3. *Иконников С.Е.* Комплексная система защиты на объектах критической информационной инфраструктуры / Материалы II Международной научно-практической конференции «Интеллектуальные транспортные системы». Москва, 25 мая 2023 года. – М.: Российский университет транспорта, 2023. – С. 475-477.

4. *Ермакова А.Е., Иконников С.Е.* Требования по информационной безопасности для автоматизированных систем диспетчерского управления на транспорте / Proceedings XV međunarodni naučno-stručni skup Informacione Tehnologije za e-Obrazovanje ITeO. 29-30.9.2023, Banja Luka. – Banja Luka: Panevropski univerzitet Apeiron, 2023. – P. 162-166.

DOI: 10.25728/iccss.2023.53.91.033

Баранов Л.А., Михалевич И.Ф., Иванова Н.Д., Соколов С.С.

Информационная безопасность системы автономного судовождения в контексте специфических для интеллектуальных транспортных систем угроз

Аннотация: В работе рассмотрена проблема обеспечения информационной безопасности как интегрированной автоматизированной системы корпоративного и технологического управления. Рассмотрен вариант управления рисками информационной безопасности системы автономного судовождения с использованием технологий дополненного интеллекта и модели системы мониторинга сложных процессов.

Ключевые слова: безопасность транспорта, свойство подлинности информации, промышленная криптография, экспертная оценка, теория нечетких множеств

Введение

С развитием технологий транспортные средства перестали являться самостоятельными объектами, и в соответствии с принципом V2X (Vehicle-to-Everytning) взаимодействуют с другими транспортными средствами, транспортной инфраструктурой и любыми другими объектами, которые могут повлиять на их

функционирование. Согласно [1] интеллектуальные транспортные системы (ИТС) представляют собой интеграцию современных информационных и телематических технологий, предназначенных для реализации автоматизированного управления транспортным средством с целью повышения безопасности и эффективности транспортного процесса.

Системы автономного судовождения (САС) представляют собой ИТС, в идеале управляемые полностью автоматически (4-й уровень автономности согласно классификации Международной морской организации (ИМО)). В их состав входят такие подсистемы как [2]:

– автоматическая идентификационная система (АИС), основной целью функционирования которой является автоматическое предоставление идентификационной информации о судне другим судам и береговым службам;

– глобальная навигационная система (ГНСС), она позволяет определять местоположение, скорость судна, а также является источником точного времени UTC (Universal Time Corrected);

– электронная картографическая навигационно-информационная система (ЭКНИС), которая предназначена для отображения информации из электронных навигационных карт, ее интеграции с данными других систем (ГНСС, АИС, лагов и эхолотов), обмена данными с другими судами и по сети Интернет для корректуры электронной карты в процессе плавания;

– радиолокационная система, которая выполняет функции обнаружения воздушных, морских и наземных объектов и определения их дальности, скорости и геометрических параметров;

– система технического зрения, она реализует обнаружение и анализ воздушных, морских и наземных объектов по их изображению.

Представленные выше системы выполняют роль источников информации для поиска и принятия системой автономного судовождения максимально эффективных сценариев управления.

Для масштабного и повсеместного внедрения систем автономного судовождения, эти системы должны быть, по крайней мере, такими же безопасными, как ИТС меньшего уровня автономности. Автономные суда могут снизить количество ошибок, вызванных человеческим фактором, но в то же время подвержены

другим опасным воздействиям обусловленным, в том числе, технологиями искусственного интеллекта (ИИ). Обеспечение информационной безопасности (ИБ) имеет решающее значение для безопасной эксплуатации автономных судов. В рамках настоящей работы отражены угрозы САС, характерные для ИТС, но игнорируемые при традиционном комплексном обеспечении ИБ. Также рассмотрена модель системы мониторинга и оценки рисков ИБ САС с использованием технологий дополненного интеллекта.

Обеспечение ИБ автоматизированной системы технологического управления ИТС

ИТС представляют собой сложные интегрированные системы, выполняющие функционал информационных технологий (ИТ) и операционных технологий (ОТ), другими словами, функционал автоматизированных систем корпоративного управления (АСКУ) и автоматизированных систем технологического управления (АСТУ) соответственно [3]. АСКУ выполняют функции корпоративного управления, управления эксплуатацией и обслуживанием судна и некоторые функции управления движением судна (в части мониторинга, планирования маршрута, отображения данных). В АСТУ выполняются функции автоматического или автоматизированного управления движением судна.

Традиционно обеспечение информационной безопасности (ИБ) определяется защитой свойств информации. Во множестве руководящих документах (требованиях приказов ФСТЭК России № 31, 17) и методиках оценки информационной защищенности систем (методике оценки угроз безопасности информации (утвержденной ФСТЭК России в 2021 году), методике оценки уязвимостей Common Vulnerability Scoring System (CVSS)) определяются три основных свойства информации: конфиденциальность, целостность и доступность. Также выделяются свойства неотказуемости, подотчетности, аутентичности и достоверности информации, при этом под защищаемой информацией подразумевается ее цифровой, а не аналоговый вид.

Обозначим за нарушение свойства подлинности информации намеренное или случайное искажение аналоговой информации до (или при) ее преобразовании в цифровые данные. Свойство

подлинности информации сочетает в себе свойства аутентичности и достоверности информации (применимо к ее аналоговому виду): информация является подлинной, если истинным является ее источник (например, датчик АСТУ) и его показания верны (датчик работает верно, откалиброван и поверен).

Ранее внимание к обеспечению ИБ акцентировалось в основном в отношении АСКУ по той причине, что прежние АСТУ функционировали в замкнутом информационном пространстве и не подвергались угрозам безопасности информации (УБИ), свойственным АСКУ. Благодаря внедрению технологий Интернета вещей (Internet of Things – IoT) в судовождении, из-за которых датчики АСТУ стали конечной точкой сети IoT [4], и повышению уровня автоматизации судов, угроза злонамеренных информационных воздействий на АСТУ начала возрастать.

Реализация угроз безопасности информации (УБИ) на АСТУ, осуществляются непосредственно на устройство, их совокупность и соединяющие каналы связи, порождая желательную для злоумышленника автоматическую реакцию, не требующую участия человека. Примерами таких воздействий могут быть УБИ из банка данных угроз ФСТЭК России:

– УБИ.107: угроза отключения контрольных датчиков (путем прерывания канала связи);

– УБИ.027: угроза искажения вводимой и выводимой на периферийные устройства информации (подмены или искажения аналоговых данных, вводимых и выводимых на датчики).

В качестве меры противодействия УБИ АСТУ предлагается интеграция оборудования АСТУ с криптомодулями (КМ) (рисунок 1), выполняющих криптографические операции с данными, передаваемыми в цифровом виде. Для интеграции криптомодулей с датчиками и исполнительными устройствами, передающими и принимающими информацию в аналоговом виде, необходимы встроенные в них аналого-цифровые и цифро-аналоговые преобразователи (АЦП и ЦАП соответственно).

На рисунке 1 представлена обобщенная схема передачи данных в АСТУ (в защищенной и незащищенной среде). В защищенной среде датчик и исполнительное устройство передают и принимают цифровую информацию (обозначенную сплошной линией) с использованием промышленного криптографического протокола

(например, CRISP (Cryptographic Industrial Security Protocol)). В незащищенной среде передачи данных в АСТУ прием и передача информации в аналоговом виде (обозначенной пунктирной линией) порождает риски нарушения подлинности информации.

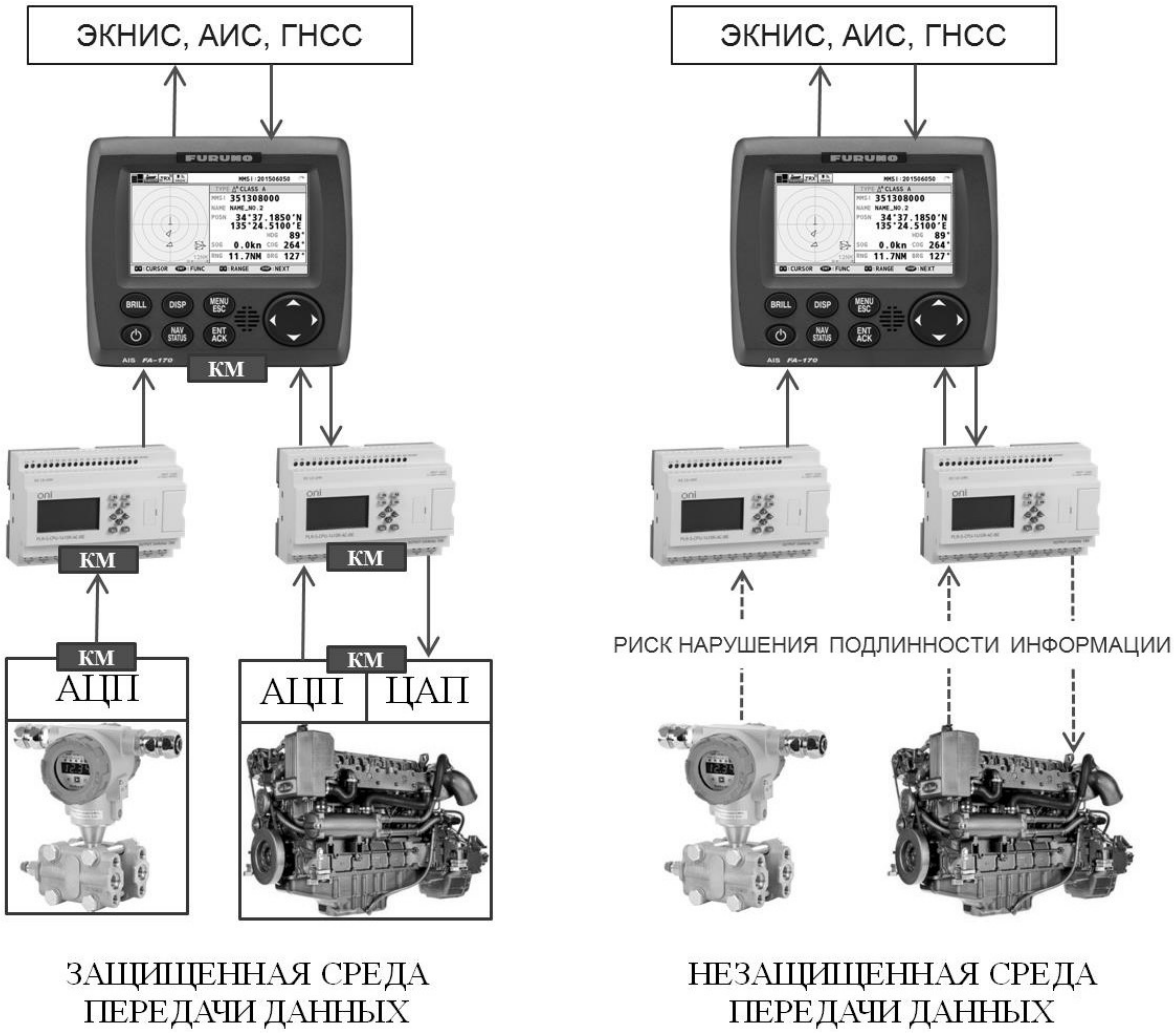

Рисунок 1 – Обобщенная схема передачи данных в АСТУ (в защищенной и незащищенной среде)

Автоматизация оценки и мониторинга рисков систем автономного судовождения

Системы автономного судовождения можно представить как совокупность информационных и телекоммуникационных технологий, технологий автоматического (автоматизированного) управления и технологий искусственного интеллекта (ИИ). Традиционно оценка рисков ИБ осуществляется преимущественно с

использованием метода экспертной оценки, который предполагает оценку рисков на основе субъективного суждения лиц, принимающих решения, и во многом зависит от уровня знаний эксперта. Например, оценка УБИ, связанных с алгоритмами ИИ, может вызвать затруднения у экспертов ИБ, не являющихся разработчиками таких систем. Потому, в том числе, с целью обеспечения мониторинга и переоценки рисков ИБ в режиме реального времени реализуется частичная или полная автоматизация процесса управления рисками ИБ.

Процесс мониторинга и оценки рисков ИБ сложных систем можно назвать слабо или плохо формализуемыми по причине большого количества учитываемых факторов и неявных связей между ними, из-за чего построение строгой математической модели невозможно либо она будет слишком абстрактна для проверки характеристик изучаемого объекта.

На рисунке 2 представлена структура модели системы мониторинга и оценки рисков ИБ систем автоматического судовождения.

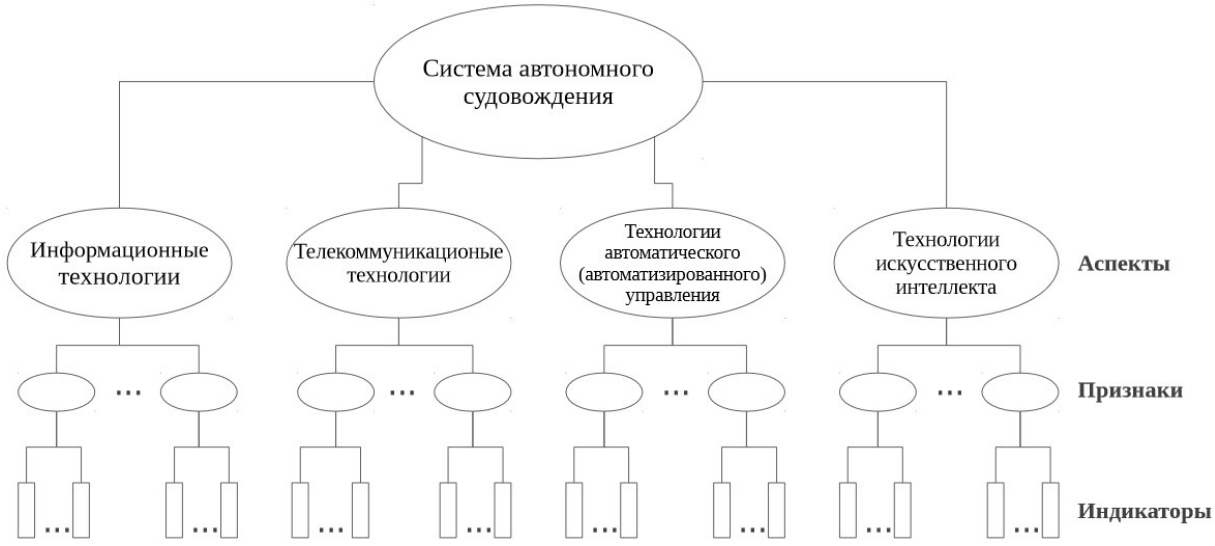

Рисунок 2 – Структура модели системы мониторинга и оценки рисков ИБ систем автоматического судовождения

В работе [5] предложена методика построения человеко-компьютерной системы мониторинга и оценки сложных процессов с использованием технологий дополненного интеллекта (augmented

intelligence). Структура системы представляет собой граф (или дерево) без циклов, вершинами которого являются понятия предметной области, а ребра определяют связь между ними. Агрегаторы информации (эксперты в областях соответствующих технологий) задают экспертные оценки узлам. В зависимости от того, относится ли вносимая информация к проблеме (предметной области) в целом или к какой-то некоторой ее части или элементу, она может быть учтена на разных уровнях иерархии (аспекты, признаки, индикаторы).

Использование методов теории нечетких множеств позволяет вносить в модель фрагментарную информацию. В исследовании [6] предложены и описаны два похода обучения ИИ на основе вносимой экспертами информации: геометрический и логический. Первый подход применим тогда, когда эксперт может только определить значение на некоторых наборах значений. Второй подход обучения ИИ поддерживает также задание некоторых условий на «поведение» оператора агрегирования – функции, которая по набору известных значений смежных вершин графа определяет неизвестное значение.

Развитие и применение человеко-компьютерной системы мониторинга и оценки рисков ИБ систем автономного судовождения согласуется с принятой практикой экспертной оценки рисков ИБ и минимизирует ее недостатки. Использование методов нечетких множеств позволяет вносить фрагментарную и меняющуюся во времени информацию путем достраивания модели операторами агрегирования.

Заключение

В результате исследования определен контекст обеспечения ИБ ИТС и систем автономного судовождения в частности. Обозначена проблема обеспечения ИБ автоматизированных систем технологического управления ИТС и предложено ее решение. Обоснована применимость человеко-компьютерной системы мониторинга и оценки рисков ИБ для систем автономного судовождения и предложена соответствующая модель.

Литература:

1. ГОСТ Р 56829-2015. Интеллектуальные транспортные системы. Термины и определения. Введ. 01.06.2016. – М.: Стандартинформ, 2018. – 14 с.

2. *Oruc A., Gkioulos V., Katsikas S.* Towards a Cyber-Physical Range for the Integrated Navigation System (INS) // Journal of Marine Science and Engineering. – 2022. – Vol. 10. Issue 1. – 31 p.

3. *Михалевич И.Ф.* Проблема цифрового неравенства автоматизированных систем корпоративного и технологического управления // Телекоммуникационные устройства и системы. – 2020. – № 3. – С. 43-46.

4. *Bohlal A., Abdelouahed R.A., Marzak A., Meriem B.* Proposal To Evaluate the Integration of IoT Technologies in The Maritime Domain // Procedia Computer Science. – 2023. – Vol. 220. – P. 1057-1064.

5. *Ryjov P., Mikhalevich I.F.* Hybrid Intelligence Framework for Improvement of Information Security of Critical Infrastructures // Handbook of Research on Cyber Crime and Information Privacy. – 2021. – P. 310-337.

6. *Рыжов А.П.* Об агрегировании информации в нечетких иерархических системах // Интеллектуальные системы. – 2001. – Т. 6. Вып. 1-4. – С. 69-79.

DOI: 10.25728/iccss.2023.89.10.034

Ведищев В.В., Батищев Р.В.

Вероятностный подход при управлении технологией как фактор повышения уровня информационной безопасности производства листового проката

Аннотация: Рассмотрена методика сохранения целостности информации с использованием математических моделей технологического процесса определяющих случайной связи распределений технологических факторов и свойств.

Ключевые слова: технология производства продукта, векторный случайный процесс, множественный