© Akhmetov B. Status, perspectives and main directions of the development of cybersecurity of information and communication transport systems of Kazakhstan // Ukrainian Scientific Journal of Information Security, 2018, vol. 24, issue 2, p.91-98.

DOI: 10.18372/2225-5036.24.13048

СОСТОЯНИЕ, ПЕРСПЕКТИВЫ И ОСНОВНЫЕ НАПРАВЛЕНИЯ РАЗВИТИЯ КИБЕРБЕЗОПАСНОСТИ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ СИСТЕМ ТРАНСПОРТА КАЗАХСТАНА

Берик Ахметов

Каспийский государственный университет технологий и инжиниринга имени Ш. Есенова, Республика Казахстан

АХМЕТОВ Берик Бахытжанович, к.т.н.

Год и место рождения: 1985 год, г. Нукус, Узбекистан.
Образование: Казахский национальный университет имени аль-Фараби, 2006 год.
Должность: ректор Каспийского государственного университета технологий и инжиниринга имени Ш. Есенова.
Научные интересы: информационная безопасность, кибербезопасность, нечеткая логика, нейросетевые технологии.
Публикации: более 30 научных и учебно-методических трудов, в том числе монографии, учебники и учебные пособия.
E-mail: 007berik@mail.ru

Аннотация. *Статья содержит результаты сравнительного анализа предшествующих исследований в области кибербезопасности информационно-коммуникационных систем транспорта (ИКСТ). Недостаточное внимание к проблематике кибербезопасности ИКСТ может привести к перехвату управлением и сбоям в системах диспетчерского управления транспорта. Как худший вариант можно допустить последствия с человеческими жертвами. Как дополнительный риск можно рассматривать отсутствие стандартизации информационно-коммуникационных систем транспорта и их компонент, отвечающих за кибербезопасность. Анализ выполнен в контексте решаемой проблемы дальнейшего развития методов и моделей распознавания киберугроз, аномалий и атак, направленных против информационно-коммуникационных систем транспорта, а также оценивания рисков для информационной безопасности транспортной отрасли как одной из составляющих критически важной инфраструктуры Республики Казахстан. Актуальность задачи также вызвана формированием единой информационно-коммуникационной среды транспортной отрасли Казахстана, внедрение новых и модернизацией существующих информационных систем на транспорте в условиях увеличения количества дестабилизирующих воздействий на доступность, конфиденциальность и целостность информации. Проведенные исследования способствуют провозглашенной в Республике Казахстан стратегии цифровизации производственных процессов, развитию транспортной и логистической инфраструктуры, внедрению цифровых технологий на транспорте и созданию интеллектуальной транспортной системы.*

Ключевые слова: *информационно-коммуникационные системы, информационная безопасность, критически важные компьютерные системы, система защиты информации, системы обнаружения кибератак.*

Введение

В условиях глобализации значительно возрастает роль транспортной инфраструктуры в обеспечении развития торгово-экономических отношений между странами, их культурных, туристических и спортивных связей, а также международных транзитных перевозок. Участие Республики Казахстан (РК) в международных интеграционных процессах в сфере транспортных перевозок – безальтернативная тенденция, но она должна сопровождаться созданием современной инфраструктуры, совместимой с инфраструктурой стран, с которыми РК взаимодействует с одновременным обеспечением защиты национальных интересов.

Решение этих задач невозможно без эффективных систем информационного обеспечения, которые интегрируют процессы управления, обработки данных, наблюдения, связи и др. Современные информационные технологии (ИТ) на транспорте в совокупности с системами навигации и наблюдения дают возможность отслеживать и анализировать транспортные потоки на железных дорогах, автодорогах, нефти и газопроводах, воздушных и водных путях и др. Также возможно, проводить накопление и анализ полученной информации в интеллектуальных транспортных сетях, использовать данные для принятия управленческих решений и функционирования транспортно-логистических центров.

Цель работы: сравнительный анализ предшествующих исследований в области кибербезопасности информационно-коммуникационных систем транспорта, в контексте решаемой проблемы дальнейшего развития методов и моделей распознавания киберугроз, аномалий и атак, направленных против информационно-коммуникационных систем транспорта, а также оценивания рисков для информационной безопасности отрасли как одной из составляющих критически важной инфраструктуры РК.

Обзор предшествующих исследований

Для Казахстана вопрос защиты информации и обеспечения информационной и кибербезопасности (ИБ и КрБ) транспортной отрасли имеют особое значение. Это связано, прежде всего, с размерами территории и геополитическим расположением Казахстана, с политическим и социально-экономическим курсами, направленными на дальнейшее укрепление суверенитета.

Вмешательство в национальные, региональные и муниципальные автоматизированные информационные и информационно-управляющие системы на транспорте часто упоминаемая угроза от кибератак злоумышленников [1–4]. Высокая степень привлечения человека к транспортной логистике и управлению процессами транспортировки не уменьшают риски, связанные с кибератаками и несанкционированным вмешательством в работу ИКСТ [4-8]. При этом статистика инцидентов по ИБ и КрБ в мировых ИКСТ пополняется каждый год, табл. 1 (данные приведены по результатам анализа [9-17]).

Факты вмешательства в работу ИКСТ Таблица 1

№	Год	Государство	Событие	Описанные последствия
1.	2002	Великобритания (ВБ)	НСД к служебной телефонной связи железной дороги и системы управления семафором.	Отключен от связи диспетчерский пункт ж.д., сбой в систме включения семафоров [11].
2.	2003	Швеция, Гетеборг	Взлом АСУ движением городских автобусов и такси.	Потеря котроля над графиком движения на несколько часов [4, 13].
3.	2014	РФ	Вирус отключил видеокамеры фиксации скоростного режима «Стрелка-СТ» в Москве и области.	Камеры выведены из строя на несколько дней [11].
4.	2003	США	Вирус SQL Slammer нарушает работу АСК авиакомпании «Continental Airlines».	Отмена рейсов [2].
5.	2008	КНР	В китайском городе Вэйфан задержан человека, совершивший крупнейшую в истории КНР атаку на китайские транспортные компании.	Простои транспортных компаний в г. Вэйфан.
6.	2008	Пакистан, Индия	Хакеры из Пакистана взломали доступ к сайту Индийской ж/д компании.	Сайт не работал более 12 часов.
7.	2012	РФ, Нидерланды, ВБ, США	Хакерская группа Anonymous совершила кибератаки на серверы «Газпром», «Роснефть», Shell, BP Global и ExxonMobil.	В свободном доступе оказались тысячи почтовых аккаунтов сотрудников и данные компаний [13, 18].
8.	2013 - 2014	Сомали, США, ВБ, Норвегия и др.	Обнародован отчет компании Ra-pid7 о фактах вмешательства в работу GPS систем нефтедобывающих платформ, танкеров и контейнервозов в персидском заливе и Аденском проливе.	Зафиксированы факты выхода из строя ПО на буровых платформах на 19 суток [11, 18].
9.	2016	Украина	Взлом системы видеотрансляции в метро г. Киев	Замена видео контента.

Увеличение количества кибератак на ИКСТ в последние годы вызвал интерес к разработке эффективных СЗИ, ориентированных на специфику транспорта [1, 3, 6, 8, 11, 14].

В основном авторы сосредотачивали внимание на проблематике ИБ и КрБ отдельных видов транспорта: авиационного [1, 2]; трубопроводного, как элемента критической инфраструктуры [3–5]; автомобильного [6]; морского и речного [7, 8]; железнодорожного [9–12]. В работах [13–17] изложены результаты комплексной оценки роли информационной и кибербезопасности транспорта как составляющей национальной безопасности государства и ее критически важных инфраструктур. Однако заметим, что рассмотренные работы не содержат описательные модели, позволяющие выявлять законо-

мерности эволюции ситуации, связанной с ИБ и КрБ на транспорте. Большинство рассмотренных исследований не имели практической реализации, в виде прикладного ПО, которое позволило бы, в частности, разработать конкретную методологическую базу организации системы защиты ИКСТ, с учетом их специфики.

Недостаточное внимание к проблематике кибербезопасности ИКСТ может привести к перехвату управлением и сбоям в системах диспетчерского управления транспорта. Как худший вариант можно допустить последствия с человеческими жертвами. Как дополнительный риск можно рассматривать отсутствие стандартизации ИКСТ и их компонент отвечающих за ИБ и КрБ [2, 6, 11, 13, 18].

В работах [14, 16] проанализирована методология интеллектуального моделирования, предназначенная для анализа и принятия решений в недостаточно структурированных ситуациях ИБ и КрБ ИКСТ. На нынешнем этапе исследования [13] не доведены до аппаратной или программной реализации. Сложными для анализа и поддержки принятия решений, касающихся обеспечения защиты ИКСТ, являются слабо поддающиеся формализации и структуризации задачи обеспечения ИБ и КрБ при появлении новых классов атак [2, 4, 5, 13, 16]. В этом случае параметры состояния ИКСТ, могут быть представлены качественными показателями, что не всегда целесообразно.

Таким образом, учитывая полемику в рассмотренных работах, представляется актуальной задача проведения новых исследований, направленных на развитие методов и моделей управления ИБ и КрБ ИКСТ с учетом особенностей их инфраструктуры, а также динамически изменяющихся требований по управлению кибербезопасностью на транспорте.

Информационно-коммуникационные системы транспорта (ИКСТ) как объект кибератаки

Активное расширение сферы применения ИТ и критически важных информационных систем транспорта (КВИСТ) в РК, особенно в сегменте мобильных, распределенных и беспроводных технологий, сопровождается возникновением новых киберугроз. Это подтверждается и ростом количества инцидентов, связанных с кибербезопасностью (КрБ) и защитой информации в КВИСТ [18, 19]. Угрозы вполне реальны, поскольку злоумышленники могут получить возможность перехватывать пароли, отдельные файлы, геолокационную информацию, транслировать аудио- и видеоданные, контролировать Wi-Fi-сети, веб-камеры, информационные табло на автомобильных и железных дорогах, вокзалах, аэропортах и др.

Сегодня многие проекты в сфере управления на транспорте развиваются в направлении создания крупных ситуационных центов (СЦ), обеспечивающих решение специфических задач, в частности, защиты КВИСТ. Инвестирование в инновационные проекты, например, в сфере КрБ и защиты информации, характеризуются высокой степенью неопределенности и рискованностью. Многие предприятия и компании, занимающиеся обслуживанием КВИСТ, расходуя большое количество средств на системы защиты информации (СЗИ) и КрБ, не испытывают уверенности, что выбранная стратегия инвестирования делает инфраструктуру ИКСТ реально безопасной.

Серьезной проблемой в области КрБ КВИСТ остается обеспечение защиты от несанкционированного доступа (НСД). О серьезности проблемы свидетельствует хотя бы тот факт, что даже один человек, который имеет доступ к КВИСТ, за непродолжительное время может полностью парализовать работу любого стратегического железнодорожного узла, морского порта, газо или нефти транспортного предприятия и др.

Практически любая ИКСТ может выступать в качестве объекта атаки. Для ее реализации злоумышленнику (злоумышленникам) необходимо активизировать уязвимости ИКСТ. Как показывает статистика [11, 13, 18] таких уязвимостей не становиться меньше.

В настоящее время транспортная отрасль во всем мире и в РК, в частности, проходит этап трансформации и адаптации к новым цифровым технологиям. Нынешнее состояние многих средств информатизации и автоматизации транспортных систем пока базируется на традиционных SCADA. Однако уже происходит активное подключение кинтернет как непосредственно транспортных средств, так и компонентов дорожной инфраструктуры: камер видеонаблюдения, информационных табло, «умных остановок», облачной инфраструктуры и др. Все эти элементы уязвимы для кибератак. По данным [18] только в период с марта 2015 г. по май 2016 г. ИКСТ более 44 раз подверглись DoS атакам и другим деструктивным воздействием со стороны компьютерных злоумышленников.

Всеобъемлющий характер задач формирования ИКСТ РК требует их систематизации и выбора приоритетов [19]. Сегодня в транспортной отрасли РК развивается ряд отраслевых информационных систем и сетей связи, работающих автономно и не взаимосвязанных друг с другом, см. табл. 2.

Автоматизированные информационные и информационно-управляющие системы транспорта (Республика Казахстан) Таблица 2

Вид транспорта	Название	Типовые решаемые задачи	Особенности
1	2	3	4
Железнодорожный транспорт	АСУ на ПС	Автоматизированные системы управления на подвижном составе.	Система работает на серверном комплексе IBM Z9. Используются PLC Siemens, ABB, GE, Schneider Electric, Emerson и др.

Продолжения Таблицы 2

1	2	3	4
	АСУ Клиент	учет грузов, оформление накладных и др.	АСУ базируется на программно-аппаратном комплексе P780 IBM, СУБД Oracle.
	АСУ «Экспресс-3»	В режиме on-line: запросы на предоставление справочной информации; покупка электронных билетов на поезда международного и республиканского сообщений; и др.	Система базируется на программно-аппаратном комплексе P780 IBM, СУБД Oracle.
	АСУ ЦГВ	Автоматизированная система контроля грузов и целостности железнодорожных вагонов в движении обеспечивает: видеонаблюдение в реальном режиме времени с прохождением поезда, состоянием вагонов, наличие запорно-пломбировочных устройств на запорных механизмах дверей и люков и прочее.	ПО TNS-INTEC (РК)
	Др.		
Автомобильный и системы контроля движения на автодорогах	АСУ Логистика, ПО «АвтоГраф»; ПО Wialon Hosting и др.	Интеграция с бизнес-информационными системами грузоперевозчиков; Определение возможностей грузоперевозчиков; Доступ к пулу заказов, соответствующих параметрам конкретного перевозчика; Формирование перевозочных документов; Оплата за оказанные услуги; Контроль прохождения грузов.	Работают на платформах Windows, Android. используются PLC GE, Schneider Electric, Emerson и др.
Морской	Navi-Harbour 1000	Единая информационная система портового сообщества (ИСПС) обеспечивает: учет работы порта (учет железнодорожных вагонов, грузовых автомобилей и др. подвижного состава, находящихся в порту) подготовку электронных и перевозочных документов; подготовку бумажных перевозочных документов; взаимодействие АИС предприятий с ИСПС; взаимодействие ИСПС с АИС таможни в части передачи электронных данных на грузы; формирование статистики, отчетности и накопления архива; др.	Система базируется на программно-аппаратном комплексе P780 IBM, СУБД Oracle, MySQL Работают на платформах Windows. используются PLC Siemens, ABB, GE, Schneider Electric, Emerson и др.
Авиационный	АСУ SAP ERP, B2B сервисы, E-ticket, (на примере Air Astana и др.)	Корпоративная система управления на базе SAP ERP Республиканского государственного предприятия на праве хозяйственного ведения «Казаэронавигация» обеспечивает: комплексную автоматизацию бизнес-процессов управления финансово-хозяйственной деятельностью предприятий; оптимизирует и унифицирует процессы обмена информацией. B2B сервисы обеспечивают: бронирование пассажирских и грузовых перевозок; просмотр расписания рейсов, свободных пассажирских и грузовых мест; оформление накладных; др.	Программное обеспечение SAP AG (Германия)
Трубопроводный	АСУ ТПТ	АСУ ТПТ и АСУ ERP обеспечивают ключевые процессы транспортировки газа и нефти на территории РК. Ключевые функции: финансовый и налоговый учет; учет оборотных и необоротных активов; учет материальных потоков и электронные торги; оперативное управление технологическим процессом; управление качеством; планирование и управление; управление бюджетами; управление затратами, доходами и анализ прибыльности; управление проектами и капитальными инвестициями; управление сбытом; администрирование персонала и организационный менеджмент построение аналитической отчетности; др.	АСУ базируется на программно-аппаратном комплексе P780 IBM, СУБД Oracle и прикладном ПО разработки «Серк Контролз» (Великобритания) и SAP AG (Германия). Используются PLC Siemens, Schneider Electric, Emerson и др. ПО TNS-INTEC (РК) и др.

Продолжения Таблицы 2

1	2	3	4
Интермодальные (мультимодальные) центры логистики, наблюдения, навигации средствами GPS, ГЛОГАСС	«Teltonika» и др. программный комплекс объединяет в себе - СУБД, ПО для сервисов, картографическое ПО и др.	«Teltonika» и др. аналогичные системы. Ключевые функции: определение координат и параметров движения; хранения данных в энергонезависимой памяти; передача данных по запросу с диспетчерского центра; передача данных и / или запись в память данных GPS; шифрование данных; оповещение о входящих / исходящих сообщениях и др.	Криптографическая защита данных.

Объектами кибератак могут стать практически все элементы ИКСТ. Как показал анализ реальных атак, наиболее уязвимыми являются следующие категории объектов в инфраструктурных решениях информационно–коммуникационных систем транспортной отрасли [1, 4, 6, 7, 11, 14, 18]: центры обработки данных, автоматизированные системы управления по различным видам транспорта (SCADA и др.); 2) компоненты периферийного оборудования (например, информационные табло); 3) устройства на программируемых логических контроллерах (PLC); 4) системы и каналы связи для обмена данными между диспетчерами и транспортными средствами; 5) системы навигации с использованием GPS и ГЛОНАСС.

При формировании политики ИБ и системы управления ИБ для перечисленных в таблице 2 ИКСТ (АСУ и АИС), делается допущение, что трактовка терминов «информационная безопасность» и «кибернетическая безопасность» шире, чем термин «безопасность информационных технологий транспорта». Таким образом, можем записать:

$$FCS = \left\{ FCS_{ij} : i = 1,2,...,m : j = 1,2,...,n \right\} \cup \cup \left\{ FCS_{q+v} : q = \sum_{i=1}^{n} n_i, v = 1,2,...,h \right\}, \quad (1)$$

где FCS – функция ИБ или КрБ ИКСТ; O_i – объекты оценки ИБ или КрБ; $i = 1,2,...,m$, $j = 1,2,...,n$, n – количество FIS для элементов систем защиты ИБ и КрБ ИКСТ; $q = \sum_{i=1}^{n} n_i$ – совокупность FCS для всех объектов оценки O_i.

Полагаем, что элементы множества FCS_{ij} могут не полностью обеспечивать выполнение требований ИБ и КрБ ИКСТ. Например, подобная ситуация возможна при появлении новых видов или классов киберугроз и уязвимостей в ИКСТ [1, 3, 5, 6, 10, 11, 13, 18]. Это, в свою очередь, приводит к возрастанию информационных рисков [2], связанных с эксплуатацией ИКСТ.

Сейчас, как правило [1, 2, 6, 11], задается уровень риска, который считается приемлемым и не требует принятия мер противодействия попыткам НСД к ИКСТ.

В дальнейшем, руководствуясь глобальной задачей исследований, принимаются следующие допущения при разработке методов, моделей и алгоритмов для системы управления ИБ и КрБ ИКСТ:

1) на ИКСТ влияют действия атакующей стороны (внешней или внутренне). Действия атакующей стороны способны привести к частичной утрате или невыполнению функций ИБ и КрБ;

2) воздействие атакующей стороны на ИКСТ не всегда носит вероятностный характер. Следовательно, традиционные модели для расчета вероятности преодоления атакующими контуров ИБ должны учитывать целенаправленность подобных атак (таргетированные атаки);

3) вектор атаки может исходить как изнутри транспортной компании так извне. Не все действия атакующей стороны (угрозы, аномалии и непосредственно кибератаки) могут быть эффективно распознаны и обнаружены;

4) оценка последствий воздействия атакующей стороны на основе методов статистического анализа не всегда корректна, если это таргетированная атака.

Ранее рядом авторов [1, 11, 6] предлагалось использовать специальный показатель для количественной характеристика степени текущей опасности кибератаки на информационные системы, в частности ИКСТ, который может быть рассчитан (измерен) в любой момент времени – показатель текущих рисков (ПТР):

$$C_{ICR} = C_{ICR}(\bar{X}), \quad (2)$$

где $\bar{X}_{ICR} = (x_{ICR_1},...,x_{ICR_i},...,x_{ICR_{MI}})$ – вектор значений ПТР (ICR), MI – число угроз для ИКСТ. Принято, что $C_{ICR} = (0 \div 1)$.

Неопределенность методов вычисления вероятностей угроз для ИКСТ, в частности для интегрирующих деятельность автономных ИС и АСУ по отдельным видам транспорта, а также потенциальных уязвимостей, является основной проблемой в процессе получения количественных оценок рисков нарушения ИБ и КрБ ИКСТ. Для сложных открытых систем, к которым можно отнести и ИКСТ, более целесообразно выполнить оценку наихудших сценариев ситуаций. В частности, можно применить метод гарантированного результата для оценки вероятностей реализации киберугроз для ИКСТ.

Можно воспользоваться параметром защищенность информации [6, 11, 13] – SE. Будем полагать, что для средства защиты информации (СРЗИ – DP_m), где m – номер СРЗИ, существует вероятность обнаружения и последующего блокирования угрозы в границах периметра – P_{PE_m}. Величину P_{PE_m} можно считать ожидаемой теоретической эффективностью периметра ИБ.

Уровень защищенности *i*-го узла периметра ИКСТ (например, SCADA, B2B, системы спутниковой навигации, информационного сервиса и др.), с учетом [1, 4, 6, 11, 13, 14] определим так:

$$SE_i = 1 - V_{cis_i}, \quad (3)$$

где V_{cis_i} – важность (значимость) инцидента ИБ на *i*-м узле ИКСТ. Тогда, для каждого узла ИКСТ значимость инцидента ИБ определим так:

$$V_{cis_i} = L_i \cdot KR_i \cdot CO_i \cdot DP_i \cdot C_{ICR}, \quad (4)$$

где V_{cis_i} – значимость инцидента ИБ и КрБ; L_i – уровень нарушения ИБ и КрБ; KR_i – критичность информационных активов (ИА); CO_i – уровень доверия к метрикам ИБ и КрБ; DP_i – уровень ЗИ; $C_{ICR} = 0-1$ – коэффициент, *i* – номер узла ИКСТ (например, сегмента сети).

Степень защищенности ИКСТ определим так:

$$SE_{CIS} = \prod_{i=1}^{n} (1 - L_i \cdot KR_i \cdot CO_i \cdot DP_i \cdot C_{ICR}), \quad (5)$$

где *n* – количество узлов (например, модулей) в составе ИКСТ.

Таким образом, в рамках исследований, необходимо продолжить работу по дальнейшему развитию методов и моделей системы управления ИБ и КрБ ИКСТ, с учетом фактора критичности данных инфраструктур, см. рис. 1.

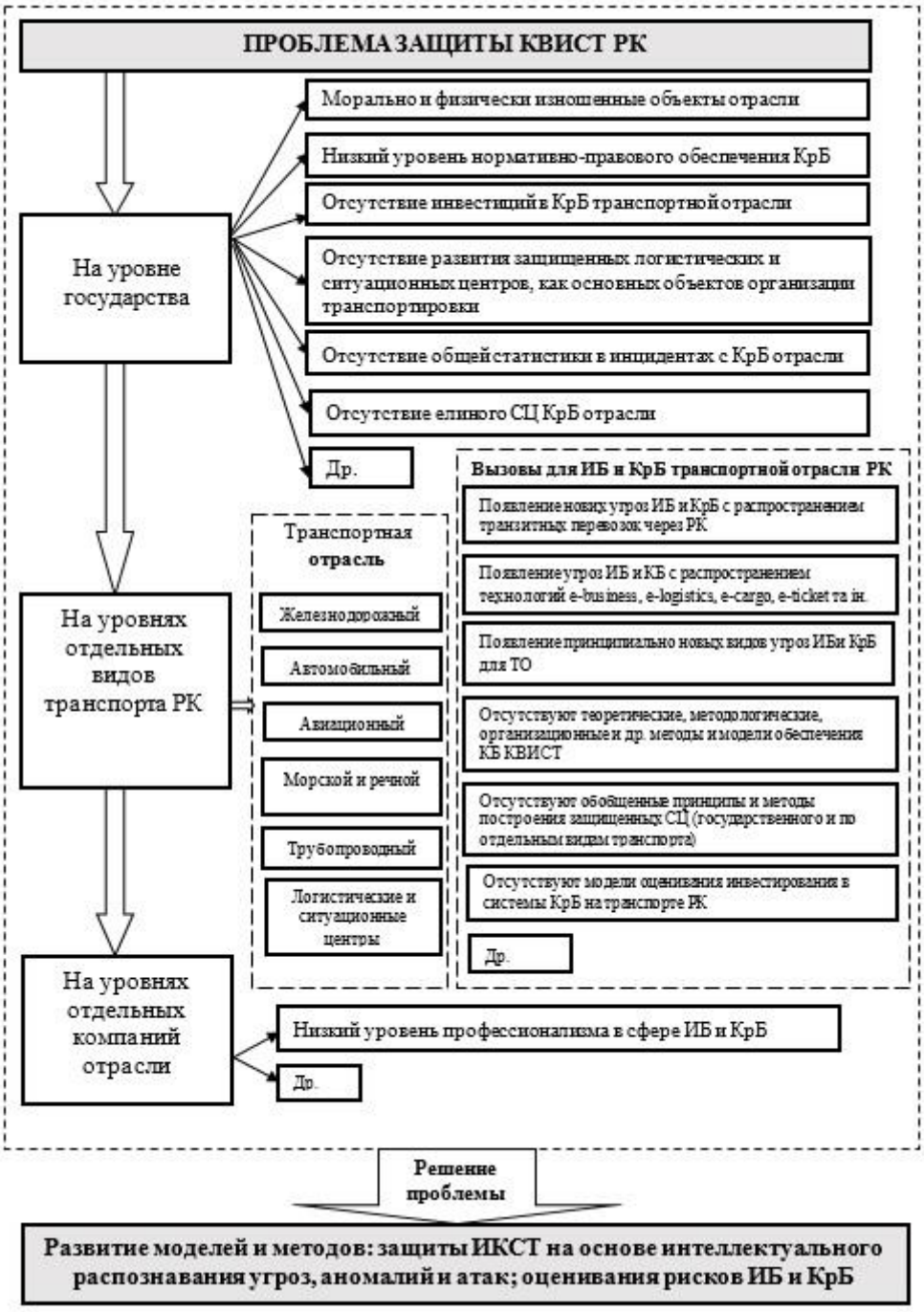

Рис. 1. Проблема обеспечения информационной безопасности транспортной отрасли РК в условиях формирования единого защищённого ситуационного центра

Это в свою очередь, позволит более эффективно выполнять оценку уровней и рисков нарушения ИБ и КрБ ИКСТ. Кроме того, ставится задача разработки интеллектуализированных систем защиты с включением в контуры ИБ подсистем поддержки принятия решения по противодействию несанкционированному доступу и кибератакам в ИКСТ. Реализация данных мероприятий позволит в ближайшей перспективе разработать эффективную методологию оперативного реагирования и принятия решений при возникновении угроз ИБ и КрБ в ИКСТ Республики Казахстан [19, 20].

Проводимые исследования способствуют провозглашенной в РК стратегии цифровизации производственных процессов, развитию транспортной и логистической инфраструктуры, внедрению цифровых технологий на транспорте и созданию интеллектуальной транспортной системы.

Выводы

В результате проведенных исследований, сделаны следующие выводы.

1. Показано, что для проведения эффективной политики ИБ и КрБ для ИКСТ, выбору и внедрению СЗИ, необходимо провести анализ киберугроз и уязвимостей для подобных систем с учетом специфики каждого вида транспорта.

2. Необходимо разработать единую методологию создания защищенных СЦ транспорта, адаптированных к условиям потенциальных целевых кибератак.

3. Необходимо продолжить комплексные исследования по моделированию стратегий потенциального нарушителя при реализации сложных таргетированных кибератак, направленных против ИКСТ. Это позволит выполнять более эффективную оценку надежности функционирования систем защиты информации для ИКСТ.

4. Следует более детально формализовать задачи и методы определения состава комплексов систем КрБ для ИКСТ с учетом потенциала инвестирования в защищенные СЦ транспортной отрасли РК.

5. Показана актуальность решаемой проблемы дальнейшего развития методов и моделей распознавания киберугроз, аномалий и атак, направленных против ИКСТ, а также оценивания рисков для информационной безопасности транспортной отрасли как одной из составляющих критически важной инфраструктуры Республики Казахстан.

Литература

[1] В.П. Бабак, В.П. Харченко, В.О. Максимов. «Безпека авіації». К.: Техніка, 2004. 584 с.

[2] О.Г. Корченко, С.О. Гнатюк, Б.Б. Ахметов. «Метод оцінювання повноти виконання вимог щодо забезпечення кібербезпеки цивільної авіації». *Безпека інформації*. 2017. Т. 23. №. 2. С. 92-99.

[3] S.M. Rinaldi, J.P. Peerenboom, T.K. Kelly. «Identifying, understanding, and analyzing critical infrastructure interdependencies». *IEEE Control Systems*. 2001. Т. 21. №. 6. С. 11-25.

[4] A. Nicholson. «SCADA security in the light of Cyber-Warfare». *Computers & Security*. 2012. Т. 31. №. 4. С. 418-436.

[5] Д. С. Бірюков, С. І. Кондратов. «Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні». К.: НІСД, 2012. 96 с.

[6] Y. A. Ivanova. «Modeling the impact of cyber threats on a traffic control centre of urban auto transport systems». *International Journal on Information Technologies & Security*. 2017. Т. 9. №. 2. С. 83-95.

[7] Г.Б. Вильский. «Исследование информационной безопасности водных путей». Судовождение: Сб. научн. трудов/ОНМА. 2010. №. 18. С. 38-47.

[8] Г.Б. Вильский. «Информационные риски судовождения». *Наук. Вістник ХДМА* № 1(4). Херсон: ХДМІ, 2012. С.17–26.

[9] Грузоперевозки – GPS мониторинг транспортных парков. URL: http://www.voyajer.ru/topovoe_work_01.html.

[10] А.А. Корниенко, М.А. Еремеев, С.Е. Ададуров. «Средства защиты информации на железнодорожном транспорте (криптографические методы и средства)». Учеб. пособие. М.: Маршрут, 2006. 256 с.

[11] С.Л. Кришталь. «Информационное обеспечение центров управления перевозками в системе МПС России»: дисс. докт. техн. наук. 05.22.08/ Кришталь Сергей Львович. М., 2002. 207 с.

[12] В.А. Лахно. «Обеспечение информационной безопасности корпоративных систем на железнодорожном транспорте». *Известия Волгоградского государственного технического университета. Серия - Актуальные проблемы управления, вычислительной техники и информатики в технических системах*. Волгоград. 2014. Вып.20. № 6 (133). С. 131–136.

[13] В.А. Лахно. «Выбор стратегии развития системы информационной безопасности на транспорте». *Поиск. Серия естественных и технических наук. Научный журнал- приложение международного журнала «Высшая школа Казахстана»*. Алма-Ата. 2013. № 4. С. 228–235.

[14] О.В. Есиков, Р.Н. Акиншин, А.С. Кислицын. «Особенности защиты информации в распределенных системах телекоммуникаций и корпоративных системах связи. В 3-х томах». Обеспечение информационной безопасности в экономической и телекоммуникационной сферах: Коллективная монография. М.:Радиотехника, 2003.

[15] V. Lahno. «Protection of information in critical application data processing systems». *MEST Journal*. Belgrade. 2014. Vol. 2, No 2. PP. 102–112.

[16] M. M. Al Hadidi. «Intelligent Systems for Monitoring and Recognition of Cyber Attacks on Information and Communication Systems of Transport». *International Review on Computers and Software (IRECOS)*. 2016. Т. 11. №. 12. С.1167-1177.

[17] V. Lahno. «Ensuring of information processes' reliability and security in critical application data processing systems». *MEST Journal*. Belgrade. 2014. Vol. 2, No 1. PP. 71–79.

[18] Featured research. URL.:https://www.ibm.com/security/resources/xforce/research.html.

[19] Государственная программа «Цифровой Казахстан» на 2017-2020 г.. URL: https://zerde.gov.kz/.

[20] Государственная программа развития и интеграции инфраструктуры транспортной системы. Республики Казахстан до 2020 года. URL: www.mid.gov.kz/images/stories/contents/gp_150520141656.pdf.

УДК 004.056 (045)

Ахметов Б.Б. Стан, перспективи та основні напрямки розвитку кібербезпеки інформаційно-комунікаційних систем транспорту Казахстану

Анотація. *Глобальний розвиток критично важливих комп'ютерних систем (КВКЗ) в енергетиці, промисловості, зв'язку та на транспорті, об'єктах інфраструктури великих мегаполісів, і т.п. Вимагає постійного відстеження кіберзагроз, а також уразливостей технічних компонентів й програмного забезпечення. Недостатня увага до проблематики кібербезпеки інформаційно-комунікаційних систем транспорті може призвести до перехоплення керування та збоїв систем диспетчерського управління транспорту. Як найгірший варіант можна допустити наслідки з людськими жертвами. Як додатковий ризик можна розглянути відсутність стандартизації інформаційно-коммунікаційних систем транспорту та їх компонент, відповідальних за кібербезпеку. Недосконаліть чинних методів кіберзахисту, а також змінний характер дій кіберна-падників, диктує необхідність продовжувати дослідження в галузі математичного та алгоритмічного розвитку систем захисту інформації, здатних своєчасно виявляти кібератаки, аномалії та загрози. Таким чином, актуальність досліджень, спрямованих на подальший розвиток моделей і методів захисту на основі інтелектуального розпізнавання загроз КВКС і забезпечення їх інформаційної безпеки, є однією з ключових проблем кіберзахисту критичної інфраструктури держави. У статті запропонована схема адаптивної системи захисту інформації КВКС і описана модель побудови системи кіберзахисту на основі логічних процедур і матриць ознак кібератак, аномалій і загроз. Проведені дослідження сприяють стратегії цифровізації виробничих процесів яка проголошена у Республіці Казахстан, а також розвитку транспортної та логістичної інфраструктури, впровадженню цифрових технологій на транспорті та створенні інтелектуальної транспортної системи країни.*

Ключові слова: *інформаційно-комунікаційні системи, інформаційна безпека, критично важливі комп'ютерні системи, система захисту інформації, системи виявлення кібератак.*

Akhmetov B. Status, perspectives and main directions of the development of cybersecurity of information and communication transport systems of Kazakhstan

Abstract*. The article contains the results of a comparative analysis of previous studies in the field of cybersecurity of information and communication transport systems. The analysis was carried out in the context of the solved problem of the further development of methods and models for the recognition of cyber threats, anomalies and attacks directed against information and communication transport systems, as well as assessing the risks of information security of the transport industry as one of the components of the critical infrastructure of the Republic of Kazakhstan. The urgency of the task is also caused by the formation of a unified information and communication environment of the transport industry in Kazakhstan, the introduction of new and modernization of existing information systems in transport in the conditions of increasing the number of destabilizing effects on the availability, confidentiality and integrity of information. The conducted researches contribute to the strategy of digitalization in Kazakhstan. This strategy is aimed at the modernization of production processes, the development of transport and logistics infrastructure. Also, new digital technologies will be developed in transport and new intelligent transport systems will be created.*

Key words*: information and communication systems, information security, critical computer systems, information security system, cyberattack detection systems.*

Отримано 30 *червня 2018 року*, затверджено редколегією 1 *серпня 2018 року*