УДК 656.2:004.732:005.92
Оригинальная статья
https://doi.org/10.21683/1729-2646-2025-25-3-42-49

Концепции обеспечения комплексной безопасности АСУ ТП верхнего уровня управления для объектов КИИ железнодорожного транспорта

Concepts for ensuring comprehensive security of upper-level ACSs of railway CII facilities

Попов П.А.[1], Розенберг Е.Н.[1], Сабанов А.Г.[1]*, Шубинский И.Б.[1]
Popov P.A.[1], Rozenberg E.N.[1], Sabanov A.G.[1]*, Shubinsky I.B.[1]
[1] *АО «НИИАС», Москва, Россия*
[1] *JSC NIIAS, Moscow, Russian Federation*
* *a.sabanov@vniias.ru*

Попов П.А.

Розенберг Е.Н.

Сабанов А.Г.

Шубинский И.Б.

Резюме. *Рассматриваются концепции обеспечения комплексной безопасности зоны управления автоматизированных систем управления железнодорожным транспортом верхнего уровня и основные требования регулятора по обеспечению защиты информации. Показано, что представленные концепции не противоречат требованиям ФСТЭК России.*

Abstract. *The paper examines concepts associated with ensuring comprehensive security of the control area of upper-level automated railway control and management systems and the primary regulatory requirements for information protection. It is shown that the presented concepts do not contradict the requirements of the FSTEC of Russia.*

Ключевые слова: *комплексная безопасность, функциональная безопасность, защита информации, автоматизированные системы управления технологическими процессами железнодорожного транспорта.*
Keywords: *comprehensive security, functional safety, information protection, railway automated control systems.*

Для цитирования: *Попов П.А., Розенберг Е.Н., Сабанов А.Г., Шубинский И.Б. Концепции обеспечения комплексной безопасности АСУ ТП верхнего уровня управления для объектов КИИ железнодорожного транспорта // Надежность. 2025. №3. С. 42-49. https://doi.org/10.21683/1729-2646-2025-25-3-42-49*
For citation: *Popov P.A., Rozenberg E.N., Sabanov A.G., Shubinsky I.B. Concepts for ensuring comprehensive security of upper-level ACSs of railway CII facilities. Dependability 2025;3: 42-49. https://doi.org/10.21683/1729-2646-2025-25-3-42-49*

Поступила: *02.04.2025* / **После доработки:** *20.04.2025* / **К печати:** *25.07.2025*
Received on: *02.04.2025* / **Revised on:** *20.04.2025* / **For printing:** *25.07.2025*

Введение

Автоматизированные системы управления технологическими процессами железнодорожного транспорта (АСУ ТП ЖТ) обеспечивают контроль и автоматизированное управление технологическим оборудованием, средствами, а также технологическими процессами по управлению и обеспечению безопасности перевозочного процесса. Такие системы выделяют в отдельный объект защиты, поскольку кроме требований транспортной безопасности к ним предъявляются основные положения Федерального закона № 187 как объектам критической информационной инфраструктуры (КИИ). По уровню управления перевозочным процессом эти системы целесообразно разделить на следующие три зоны управления:

- низового уровня систем автоматического управления исполнительными устройствами (семафоры, стрелки, ж/д переезды и т.п.), характеризующегося отсутствием человека в замкнутой системе управления, не имеющей выхода на коммуникационные сети общего пользования;
- среднего (промежуточного) уровня;
- верхнего уровня систем управления перевозочным процессом с применением телекоммуникационных сетей общего пользования.

Обеспечение комплексной безопасности функционирования систем низового уровня рассмотрено в статье [1], в которой представлен обзор 56 стандартов, рассмотрены теоретические вопросы обеспечения функциональной безопасности, представлена концепция безопасности зоны управления перевозочным процессом низового уровня и впервые сформулированы основные принципы обеспечения безопасности. В зоне управления движением поездов низового уровня комплексная безопасность сводится к выполнению требований функциональной безопасности (ФБ). Заметим, что за время публикации рассматриваемой статьи было опубликовано еще два межгосударственных стандарта по исследуемой теме. Так, в стандарте [2] предлагается математически строго обоснованное определение уровня полноты безопасности (Safety Integrity Level, SIL) для систем механизмов и машин на основе количественного анализа рисков, которое может быть применено для систем АСУ ТП ЖТ низового уровня. Стандарт [3] содержит положения ФБ и защиты информации (ЗИ) на различных этапах жизненного цикла, оптимизацию оценки рисков, повышение эффективности действий по ЗИ и обеспечению ФБ, в том числе при проектировании, концепцию предупреждения конфликтов между функциями обеспечения функциональной безопасности и контрмерами ЗИ.

Настоящая статья является продолжением работы [1] в контексте развития теоретической модели обеспечения комплексной безопасности АСУ ТП ЖТ, включающей в себя ФБ и ЗИ. Целью данной работы является рассмотрение концепций обеспечения ФБ и ЗИ зоны управления перевозочным процессом верхнего уровня, где требования обеспечения безопасности информации АСУ ТП ЖТ превалируют над требованиями обеспечения ФБ в силу использования сетей общего пользования, являющихся источником многочисленных и разнообразных кибератак.

1. Основные отличия систем верхнего и низового уровней управления

Приведем три наиболее существенных отличия систем верхнего и нижнего уровней управления.

Самым существенным отличием систем верхнего уровня от рассмотренных в работе [1] замкнутых систем исполнительных устройств низового уровня является наличие подключенных сетей общего пользования и значительный объем принимаемой, обрабатываемой и отправляемой информации. На верхнем уровне, как правило, находятся операторские (диспетчерские), инженерные автоматизированные рабочие места, промышленные серверы (SCADA-серверы) с установленным на них общесистемным и прикладным программным обеспечением (ПО), телекоммуникационное оборудование (коммутаторы, маршрутизаторы, межсетевые экраны, иное оборудование), а также каналы связи. Управляющая информация для среднего уровня, как правило, поступает именно с верхнего уровня.

Вторым отличием является разнообразие обрабатываемой системами АСУ ТП ЖТ информации. Если на низовом уровне входящая информация поступает с рельсовых цепей в виде небольших по объему сигналов, то системы верхнего уровня, особенно, системы интеллектуального управления движением, технического зрения, показания датчиков интернета вещей и подключаемого искусственного интеллекта характеризуются значительными массивами обрабатываемой информации. В случаях обработки информационной системой АСУ ТП ЖТ конфиденциальной информации перечень рассматриваемых угроз безопасности информации должен включать в себя угрозы утечки информации ограниченного доступа. При необходимости обеспечения целостности и конфиденциальности информации, принимаемой и обрабатываемой на верхнем уровне, применяются средства защиты информации (СЗИ) и средства криптографической защиты информации в соответствии с требованиями ФСБ России.

К третьему отличию можно отнести смену приоритетов свойств обрабатываемой системами верхнего и низового уровня информации. Если для низового уровня исполнительных устройств общепризнанно приоритеты по уменьшению значимости выстраиваются в порядке «доступность, целостность, конфиденциальность», то для систем верхнего уровня порядок обратный: конфиденциальность, целостность, доступность для уполномоченных пользователей. Для некоторых видов

управляющей информации бывает важен учет неотказуемости от авторства, достоверности, актуальности, подотчетности и т.п. Приоритетность свойств обрабатываемой информации тесно связана с обеспечением безопасности функционирования систем верхнего и нижнего уровней управления. Так, общепризнано, что нейтрализация угроз функционированию систем низового уровня управления полностью обеспечивается выполнением мер функциональной безопасности. В то же время для систем верхнего уровня управления в первую очередь важно выполнение мер ЗИ, при этом системы ЗИ не должны нарушать выполнению мер ФБ. Основные теоретические положения и требования ФБ достаточно подробно представлены в работе [1], рассмотрим требования ЗИ, поскольку для верхнего уровня управления количество угроз безопасности информации превалирует над количеством угроз, связанным с функциями безопасности движения.

2. Требования защиты информации

Требования обеспечения безопасности информации в системах АСУ ТП ЖТ в основном определяются нормативными правовыми актами ФСТЭК России. В полной мере это относится к системам верхнего уровня управления, к которым одновременно необходимо применять требования приказов ФСТЭК России № 31 для АСУ ТП и № 239 для объектов КИИ, а также приказов № 17, № 21 и методики оценки угроз безопасности информации от 05.02.2021 г. Так, в приказе № 31 определены три уровня АСУ:

- верхний уровень операторского (диспетчерского) управления;

- средний уровень автоматического управления, на котором функционируют программируемые логические контроллеры, иные технические средства с установленным ПО, получающие данные с нижнего (полевого) уровня, передающие данные на верхний уровень для принятия решения по управлению объектом и (или) процессом и формирующие управляющие команды (управляющую (командную) информацию) для исполнительных устройств, а также промышленная сеть передачи данных;

- нижний (полевой) уровень ввода/вывода данных исполнительных устройств, на котором находятся датчики, исполнительные механизмы, иные аппаратные устройства с установленными в них микропрограммами и машинными контроллерами.

Видно, что зоны управления с точки зрения ФБ, определенные во введении данной статьи, немного не совпадают с представленными в приказе № 31 уровнями. Так, низовой уровень управления системами АСУ ТП ЖТ включает в себя нижний и средний уровни, определенные в [4]. В этой зоне требования обеспечения безопасности информации, как было показано в предыдущем разделе, происходят из требований ФБ и для ПО иерархия приоритетов безопасности информации может быть представлена в виде: целостность, доступность, отсутствие уязвимостей и недекларированных возможностей (НДВ).

Рассмотрим требования [4] регулятора к обеспечению безопасности информации АСУ ТП подробнее. При проектировании системы защиты автоматизированной системы управления должны учитываться особенности функционирования ПО и технических средств на каждом из уровней автоматизированной системы управления. В автоматизированной системе управления объектами защиты являются:

- информация (данные) о параметрах (состоянии) управляемого (контролируемого) объекта или процесса (входная (выходная) информация, управляющая (командная) информация, контрольно-измерительная информация, иная критически важная (технологическая) информация);

- программно-технический комплекс, включающий технические средства (в том числе автоматизированные рабочие места, промышленные серверы, телекоммуникационное оборудование, каналы связи, программируемые логические контроллеры, исполнительные устройства), ПО (в том числе микропрограммное, общесистемное, прикладное), а также средства ЗИ.

Организационные и технические меры ЗИ:

- должны обеспечивать доступность обрабатываемой в автоматизированной системе управления информации (исключение неправомерного блокирования информации), ее целостность (исключение неправомерного уничтожения, модифицирования информации), а также, при необходимости, конфиденциальность (исключение неправомерного доступа, копирования, предоставления или распространения информации);

- должны соотноситься с мерами по промышленной, физической, пожарной, экологической, радиационной безопасности, иными мерами по обеспечению безопасности автоматизированной системы управления и управляемого (контролируемого) объекта и (или) процесса;

- не должны оказывать отрицательного влияния на штатный режим функционирования автоматизированной системы управления.

Определение угроз безопасности информации осуществляется на каждом из уровней автоматизированной системы управления и должно включать:

- выявление источников угроз безопасности информации и оценку возможностей (потенциала) внешних и внутренних нарушителей;

- анализ возможных уязвимостей автоматизированной системы и входящих в ее состав программных и программно-аппаратных средств;

- определение возможных способов (сценариев) реализации (возникновения) угроз безопасности информации;

- оценку возможных последствий от реализации (возникновения) угроз безопасности информации, нарушения отдельных свойств безопасности информации (целостности, доступности, конфиденциальности) и автоматизированной системы управления в целом.

В качестве исходных данных при определении угроз безопасности информации используется банк данных угроз безопасности информации, ведение которого осуществляется ФСТЭК России, а также иные источники, содержащие сведения об уязвимостях и угрозах безопасности информации.

По результатам определения угроз безопасности информации могут разрабатываться рекомендации по корректировке структурно-функциональных характеристик автоматизированной системы управления, направленные на блокирование (нейтрализацию) отдельных угроз безопасности информации.

Модель угроз безопасности информации должна содержать описание автоматизированной системы управления и угроз безопасности информации для каждого из уровней автоматизированной системы управления, включающее описание возможностей нарушителей (модель нарушителя), возможных уязвимостей автоматизированной системы управления, способов (сценариев) реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации (доступности, целостности, конфиденциальности) и штатного режима функционирования автоматизированной системы управления.

Рассмотрим требования регулятора к верхнему уровню управления.

На основе модели угроз на верхнем уровне управления АСУ ТП определяются меры ЗИ при информационном взаимодействии с иными автоматизированными (информационными) системами и информационно телекоммуникационными сетями, а также осуществляется проверка (в том числе при необходимости с использованием макетов или тестовой зоны) корректности функционирования автоматизированной системы управления с системой защиты и совместимости выбранных средств ЗИ с ПО и техническими средствами автоматизированной системы управления.

Наличие межсетевого взаимодействия и требование защиты от несанкционированного доступа (НСД) передающихся по сетям общего пользования команд управления движением железнодорожного транспорта накладывает дополнительные требования к обеспечению безопасности информации.

По этой причине на верхнем уровне управления количество задач ЗИ возрастает в разы относительно низового уровня. В зависимости от угроз безопасности информации и потенциальных последствий от их реализации, зачастую на первый план выходят задачи обеспечения конфиденциальности передаваемой и принимаемой информации, а задачи обеспечения доступности и целостности отступают на второй план. Цифровизация и применение новых технологий (развитие квантовых коммуникаций и использование квантового распределения ключей, техническое зрение, применение искусственного интеллекта, автоматизация управления движением без участия машиниста) усложняет задачи ЗИ. К тому же почти все сертифицированные СЗИ не удовлетворяют требованиям ОАО «РЖД» в части температурных режимов, вибростойкости, электромагнитной совместимости и др. В итоге в ОАО «РЖД» разрабатываются специализированные СЗИ, примером является линейка продуктов с общим названием ТИТАН.

Таким образом, в связи с ростом количества угроз информации при переходе от низового уровня до верхнего уровня существенно увеличивается и количество задач обеспечения безопасности информации. На верхнем уровне количество задач ЗИ превалирует над задачами функциональной безопасности. Тем не менее, установка любых СЗИ на верхнем уровне не должна оказывать значительного снижения эффективности функций безопасности.

На промежуточном (среднем) уровне соотношение предметных областей и задач ФБ и обеспечения безопасности информации также определяется из анализа актуальных угроз.

3. Концепции обеспечения безопасности верхнего уровня управления

3.1 Концепция взаимозависимости предметных областей функциональной и информационной безопасности

Рассмотрим вопрос взаимозависимости зон ответственности ФБ и информационной безопасности (ИБ) с использованием материалов, представленных в стандарте [5].

Соотношение предметных областей ФБ и ИБ и рассматриваемого стандарта представлено на рис. 1.

Рис. 1. Соотношение предметных областей ФБ и ИБ [5].

Рассмотрим, какие функции безопасности являются общими в решении задач ФБ и ИБ. Минимальный набор требований ЗИ для общей области ФБ и ИБ для низовых систем (условно – до уровня диспетчерской централизации), которые работают в автоматическом режиме без связи с общедоступными сетями передачи

данных (ОбТН), на основе анализа стандартов по ФБ выделен в работе [1].

На верхнем уровне взаимодействия с использованием ОбТН существенно возрастают риски, связанные с потенциальными вероятными опасными событиями нарушений безопасности информации. Для категорированных значимых объектов КИИ (а также для объектов без категории) согласно требованиям приказа ФСТЭК России [6] базовые требования к системам АСУ ТП ЖТ как объектов КИИ независимо от категории (в том числе объектов КИИ без категории) состоят из минимального набора, базового набора и уточненного набора требований.

Минимальный набор состоит из следующих требований:

- защита от НСД;
- обеспечение целостности программ и данных;
- обеспечение доступности информации для легальных пользователей в пределах их полномочий;
- отсутствие НДВ;
- отсутствие уязвимостей.

Указанный минимальный набор требований к АСУ ТП ЖТ установлен как из требований стандартов функциональной безопасности, так и из требований действующей нормативно-правовой базы ЗИ объектов КИИ. Данный набор требований может быть представлен в виде общей предметной области для сетей ОбТН на рис. 1. Заметим, что наборы минимальных требований по ЗИ, общих для ФБ и ИБ, в замкнутых системах управления железнодорожным транспортом и системах, имеющих выход на общедоступные коммуникационные сети, практически совпадают.

Для ПО значимых объектов КИИ согласно п. 22 приказа [6] базовый набор требований шире и включает в себя следующие организационно-технические меры ЗИ:

- идентификация и аутентификация (ИАФ);
- управление доступом (УПД);
- ограничение программной среды (ОПС);
- защита машинных носителей информации (ЗНИ);
- аудит безопасности (АУД);
- антивирусная защита (АВЗ);
- предотвращение вторжений (компьютерных атак) (СОВ);
- обеспечение целостности (ОЦЛ);
- обеспечение доступности (ОДТ);
- защита технических средств и систем (ЗТС);
- защита информационной (автоматизированной) системы и ее компонентов (ЗИС);
- управление конфигурацией (УКФ);
- управление обновлениями ПО (ОПО);
- реагирование на инциденты ИБ (ИНЦ);
- обеспечение действий в нештатных ситуациях (ДНС).

При этом для объектов КИИ на ПО в составе СЗИ применимы положения приказа ФСТЭК России [6], указанные СЗИ должны быть сертифицированы по требованиям ФСТЭК России [7] не ниже 6 уровня доверия.

Базовый набор мер по обеспечению безопасности значимого объекта подлежит адаптации (уточнению) в соответствии с угрозами безопасности информации, применяемыми информационными технологиями и особенностями функционирования значимого объекта. При этом из базового набора могут быть исключены меры, непосредственно связанные с информационными технологиями, не используемыми в значимом объекте, или характеристиками, не свойственными значимому объекту. В случае, если базовый набор мер не позволяет обеспечить блокирование (нейтрализацию) всех угроз безопасности информации [8], в него включаются дополнительные меры защиты. В этом случае согласно пункту 23 приказа [6] применительно к значимому объекту КИИ (определенному классу объектов) разрабатывается адаптированный набор мер защиты на основе анализа рисков, утвержденной модели угроз безопасности информации, а также категории значимости объектов КИИ ЖТ как объекта КИИ. Таким образом формируется уточненный набор мер информационной безопасности объектов КИИ ЖТ.

Требования к отсутствию уязвимостей и НДВ в АСУ ТП ЖТ задают через уровень доверия на основе модели угроз безопасности информации и категории значимости объектов КИИ ЖТ как объекта КИИ, определяемого в соответствии с Федеральным законом 187-ФЗ, Постановлением Правительства Российской Федерации от 14.11.2023 № 1912 и приказом ФСТЭК России [6].

Как правило, в практической деятельности внедрение мер ИБ осуществляется на этапе опытной эксплуатации системы. В случае, когда набор мер по ЗИ, определенный на основе модели угроз, не обеспечивает блокирование (нейтрализацию) всех угроз безопасности информации объектов КИИ ЖТ, должны применяться меры и соответствующие им дополнительные, наложенные СЗИ, отвечающие требованиям как ФБ, так и ИБ. При этом должна проводиться оценка влияния СЗИ на все необходимые функции безопасности системы. В таком случае для объектов КИИ ЖТ с реализованным набором мер безопасности должно быть разработано доказательство безопасности [9].

3.2 Концепция защищенной среды

Чтобы правильно понять рассмотренную в предыдущем разделе и представленную на рис. 1 общую область для предметных областей ФБ и ИБ, рассмотрим предложенную в [5] концепцию «защищенной среды». Защищенная среда, представленная на рис. 2, включает в себя набор мер ЗИ, необходимых для обеспечения эффективной защиты среды при выполнении функций безопасности системой ФБ. Однако эти меры защиты не ограничиваются лишь защитой функций безопасности.

Защищенная среда включает (но этим не ограничивается) следующие меры ЗИ:

- меры ЗИ, защищающие периметры защищенной среды;

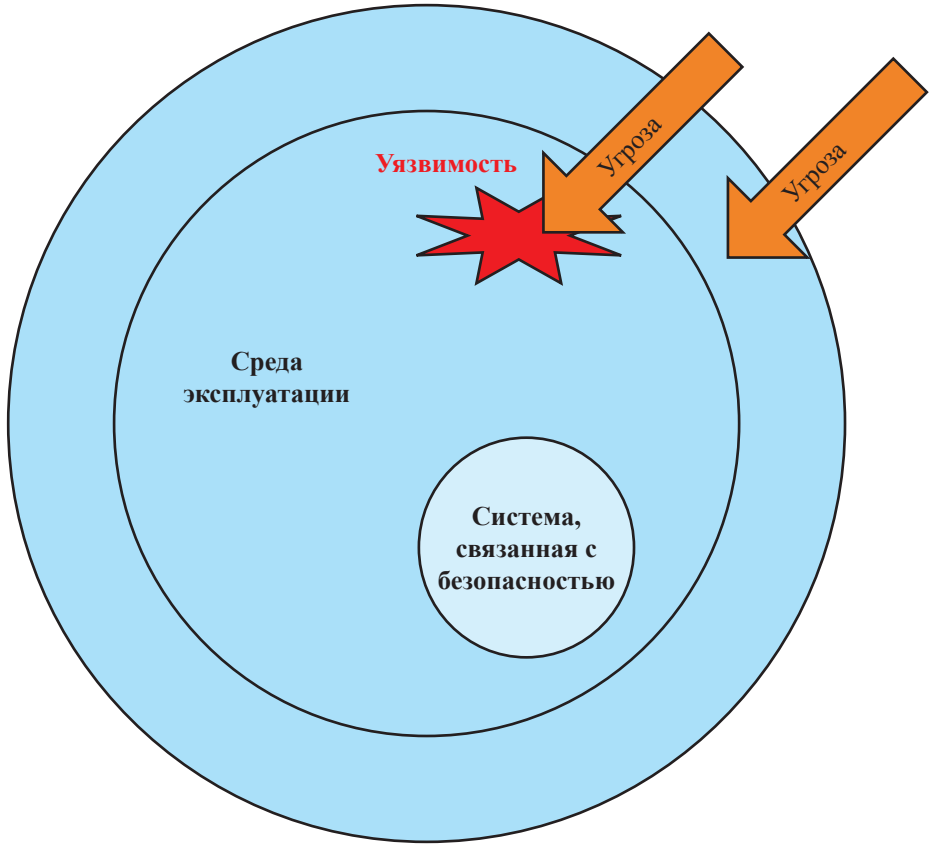

Рис. 2. Защищенная среда [5]

- меры ЗИ, касающиеся взаимодействия между различными функциональными элементами в защищенной среде;
- меры ЗИ, применяемые в функциональных элементах в защищенной среде.

При этом на практике меры ЗИ могут охватывать не только функции безопасности. В зависимости от актуальности угроз безопасности информации защищенная среда может быть построена по принципу «эшелонированной обороны» для достижения достаточной устойчивости приложений от внешних воздействий.

Меры ЗИ в защищенной среде могут быть интегрированы в любой функциональный элемент технической системы, включая функциональный элемент системы, связанной с безопасностью. В качестве мер ЗИ для защищенной среды могут быть определены одна или несколько зон.

Для предотвращения влияющих на функции безопасности и использующих уязвимости угроз от НСД или ошибок персонала защищенную среду необходимо сформировать и поддерживать.

На рис. 2 показаны взаимосвязи между защищенной средой, средой эксплуатации и системой, связанной с безопасностью.

3.3 Концепция единой модели угроз

Логичным развитием концепции защищенной среды представляется разработка единой модели угроз, включающей в себя как угрозы невыполнения заданных функций безопасности по требованиям ФБ, так и угрозы нарушения безопасности информации.

Построение модели угроз наиболее эффективно, когда в ней учитываются наиболее актуальные риски. Для выявления и классификации рисков их оценку можно рассматривать на уровне системы, охватывая как вопросы информационной безопасности, так и вопросы функциональной безопасности. Процессы оценки рисков (ФБ) и оценки рисков-угроз (ИБ) являются схожими, поскольку в обоих случаях предполагается учитывать последствия угроз и/или отказов. Однако по ряду аспектов они различаются. Например, вероятность того, что злоумышленники воспользуются уязвимостью, не детерминирована и может быть оценена только качественно на основе накопленного опыта. Характеристики ЗИ, как правило, также невозможно определить количественно.

Оценка рисков ФБ и ИБ должна соответствовать требованиям ГОСТ 33433, ГОСТ Р 51901, ГОСТ Р ИСО/МЭК 27001 и ГОСТ Р ИСО/МЭК 27005 с применением методов оценки рисков ГОСТ Р 31010. Все действия по оценке рисков и разработке единой модели угроз в областях ФБ и ИБ могут выполняться независимо отдельными группами специалистов, но лучше, если они объединены одной общей командой. При этом эксперты по ФБ и эксперты по ИБ должны пытаться достичь согласия и работать сообща.

3.4 Основополагающие принципы

В работе [5] содержится ряд рекомендаций, сформулированных в виде основополагающих принципов. Модернизируем эти принципы для верхнего уровня управления АСУ ТП ЖТ, дополнив их учетом обеспечения безопасности перевозочного процесса.

Принцип 1. Выполнение заданных функций безопасности. Безопасность перевозочного процесса обеспечивается бесперебойным функционированием автоматизированной системы управления в штатном режиме, при котором обеспечивается соблюдение проектных пределов значений параметров выполнения целевых функций безопасности автоматизированной системы управления в условиях воздействия угроз безопасности информации. Согласно [4] применяемые меры ЗИ не должны оказывать отрицательного влияния на штатный режим функционирования автоматизированной системы управления.

Принцип 2. ЗИ в реализациях систем, связанных с безопасностью. Меры ЗИ должны эффективно предотвращать и/или защищать от негативного влияния угроз системы ФБ и реализуемые ими функции безопасности. Оценки функций безопасности должны учитывать допущение о наличии эффективных мер ЗИ.

Принцип 3. Защита реализаций систем ИБ. Меры обеспечения ФБ не должны оказывать негативное влияние на эффективность реализации мер ЗИ. При этом человеческий фактор учитывается как в предметной области ФБ, так и в предметной области ЗИ.

Принцип 4. Совместимость реализаций. Средства реализации ЗИ и средства реализации системы ФБ не должны оказывать негативного влияния на функционирование друг друга. Если рассматривать снижение уровня рисков, реализуемое системами ФБ и ИБ, то заранее определенного предпочтения между ними, как правило, не существует [5].

Видно, что представленные принципы не противоречат основным положениям приказов № 31 и № 239 ФСТЭК России. Рассмотренные принципы фактически детализируют известный подход по учету требований ИБ на ранних стадиях проектирования, известный как Secure by Design.

Заключение

Рассмотрены основные отличия верхнего уровня управления АСУ ТП ЖТ от низового уровня, а также разницу в подходах к определению уровней управления АСУ ТП общего назначения, рассмотренных в приказе № 31 ФСТЭК России, от АСУ ТП железнодорожного транспорта. Рассмотрены проблемы обеспечения комплексной безопасности в АСУ ТП ЖТ верхнего уровня управления и требования регулятора к ЗИ. Представлены концепции безопасности зоны управления перевозочным процессом верхнего уровня. Показано, что представленные концепции не противоречат требованиям ФСТЭК России.

Данная работа рассматривается в качестве подготовки материала для научно обоснованной разработки стандартов, объединяющих требования функциональной и информационной безопасности к АСУ ТП ЖТ.

Список литературы

1. Комплексная безопасность АСУ ТП объектов КИИ железнодорожного транспорта / П.А. Попов, Е.Н. Розенберг, А.Г. Сабанов, И.Б. Шубинский // Надежность. 2024. № 4. С. 48-57. DOI: 10.21683/1729-2646-2024-24-4

2. ГОСТ Р 71454-2024/IEC TR 63161:2022 Назначение требований к полноте безопасности. Обоснование. М.: Российский институт стандартизации, 2024. IV, 36 с.

3. ГОСТ Р 71452-2024/IEC/PAS 63325:2020. Требования к функциональной безопасности и защите системы контроля промышленной автоматизации (IACS) на протяжении жизненного цикла. М.: Российский институт стандартизации, 2024. IV, 12 с.

4. Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и окружающей природной среды, утвержденные приказом ФСТЭК России от 14.03.2014 № 31.

5. ГОСТ Р 59505-2021 Измерение, управление и автоматизация промышленного процесса. Основные принципы обеспечения функциональной безопасности и защиты информации. М.: Стандартинформ, 2021. IV, 28 с.

6. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденные приказом ФСТЭК России от 25.12.2017 № 239.

7. Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий, утвержденные приказом ФСТЭК России от 02.06.2020 № 76.

8. Надеждин Ю.М. Безопасность АСУ ТП критически важных объектов // Системы безопасности. 2014. № 2. С. 34–39.

9. ГОСТ 33432-2015 Безопасность функциональная. Политика, программа обеспечения безопасности. Доказательство безопасности объектов железнодорожного транспорта.

References

1. Popov P.A., Rozenberg E.N., Sabanov A.G., Shubinsky I.B. Integrated Safety of ACS of Railway CII Facilities. *Dependability* 2024;24(4):48-57. (in Russ.) https://doi.org/10.21683/1729-2646-2024-24-4-48-57.

2. GOST R 71454-2024/IEC TR 63161:2022. Assignment of a safety integrity requirements. Basic rationale. Moscow: Russian Standardization Institute; 2024. (in Russ.)

3. GOST R 71452-2024/IEC/PAS 63325:2020. Lifecycle requirements for functional safety and security for IACS. Moscow: Russian Standardization Institute; 2024. (in Russ.)

4. [Information security requirements for automated process management systems at critical facilities, potentially hazardous facilities, as well as facilities that pose an increased danger to human life and health and the environment approved by order of the FSTEC of Russia dated 14.03.2014 No. 31.] (in Russ.)

5. GOST R 59505-2019. Industrial-process measurement, control and automation. Framework for functional safety and security. Moscow: Standartinform; 2021. (in Russ.)

6. [Safety requirements for significant facilities of critical information infrastructure of the Russian Federation approved by the order of the FSTEC of Russia dated December 25.12.2017 No. 239]. (in Russ.)

7. [Information security requirements that define the levels of trust to the information security and information technology protection tools approved by order of the FSTEC of Russia dated 02.06.2020 No. 76]. (in Russ.)

8. Nadezhdin Yu.M. Security of critical facility PCS. *Security and Safety* 2014;2:34-39. (in Russ.)

9. GOST 33432-2015. Functional safety. Policy and programm of safety provision. Safety proof of the railway objects.

Сведения об авторах

Попов Павел Александрович – кандидат технических наук, заместитель Генерального директора – директор Санкт-Петербургского филиала АО «НИИАС» Москва Российская Федерация, e-mail: P.Popov@vniias.ru

Розенберг Ефим Наумович – профессор, доктор технических наук, первый заместитель Генерального директора АО «НИИАС», Москва, Российская Федерация, e-mail: info@vniias.ru

Сабанов Алексей Геннадьевич – доцент, доктор технических наук, главный эксперт научно-технического комплекса «Технологии информационного общества» АО «НИИАС», Москва, Российская Федерация, e-mail: asabanov@mail.ru

Шубинский Игорь Борисович – профессор, доктор технических наук, эксперт Научного совета при Совете Безопасности РФ, главный эксперт АО «НИИАС», Москва, Российская Федерация, e-mail: igor-shubinsky@yandex.ru

About the authors

Pavel A. Popov, Candidate of Engineering, Deputy Director General, Director, Saint Petersburg Branch, JSC NIIAS, Moscow, Russian Federation, e-mail: P.Popov@vniias.ru.

Efim N. Rozenberg, Professor, Doctor of Engineering, First Deputy Director General, JSC NIIAS, Moscow, Russian Federation, e-mail: info@vniias.ru.

Alexey G. Sabanov, Associate Professor, Doctor of Engineering, Chief Expert, Information Society Technologies Integrated Research and Development Unit, JSC NIIAS, Moscow, Russian Federation, e-mail: asabanov@mail.ru.

Igor B. Shubinsky, Professor, Doctor of Engineering, Expert, Scientific Council under the Security Council of the Russian Federation, Chief Expert, JSC NIIAS, Moscow, Russian Federation, e-mail: igor-shubinsky@yandex.ru.

Вклад авторов в статью

Попов П.А. – функционирование АСУ ТП ЖТ.

Розенберг Е.Н. – постановка задачи.

Сабанов А.Г. – задачи ИБ, анализ стандартов.

Шубинский И.Б. – функциональная надежность и функциональная безопасность АСУ ТП ЖТ.

Конфликт интересов

Авторы заявляют об отсутствии конфликта интересов.