей, анализ и верификация протоколов безопасности и систем защиты информации, защита программного обеспечения от взлома и управление цифровыми правами, технологии моделирования и визуализации для противодействия кибер–терроризму. Число научных публикаций — более 450. ivkote@comsec.spb.ru, www.comsec.spb.ru; СПИИРАН, 14-я линия В.О., д.39, Санкт-Петербург, 199178, РФ; р.т. +7(812)328–2642, факс +7(812)328–4450.

Kotenko Igor Vitalievich — Ph.D., Dc.Sci., Prof.; head of Laboratory of Computer Security Problems, SPIIRAS. Research interests: computer network security, including security policy management, access control, authentication, network security analysis, intrusion detection, firewalls, deception systems, malware protection, verification of security systems, digital right management, modeling, simulation and visualization technologies for counteraction to cyber terrorism; The number of publications — more 450. ivkote@comsec.spb.ru, www.comsec.spb.ru; SPIIRAS, 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone +7(812) 328–2642, fax +7(812)328–4450.

Саенко Игорь Борисович — д.т.н., проф.; ведущий научный сотрудник лаборатории проблем компьютерной безопасности СПИИРАН. Область научных интересов: автоматизированные информационные системы, информационная безопасность. Число научных публикаций — 250. ibsaen@mail.ru; СПИИРАН, 14-я линия В.О., 39, Санкт-Петербург, 199178, РФ; р.т. +7(812)328–2642, факс +7(812)328–4450.

Saenko Igor Borisovich — Ph.D., Dc.Sci., Prof.; leading research scientist, Laboratory of computer network security, SPIIRAS. Research interests: automated information systems, information security. The number of publications — 250. ibsaen@mail.ru; SPIIRAS, 14-th line, 39, St. Petersburg, 199178, Russia; office phone +7(812)328–2642, fax +7(812)328–4450.

Чернов Андрей Владимирович — д.т.н., проф.; профессор кафедры информатики Ростовского государственного университета путей сообщения (РГУПС). Область научных интересов: техническая диагностика информационных систем, дискретный анализ и синтез надежных систем. Число научных публикаций — 80. avche@yandex.ru; РГУПС, пл. Ростовского Стрелкового полка Народного Ополчения, 2, Ростов–на–Дону, 344038, РФ; р.т. +7(863)272–6543, факс +7(863)245–0613.

Chernov Andrey Vladimirovich — Ph.D., Dc.Sci., Prof.; professor, informatics department, Rostov State Transport University (RSTU). Research interests: technical diagnosis of information systems, discrete analysis and synthesis of reliable systems. The number of publications — 80. avche@yandex.ru; RSTU, sq. Rostovskogo Strelkovogo polka Narodnogo Opolchenija, 2, Rostov–on–Don, 344038, Russia; office phone +7(863)272–6543, fax +7(863)245–0613.

Бутакова Мария Александровна — д.т.н., проф.; профессор кафедры информатики Ростовского государственного университета путей сообщения (РГУПС). Область научных интересов: теория телетрафика, автоматизированные системы управления на транспорте. Число научных публикаций — 97. inf-rgups@yandex.ru; РГУПС, пл. Ростовского Стрелкового полка Народного Ополчения, 2, Ростов–на–Дону, 344038, РФ; р.т. +7(863)272–6543, факс +7(863)245–0613.

Butakova Maria Alexandrovna — Ph.D., Dc.Sci., Prof.; professor, informatics department, Rostov State Transport University (RSTU). Research interests: teletraffic theory, automated control systems for transport. The number of publications — 97. avche@yandex.ru; RSTU, sq. Rostovskogo Strelkovogo polka Narodnogo Opolchenija, 2, Rostov-on-Don, 344038, Russia; office phone +7(863)272–6543, fax +7(863)245–0613.

Поддержка исследований. В публикации представлены результаты исследований, поддержанны грантами РФФИ (проекты 13–07–13159–офи_м_РЖД, 13–01–00843–а и 11–07–00435–а) и программой фундаментальных исследований ОНИТ РАН (проект 2.2).

Рекомендовано лабораторией криптологии, заведующий лабораторией Молдовян Н.А., д.т.н., проф., заслуженный изобретатель РФ.
Статья поступила в редакцию 10.09.2013.

РЕФЕРАТ

Котенко И.В., Саенко И.Б., Чернов А.В., Бутакова М.А. **Построение многоуровневой интеллектуальной системы обеспечения информационной безопасности для автоматизированных систем железнодорожного транспорта.**

В статье на основе анализа особенностей построения и функционирования автоматизированных систем железнодорожного транспорта делается вывод о необходимости разработки и применения для защиты информации в таких системах многоуровневой интеллектуальной системы обеспечения информационной безопасности.

В качестве основных отличительных факторов построения и функционирования автоматизированных систем железнодорожного транспорта выделены достаточно большое многообразие и разнородность таких систем, их взаимная связность и связность с сетями общего пользования и сильная разнородность внутренних пользователей.

Представлена и рассмотрена архитектура многоуровневой системы обеспечения информационной безопасности, которая включает три уровня. На нижнем уровне находятся традиционные средства защиты информации. Помимо функций априорной защиты информации эти средства обеспечивают формирование и предоставление информации о событиях безопасности.

Для хранения данных о безопасности в многоуровневой интеллектуальной системе защиты предложено использование гибридного онтологического репозитория, который является основным элементом среднего уровня рассматриваемой системы защиты. В онтологическом репозитории предлагается совместно использовать реляционное моделирование данных, XML–ориентированное моделирование и моделирование данных в виде триплетов «субъект — предикат — объект».

Для интеллектуальных сервисов анализа данных, находящихся на верхнем уровне рассматриваемой системы защиты, предложены формальные постановки задачи. Все интеллектуальные сервисы анализа данных используют в качестве своих исходных данных информацию о системе, о событиях безопасности, о шаблонах и инцидентах безопасности и о политиках безопасности. Задача сервиса управления корреляции сводится к нахождению функции корреляции, позволяющей находить среди множества событий безопасности критические события. Сервис анализа защищенности предназначен для расчета значений различных метрик защищенности. Сервис моделирования атак призван находить элементы системы, на которые во времени распространяются атаки. Сервис поддержки принятия решений находит наилучшие контрмеры. Сервис визуального анализа определяет наилучшие формы визуального представления данных. Первые три аналитических сервиса решают задачи анализа. В последних двух сервисах решаются задачи синтеза. Методология решения данных задач рассматривается как направление дальнейших исследований.

SUMMARY

Kotenko I.V., Saenko I.B., Chernov A.V. **The construction of a multi-level intelligent information security system for automated systems of railway transport.**

The article, based on an analysis of the characteristics of construction and functioning of automated systems of railway transport, concludes the need for development and application of the multilevel intelligent information security system.

As main distinguishing factors, the great variety and diversity of construction and functioning of the automated systems of railway transport, their mutual corelationships, links with public networks, and strong heterogeneity of internal user are highlighted.

The architecture of a multi-level intelligent information security system is presented and discussed. It includes three levels. At the lowest level the traditional means of information protection are presented. In addition to the functions of a priori information protection these means provide formation and provision of security event information.

To store data about security a multilevel intelligent system of protection uses a hybrid ontology repository, which is a key element of the middle level of the protection system discussed. An ontological repository jointly uses relational data modeling, XML–oriented modeling and simulation data in the form of "subject — predicate — object" triplets.

Formal task statements for intelligent services of data analysis at the top level of the reviewed protection systems are offered. All the intelligent data analysis services use as its source data the system information about security events, templates and security incidents and security policies. The task of service management correlation consists in finding the correlation function to find critical events among the set of security events. Security analysis service is for calculation the values of various metrics. Modeling service should be designed to find elements of the system, which are responsible for attacks in time. Decision support service finds the best countermeasures. Visual analysis service determines the best visual representation of data. The first three analytical services solve the analysis problem. In the last two services the synthesis tasks are fulfilled. The methodology to solve these tasks is considered as the direction of future research.