Баранов Л.А., Михалевич И.Ф., Соколов С.С.

Концепция создания доверенной среды функционирования объектов автономного судоходства

Аннотация: В работе рассматриваются вопросы развития отечественных решений в области аппаратно-программных платформ и программно-аппаратных комплексов автономного судоходства, основанные на концепции создания доверенной среды функционирования автоматизированных систем в защищенном исполнении.

Ключевые слова: автономное судоходство, акт незаконного вмешательства, аппаратно-программная платформа, безопасность функционирования, интеллектуальная система водного транспорта, компьютеризированная система, критическая информационная инфраструктура, программно-аппаратный комплекс, угроза, уязвимость

Введение

На объектах автономного судоходства (ОАС) и интеллектуальных систем водного транспорта (ИСВТ) используются разнообразные компьютеризированные системы (информационные, автоматизированного и автоматического управления, искусственного интеллекта (ИИ)) [1]. Их функционирование сопряжено с актами незаконного вмешательства (АНВ) физического и нефизического характера, к которым относятся любые противоправные действия (в том числе компьютерные атаки) или бездействие, угрожающие безопасности ОАС, повлекшие за собой причинение вреда жизни и здоровью людей, материальный ущерб либо создавшие угрозу наступления таких последствий [2].

Обновленной 15.02.2024 г. [3] Национальной стратегией развития ИИ [4] определены новые для страны вызовы. В их числе указано на недостаточное развитие отечественных решений в области аппаратно-программных платформ (АПП) и программно-аппаратных комплексов (ПАК), что в условиях ограничения доступа к новым технологиям в связи с недобросовестной

конкуренцией со стороны недружественных иностранных государств может замедлить научно-технологическое развитие страны, повлечь ее экономическое и технологическое отставание.

Указом Президента Российской Федерации от 18.06.2024 г. № 529 технологии создания доверенного системного и прикладного программного обеспечения включены в перечень важнейших наукоемких критических технологий [5].

Проблема недостаточного развития отечественных решений в области АПП и ПАК для областей, в которых может быть нанесен ущерб национальной безопасности, возникла задолго до 2024 г. Она находит свое отражение, в частности, в стратегиях: национальной безопасности [6], научно-технологического развития [7], развития информационного общества [8], транспортной стратегии [1], Национальной стратегии развития ИИ [4], Доктрине информационной безопасности [9].

Транспортная отрасль отличается от многих других областей цифровой экономики тем, что на ее объектах может одновременно обрабатываться информация различных уровней конфиденциальности: от открытой (общедоступной) до информации, содержащей сведения, составляющие государственную тайну [10], – а архитектура ОАС, как правило, является интегрированной [11].

Изложенные обстоятельства оказывают существенное влияние на доверенные платформенные решения, допустимые к применению в автономном судоходстве с взаимосвязанных позиций национальной безопасности, безопасности критической информационной инфраструктуры (КИИ), транспортной и информационной безопасности.

Концепция создания доверенной среды функционирования объектов автономного судоходства и ИСВТ

В соответствии с [4] доверенными являются решения, отвечающие стандартам безопасности, разработанные с учетом принципов объективности, недискриминации, этичности, исключающие при их использовании возможность причинения вреда человеку и нарушения его основополагающих прав и свобод, нанесение ущерба интересам общества и государства.

Концепция создания доверенной среды функционирования ОАС и ИСВТ является развитием Концепции создания доверенной среды функционирования автоматизированных систем [12], реализованной с учетом [13-14] при создании и внедрении АПП типовых технических решений построения автоматизированных систем в защищенном исполнении (АСЗИ).

Учитывая требования закона, компьютеризированные системы ОАС и ИСВТ относятся к АСЗИ [10]. При развитии Концепции были учтены особенности функционирования ОАС и ИСВТ, рассмотренные, в частности, в [15-17] и вытекающие из отечественного и международного опыта обеспечения безопасности функционирования компьютеризированных систем [18-22].

В соответствии с Концепцией доверенной средой функционирования ОАС (ИСВТ) является среда, отвечающая требованиям по безопасности, созданная с учетом следующих основных принципов [2]:

1) безопасность: недопустимость использования АПП, создающих угрозы безопасности информации ОАС (ИСВТ) или угрозы нарушения (прекращения) функционирования ОАС (ИСВТ) вследствие применения информации, безопасность которой была нарушена;

2) защищенность: безопасность и правовая охрана решений в области АПП для ОАС (ИСВТ), разграничение ответственности организаций – разработчиков АПП и пользователей АПП, а также защита указанных пользователей от негативного влияния АПП на функционирование и безопасность ОАС (ИСВТ) и взаимодействующих с ними иных объектов КИИ;

3) контролируемость: наличие полного комплекта документации на АПП, в том числе о соответствии всех компонентов АПП и процессов достижения результатов их работы по отдельности и совместно в составе вычислительных систем (ПАК) требованиям по безопасности;

4) технологический суверенитет: преимущественное использование отечественных решений в области АПП, независимость от импорта и технологическая независимость: обеспечение полноценности, способности сохранять заявленные характеристики, развиваться и поддерживаться независимо от внешнеполитических и внешнеэкономических

факторов, без применения импортных компонентов, без иностранного участия, принудительного обновления компонентов и управления из-за рубежа, передачи информации, в том числе технологической, за пределы РФ;
5) полноценность: обеспечение полноты состава АПП, необходимого для функционирования ОАС (ИСВТ) различного назначения, разных классов защищенности, уровней топологической и архитектурной сложности;
6) промышленный уровень: обеспечение необходимого уровня производительности, отказоустойчивости и других заявленных характеристик ОАС (ИСВТ) сложных топологии и архитектуры, при высоких нагрузках и больших объемах данных в течение всего срока эксплуатации;
7) универсальность: обеспечение на основе собственных базовых компонентов создание (модернизацию) ОАС (ИСВТ) различного назначения, разных классов защиты и уровней топологической и архитектурной сложности;
8) гарантии развития и поддержки: обеспечение развития, эксплуатации, обслуживания и модернизации ОАС (ИСВТ), созданных на основе АПП;
9) совместимость: обеспечение необходимого уровня аппаратной и программной совместимости компонентов АПП, включенных в вычислительную систему (ПАК), возможность создания на их основе интегрированной программной среды (экосистемы);
10) гибкость: обеспечение возможности создания разнообразных архитектур вычислительных систем (ПАК) на основе компонентов АПП;
11) оперативность: обеспечение сокращения сроков перехода от научного или прикладного исследования к созданию вычислительных систем (ПАК);
12) преемственность (наследование): обеспечение постепенного перехода на отечественное специальное программное обеспечение (СПО) путем последовательного замещения СПО, функционирующего под управлением операционных систем (ОС) из недружественных стран (унаследованное ПО);

13) целостность инновационного цикла: обеспечение тесного взаимодействия научных исследований и разработок в области АПП с реальными потребностями ОАС (ИСВТ);

14) поддержка конкуренции: развитие рыночных отношений и недопустимость действий, направленных на монополизацию и ограничение конкуренции между российскими организациями, осуществляющими деятельность в области АПП.

Функциональными требованиями к АПП РАС (ИСВТ) являются:

– создание (модернизация) и эксплуатация ОАС (ИСВТ) разных классов защиты, безопасное ведомственное, межведомственное взаимодействие ОАС (ИСВТ) и их взаимодействие с зарегистрированными пользователями;

– создание защищенной (доверенной) среды функционирования СПО, разработанного для ОАС (ИСВТ), обеспечение безопасности информации, исходя из класса защиты (категории значимости) ОАС (ИСВТ);

– возможность «мягкой» поэтапной модернизации ОАС (ИСВТ), предполагающая их функционирование при замене средств вычислительной техники и иного оборудования на новое;

– возможность «мягкой» поэтапной модернизации СПО, предполагающая использование введенного ранее в эксплуатацию СПО;

– организация производительного, устойчивого, масштабируемого вычислительного процесса, надежного хранения больших объемов информации, сохранение ее конфиденциальности, доступности и целостности;

– поддержка основных сетевых служб системного и пользовательского уровней;

– сбор, обработка и хранение данных в территориально распределенных ОАС (ИСВТ), возможность безопасного удаленного доступа к этим данным (в установленном порядке), поддержка технологий интеграции вычислительных ресурсов и систем хранения данных, обеспечение строительства (модернизации) и эксплуатации центров обработки данных;

– поддержка многоуровневости и одновременной работы множества пользователей с одними и теми же данными баз (банков) данных, публикация и поиск данных, доступ к данным,

управление контентом, резервирование и архивирование данных, синхронизация обновлений в базах данных;

– контроль и управление функционированием всех устройств, комплексов средств автоматизации, ПАК и др., входящих в состав ОАС (ИСВТ);

– резервирование основных компонентов ОАС (ИСВТ) и содержащейся в них информации;

– работа комплексов информационно-расчётных, аналитических, прогнозных задач, в том числе с применением Web-технологий обработки геопространственных данных и многоэкранного режима, текстовых, графических редакторов, обработка мультимедийной информации;

– доверенная среда разработки СПО.

Заключение

Разработка и реализация компьютеризированных систем объектов автономного судоходства и интеллектуальных систем водного транспорта на основе приведенной Концепции смягчает проблему недостаточности развития отечественных решений в области аппаратно-программных платформ и программно-аппаратных комплексов автономного судоходства, повышает оперативность их разработки, обоснованность принимаемых решений, обеспечивает создание доверенной среды функционирования объектов.

Литература:

1. Транспортная стратегия Российской Федерации до 2030 года с прогнозом на период до 2035 года (утв. распоряжением Правительства Российской Федерации от 27.11.2021 г. № 3363-р).

2. *Михалевич И.Ф.* Проблемы обеспечения безопасности автономного судоходства на внутренних водных путях. – М.: Горячая линия-Телеком, 2024. – 336 с.

3. Указ Президента Российской Федерации от 15.02.2024 № 124 «О внесении изменений в Указ Президента Российской Федерации от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» и в Национальную стратегию, утвержденную этим Указом».

4. Национальная стратегия развития искусственного интеллекта на период до 2030 года (утв. Указом Президента Российской Федерации от 10.10.2017 г. № 490).

5. Указ Президента Российской Федерации от 18.06.2024 г. № 529 «Об утверждении приоритетных направлений научно-технологического развития и перечня важнейших наукоемких технологий».

6. Стратегия национальной безопасности Российской Федерации (утв. Указом Президента Российской Федерации от 02.07.2021 г. № 400).

7. Стратегия научно-технологического развития Российской Федерации (утв. Указом Президента Российской Федерации от 01.12.2016 г. № 642).

8. Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы (утв. Указом Президента Российской Федерации от 09 мая 2017 г. № 203).

9. Доктрина информационной безопасности Российской Федерации (утв. Указом Президента Российской Федерации от 05.12.2016 г. № 646).

10.Федеральный закон от 09.02.2007 г. № 16-ФЗ «О транспортной безопасности».

11. *Михалевич И.Ф.* Концептуальные проблемы транспортной безопасности водных интеллектуальных транспортных систем // Надежность. – 2024. – № 2. – С. 72-87. – URL: https://doi.org/10.21683/1729-2646-2024-24-2-72-87 (дата обращения 10.10.2024).

12. *Михалевич И.Ф.* Проблемы создания доверенной среды функционирования автоматизированных систем управления в защищенном исполнении / Труды XII Всероссийского совещания по проблемам управления (ВСПУ-2014, Москва). – М.: Институт проблем управления им. В.А. Трапезникова РАН, 2014. – С. 9201-9207.

13. *Зегжда Д.П., Ивашко А.М.* К созданию защищенных систем обработки информации // Проблемы информационной безопасности. Компьютерные системы. – 1999. – № 1. – С. 99.

14.*Зегжда Д.П., Ивашко А.М.* Технология создания безопасных систем обработки информации на основе отечественной

защищенной операционной системы // Проблемы информационной безопасности. Компьютерные системы. – 1999. – № 2. – С. 59.

15. *Розенберг И.Н., Соколов С.С., Дубчак И.А.* Методы формирования цифрового двойника акватории для навигации беспилотных судов // Мир транспорта. – 2023. – Т. 21(6). – С. 6-13. – URL: https://doi.org/10.30932/1992-3252-2023-21-6-1 (дата обращения 10.10.2024).

16. *Шубинский, И.Б.* Надежность, риски, безопасность систем управления на железнодорожном транспорте. – Москва; Вологда: Инфра – Инженерия, 2024. – 416 с.

17. *Баранов Л.А., Иванова Н.Д., Михалевич И.Ф., Соколов С.С.* Информационная безопасность системы автономного судовождения в контексте специфических для интеллектуальных транспортных систем угроз / Проблемы управления безопасностью сложных систем: материалы XXXI Международной научной конференции. – Москва: Институт проблем управления им. В.А. Трапезникова РАН, 2023. – С. 249-256.

18. Стратегическое направление в области цифровой трансформации транспортной отрасли Российской Федерации до 2030 года (утв. распоряжением Правительства Российской Федерации от 21.12.2021 г. № 3744-р).

19.Стратегический проект «Электронная навигация и безэкипажное (автономное) судовождение». Программа стратегического академического лидерства «Приоритет-2030». Раздел сайта РУТ (МИИТ). – URL: https://www.miit.ru/page/178854 (дата обращения 01.10.2024).

20.Перечень типовых отраслевых объектов критической информационной инфраструктуры, функционирующих в сфере транспорта (утв. Минтрансом России 15.05.2023 г.). – URL: https://mintrans.gov.ru/documents/7/12506?ysclid=lu2d7qdxnk974324093 (дата обращения 22.09.2024).

21.Методические рекомендации по категорированию объектов критической информационной инфраструктуры, функционирующих в сфере транспорта (утв. Министерством транспорта Российской Федерации 24.01.2024). – URL: https://mintrans.gov.ru/documents/10/13201?ysclid=lu2cx9gfse525544140 (дата обращения 10.09.2024).

22.Principles of operational technology cyber security. – URL: https://www.cyber.gov.au/sites/default/files/2024-10/principles_of_operational_technology_cyber_security.pdf (дата обращения 03.10.2024).

Лещенко В.В., Пантелеймонов И.Н.

Средства систем лазерной космической связи

Аннотация: Рассмотрены средства системы лазерной космической связи (ЛКС). Изложены примеры уровня техники средств такой связи за рубежом и в России. Определены ожидаемые в ближайшем будущем достижения в создании систем ЛКС на примере сети Starlink американской корпорации SpaceX.

Ключевые слова: безопасность, космическая связь, спутниковая связь, лазерная связь, средства связи, межспутниковые каналы

В настоящее время происходит стремительный взлёт темпов создания и использование глобальных систем спутниковой связи (ССС). В этом процессе особое значение приобретают многоспутниковые низкоорбитальные ССС, способные обеспечить абонентов высокоскоростной связью с низкой задержкой, использующие лазерную связь, которая обеспечивает защиту передаваемой информации от несанкционированного доступа к ней и предотвращения внесения в нее помех или недостоверной информации.

Современный технический уровень средств нисходящей высокоскоростной лазерной связи в США и Японии, оцениваемый ими как самый передовой в мире, иллюстрирует рисунок 1, на котором представлен терминал TeraByte InfraRed Delivery (TBIRD) [1].

На рисунке 2 представлена иллюстрация нисходящей линии лазерной связи со скоростью 200 гигабит в секунду [2].

24 мая 2022 г. CubeSat продемонстрировал самую быструю лазерную связь НАСА из космоса. Миссия НАСА Pathfinder