АВТОМАТИКА, ТЕЛЕМЕХАНИКА И СВЯЗЬ

УДК 621.38:656.26

К. А. БОЧКОВ, доктор технических наук, С. Н. ХАРЛАП, кандидат технических наук, А. Н. КОВРИГА, канд. техн. наук, Белорусский государственный университет транспорта, г. Гомель

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МИКРОЭЛЕКТРОННЫХ СИСТЕМ ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ В ЖИЗНЕННОМ ЦИКЛЕ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

Рассмотрены подходы к обеспечению функциональной и информационной безопасности в рамках единого жизненного цикла систем железнодорожной автоматики и телемеханики. Обоснована возможность использования методов обеспечения функциональной безопасности для решения задач информационной безопасности. Приведены примеры обеспечения доступности, целостности и конфиденциальности информации методами функциональной безопасности. Сформулированы задачи функциональной и информационной безопасности, которые должны быть решены в рамках единого жизненного цикла.

На современном этапе развития информационных технологий, в результате активного внедрения этих технологий в различные сферы экономики и промышленности, вопросы информационной безопасности становятся всё более актуальными и их значение возрастает. В последнее время актуальными стали вопросы защиты объектов информационной инфраструктуры железнодорожного транспорта от кибератак и кибертерроризма.

Кибератака – целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации [1].

Кибертерроризм – атаки на информационные системы, несущие угрозу здоровью и жизни людей, а также способные спровоцировать серьезные нарушения функционирования критически важных объектов в целях оказания воздействия на принятие решений органами власти либо воспрепятствования политической или иной общественной деятельности, либо устрашения населения, либо дестабилизации общественного порядка [1].

Следует учитывать, что объектами критической информационной инфраструктуры (КИИ), к которым предъявляются требования информационной безопасности, являются системы, очень сильно отличающиеся друг от друга в части требований условий функционирования, надежности и готовности, функциональной безопасности, коммуникаций и т. д. Многообразие объектов КИИ требует в ответ многообразия методов обеспечения информационной безопасности, а также признания того, что одни и те же методы будут иметь различную эффективность при их применении к различным объектам КИИ.

При этом безопасность людей, социальной и экологической сферы не является предметом информационной защиты. Методы и средства, обеспечивающие исключительно информационную безопасность, не в силах решить эти задачи. Особенно это актуально для автоматизированных систем управления ответственными технологическими процессами (АСУ ОТП), которые широко применяются на железнодорожном транспорте.

Типовым представителем систем управления ответственными технологическими процессами на железнодорожном транспорте являются системы железнодорожной автоматики и телемеханики (ЖАТ). Особенностью систем ЖАТ является то, что в первую очередь данные системы должны выполнять требования функциональной безопасности, заключающиеся в обеспечении безопасности движения поездов, и только во вторую очередь все остальные требования, включая требования информационной безопасности. Такой подход отражен как в Техническом регламенте Таможенного союза «О безопасности инфраструктуры железнодорожного транспорта» [2], так и в Приказах ФСТЭК России № 31 от 14.03.2014 и № 239 от 25.12.2017.

Подходы к обеспечению функциональной и информационной безопасности. На протяжении уже более 200 лет разрабатывались и успешно применялись различные подходы, принципы и методы обеспечения функциональной безопасности, многие из которых не зависят от используемой элементной базы. Более 50 лет эти методы успешно применяются при построении микроэлектронных программируемых систем железнодорожной автоматики. Накопленные знания в области построения безопасных систем ЖАТ на текущем этапе развития могут успешно применяться и для решения новых задач, связанных с нарушением информационной безопасности.

Функциональная безопасность (*functional safety*) – это часть общей безопасности системы управления, зависящая от правильности ее функционирования и обеспечивающая отсутствие неприемлемого риска здоровью людей, их собственности или окружающей среде со своей стороны [3]. То есть система, отвечающая требованиям функциональной безопасности, не должна подвергать опасности здоровье и жизнь людей, приводить к значительным экономическим потерям и разрушению окружающей среды.

Основополагающим стандартом верхнего уровня в области функциональной безопасности стал IEC 61508

«Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью». В Российской Федерации он известен как ГОСТ Р МЭК 61508–2012. Этот фундаментальный стандарт в семи частях содержит не только требования к системам АСУ ТП, но и основные методы для достижения выполнения этих требований. Он ранжирует системы, связанные с безопасностью, по уровню полноты безопасности (УПБ), который может быть определен как количественно через интенсивность или вероятность опасного события, так и качественно через величину возможного ущерба. Положения этого стандарта детализированы в соответствующих отраслевых стандартах. Системы ЖАТ по данной классификации относятся к наивысшему четвертому уровню полноты безопасности УПБ4.

В последних поколениях систем ЖАТ, построенных с использованием аппаратно-программных комплексов на базе локальных и внешних сетей связи с автоматизированными рабочими местами операторов и центрами управления движением поездов, естественным образом возникает проблема обеспечения информационной безопасности. На сегодня проблема информационной безопасности систем ЖАТ решается следующим образом. Разработчик сначала должен выполнить все установленные процедуры по подтверждению соответствия требованиям функциональной безопасности (испытания, верификацию ПО и т. д.) и экспертизу специального документа «Доказательство безопасности» в соответствующей лаборатории, аккредитованной в области функциональной безопасности. Далее он должен выполнить ряд процедур подтверждения соответствия требованиям информационной безопасности с участием лаборатории, аккредитованной в области информационной безопасности. Результатом выполнения таких процедур является создание дополнительных средств защиты, которые являются внешними по отношению к средствам обеспечения функциональной безопасности.

Такой подход является избыточным, так как методы защиты частично могут дублировать друг друга. И хотя в Приказе № 239 ФСТЭК России от 25.12.2017 рекомендовано, что если меры функциональной безопасности являются достаточными для нейтрализации актуальных угроз информационной безопасности, то дополнительные меры защиты можно не применять, эти рекомендации на практике не выполняются. Основанием для этого служат различия в перечне угроз и объектов защиты. Интегрировать же дополнительные средства защиты в комплекс мер функциональной безопасности невозможно, т. к. это потребует повторной процедуры подтверждения соответствия требованиям функциональной безопасности.

Кроме того, следует отметить, что законодательство Республики Беларусь не определяет область обеспечения функциональной безопасности, процессы ее взаимодействия с информационной безопасностью, методы организации и какие-либо требования к ней. Все вопросы обеспечения кибербезопасности включают в себя исключительно информационную безопасность, а зачастую именно так и называются.

Практический опыт испытаний и экспертиз различных систем ЖАТ позволяет сделать вывод о том, что методы обеспечения функциональной безопасности и информационной безопасности достаточно близки и могут быть интегрированы на ранних этапах разработки. При этом приоритет должен отдаваться методам обеспечения функциональной безопасности и решению с их помощью задач информационной безопасности.

Стратегии обеспечения функциональной безопасности. Для обеспечения функциональной безопасности используются несколько подходов (стратегий): безотказность, отказоустойчивость и безопасное поведение при отказах [4]. В первом случае предлагается использовать высоконадежные элементы, во втором – различные методы резервирования и восстановления для обеспечения отказоустойчивости. То есть первые две стратегии направлены на общее повышение надежности (безотказности) и, как следствие, повышение безопасности за счет сохранения работоспособности системы и обеспечения ее правильной работы в различных ситуациях, в том числе ее устойчивости при воздействии внешних факторов. Однако такой подход ограничен надежностью используемой элементной базы и при текущем состоянии производства микроэлектронных компонентов и может использоваться при построении систем с уровнем полноты безопасности, не превышающем УПБ3. Для систем с УПБ4 такой подход не обеспечивает выполнение всех требований функциональной безопасности.

Третья стратегия является специфичной для систем ЖАТ и предполагает разделение неработоспособного состояния системы на два состояния: неработоспособное защитное (безопасное) и неработоспособное опасное. Для этой цели все функции, выполняемые системой, делятся на два класса: технологические функции, не связанные с обеспечением безопасности, и функции обеспечения безопасности. Если часть технологических функций по каким-либо причинам не может быть выполнена, но при этом все функции обеспечения безопасности выполняются в полном объеме, то система находится в защитном (безопасном) состоянии. При невыполнении хотя бы одной функции обеспечения безопасности система переходит в опасное состояние. Соответственно различают опасные и защитные отказы.

Опасный отказ системы ЖАТ может привести к возникновению аварии или крушению поезда, но в подавляющем большинстве случаев этого не происходит, поскольку причины возникновения аварии (крушения) также связаны с существующей в данный момент поездной ситуацией и действиями человека-оператора (машинист, дежурный по станции, поездной диспетчер, электромеханик и др.)

Исходя из этого отказ системы ЖАТ считается опасным, если нарушен критерий опасного отказа, даже если авария (крушение) при этом не произошла. Это позволяет рассматривать безопасность системы или отдельного её элемента как свойство объекта вне связи с ошибками человека или движением поездов. Диаграммы состояний объекта СЖАТ представлены на рисунке 1.

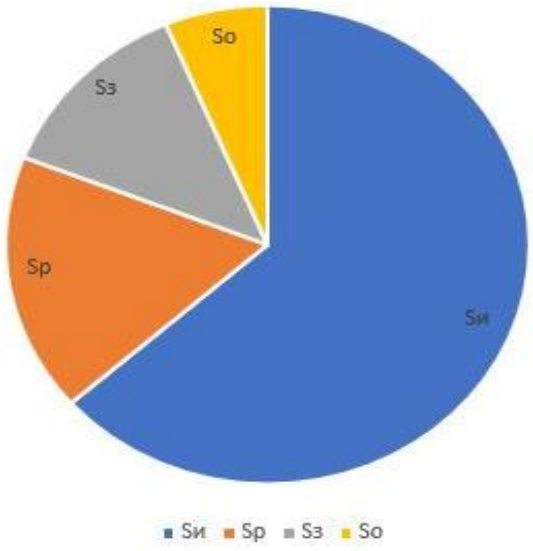

Рисунок 1 – Диаграмма состояний объекта СЖАТ:
$S_И$, $S_Р$, $S_З$, $S_О$ – подмножества исправных, работоспособных, защитных и опасных состояний соответственно

Безопасность системы ЖАТ при этом определяется как свойство системы непрерывно сохранять исправное, работоспособное или защитное состояние в течение некоторого времени или наработки.

Защитный отказ нарушает безотказность, но не нарушает безопасность. Опасный отказ нарушает и безотказность, и безопасность.

Безотказность характеризуется множеством состояний

$$S_Н = S_И \cup S_Р,$$

а безопасность – множеством состояний

$$S_Б = S_И \cup S_Р \cup S_З.$$

Критерии опасных отказов в обязательном порядке устанавливаются в соответствующей нормативной документации. Такой подход позволяет сконцентрироваться на относительно небольшом множестве функций и критических элементов и использовать достаточно сложные методы защиты.

Иерархия уровней защиты. Многообразие отказов и форм их проявления требует применения методов обеспечения безотказности и безопасности на различных функциональных уровнях микроэлектронных систем ЖАТ. На сегодняшний день наиболее перспективным для управления рисками считается принцип «Защита в глубину» (*defense-in-depth*), который заключается в том, что в системе должен применяться набор разнотипных методов защиты, с тем чтобы инцидент либо авария на объекте контроля и управления не могли пройти все уровни. Обычно выделяют пять уровней защиты: аппаратный (самый низкий), информационный, программный, структурный и уровень интерфейса (самый высокий) [5].

Такая иерархия обусловлена тем, что на каждом из этих уровней можно осуществлять мероприятия по защите от отказов, позволяющие компенсировать последствия отказов, возникающих на более низких уровнях. Например, использование парафазного кодирования на информационном уровне позволяет контролировать исправную работу самопроверяемых схем, использование на структурном уровне диверситетного программного обеспечения позволяет защититься от ошибок в программном обеспечении.

На практике далеко не всегда защита осуществляется на всех уровнях одновременно. Обязательным является применение структурных методов обеспечения безопасности и безопасного интерфейса с исполнительными объектами, то есть высших уровней защиты. Мероприятия по защите от опасных отказов на остальных уровнях применяются при необходимости повышения показателей функциональной безопасности.

На каждом из уровней защиты от опасных отказов могут использоваться различные подходы и стратегии обеспечения безопасности. Например, на информационном и программном уровнях наиболее часто применяют стратегию отказоустойчивости, а на аппаратном, структурном и уровне интерфейса – стратегию безопасного поведения при отказах. Кроме того, на одном уровне защиты могут использоваться несколько различных стратегий одновременно. Например, стратегия безопасного поведения может применяться совместно со стратегией отказоустойчивости. В этом случае, если при возникновении отказов система исчерпала резервные возможности и в результате деградации и реконфигурации перестала быть отказоустойчивой, то при появлении еще одного отказа она должна необратимо перейти в защитное состояние.

Такой подход обеспечивает многообразие путей решения проблемы обеспечения заданных показателей безопасности, но окончательный выбор всегда остается за разработчиком системы.

Возможность использования методов обеспечения функциональной безопасности для решения задач информационной безопасности. Для того чтобы сравнить эффективность применения методов функциональной безопасности для решения задач информационной безопасности, необходимо рассмотреть следующие элементы: поставленные цели, последствия (величина ущерба), объект защиты, угрозы безопасности.

В соответствии с Приказом ФСТЭК России № 31 от 14.03.2014 целью мер по обеспечению информационной безопасности, в первую очередь, является обеспечение доступности, целостности и конфиденциальности обрабатываемой в АСУ ТП информации. Таким образом, внимание концентрируется на защите информации с целью недопущения ее искажения (в том числе недоступности актуальной информации), которое может привести к нарушению функционирования АСУ ТП. Цели функциональной безопасности заключаются в отсутствии неприемлемого риска здоровью людей, их собственности или окружающей среде со стороны АСУ ТП при нарушении ее правильного функционирования [3]. Очевидно, что цели функциональной безопасности шире, так как в качестве причин нарушения функционирования АСУ ТП учитываются не только возможные искажения информации, но и отказы аппаратных средств, ошибки в программном обеспечении и др.

Если внимательно посмотреть на критерии значимости объектов КИИ и сравнить их с критериями ранжирования систем управления по функциональной безопасности, то можно сделать вывод, что требования функциональной безопасности гораздо жёстче, чем требования информационной безопасности. Так, ГОСТ 33433–2015 «Безопас-

ность функциональная. Управление рисками на железнодорожном транспорте» [6], устанавливающий типовые уровни тяжести последствий, относит к наивысшему, катастрофическому, уровню последствий аварийную ситуацию, повлекшую гибель одного или более людей. В то время как согласно Перечню показателей критериев значимости объектов критической информационной инфраструктуры, утвержденному постановлением Правительства РФ № 127 от 8 февраля 2018, если инцидент на объекте КИИ приведет к гибели от одного до пятидесяти человек, то такой объект относят к низшей (третьей) категории.

Объектами защиты в АСУ ТП с точки зрения как функциональной, так и информационной безопасности являются:

– технические средства;

– программное обеспечение;

– информация о параметрах или состоянии управляемого объекта или процесса.

Однако при рассмотрении вопросов информационной безопасности концентрируют внимание на конфиденциальности, доступности и целостности информации, а технические средства и программное обеспечение рассматривают только как источники уязвимостей, возможного искажения информации, временной недоступности или несанкционированного доступа к информации. При реализации мер по обеспечению функциональной безопасности в равной мере уделяют внимание как последствиям отказов технических средств, так и возможным ошибкам в программном обеспечении, в том числе приводящих к искажению критической информации.

Исходя из вышесказанного можно сделать вывод о том, что методы обеспечения функциональной безопасности позволяют достичь тех же целей, защищают те же объекты и требования к их реализации более жесткие по сравнению с аналогичными методами информационной безопасности.

Угрозы информационной и функциональной безопасности. Типичными угрозами информационной безопасности являются события, связанные с нарушением доступности и целостности обрабатываемой в АСУ ТП информации [7, 8].

1 Внешние угрозы:

– несанкционированный доступ;

– саботаж или намеренное причинение ущерба сторонними лицами;

– вредоносное ПО (вирусы);

– целевые атаки.

2 Внутренние угрозы:

– ошибки конфигурации оборудования;

– саботаж или намеренное причинение ущерба сотрудниками;

– уязвимости в индустриальном ПО и протоколах, в том числе недекларированные возможности.

Типичными угрозами функциональной безопасности являются [5]:

1 Внешние угрозы:

– случайные искажения информации в каналах связи;

– отказы внешней инфраструктуры.

2 Внутренние угрозы:

– отказы оборудования;

– случайные искажения внутренней информации;

– ошибки персонала (непреднамеренные действия);

– ошибки в программном обеспечении.

Сравнение типичных угроз информационной и функциональной безопасности позволяет сделать следующий вывод. Методы функциональной безопасности направлены в первую очередь на защиту от случайных событий (неумышленных действий), в то время как информационная безопасность сконцентрирована на защите от умышленных (преднамеренных) действий злоумышленников. В этом и заключается основное отличие в подходах. На первый взгляд это требует применения принципиально разных подходов, но более глубокий анализ показывает, что это далеко не так.

Обеспечение доступности, целостности и конфиденциальности информации методами функциональной безопасности. Рассмотрим более подробно угрозы информационной безопасности применительно к основной цели – обеспечению доступности, целостности и конфиденциальности информации.

Доступность – способность компонента выполнить требуемую функцию при заданных условиях в заданный момент времени или в течение заданного интервала времени, если предоставлены необходимые внешние ресурсы [9].

Целостность – свойство системы, отражающее логическую корректность и безотказность операционной системы, логическую полноту аппаратных средств и программного обеспечения, которые реализуют защитные механизмы, а также согласованность структуры и содержания хранимых данных [9].

Конфиденциальность – гарантия того, что информация не будет раскрыта несанкционированным лицам, процессам или устройствам [9].

Все рассмотренные выше угрозы при некоторых условиях могут нарушить доступность информации. При этом АСУ ТП перестанет получать актуальную информацию о состоянии объектов управления и контроля, что может стать потенциально опасным. Однако к таким последствиям могут привести также и случайные события, которые в обязательном порядке учитываются при разработке АСУ ТП в рамках обеспечения функциональной безопасности. Например, информация с рельсовых цепей участка железной дороги позволяет системе ЖАТ определить местоположение поезда и, в соответствии с этой информацией, включить соответствующую сигнализацию на проходных светофорах.

Парирование последствий возможного нарушения доступности информации можно выполнять по двум направлениям:

1) поддержание доступности информации при возникновении угроз. В этом случае решение сводится к задаче повышения общей надежности системы, которая решается резервированием;

2) сохранение безопасного состояния системы при отсутствии доступа к критической информации. В этом случае могут быть использованы методы функциональной безопасности, которые, например, применяются в системах обеспечения безопасности при обрыве линии связи с источником ответственной информации.

В этом случае выполняется ряд мероприятий, позволяющих исключить возникновение опасной ситуации:

– ограничение времени жизни (актуальности) критической информации. Если информация не обновилась за указанный период времени, то она автоматически заменяется на более безопасное значение. Например, для рельсовой цепи при потере связи принимается, что контролируемый участок пути занят поездом;

– ограничение времени жизни команд. Бистабильные команды, которые вызывают переключение объекта (например, команды включить / выключить лампу светофора) имеют ограниченное время жизни. Если время жизни команды истекло, то объект автоматически переключается в защитное состояние;

– контроль последовательности выполнения процедур в программном обеспечении, который гарантирует, что процедуры проверки актуальности информации / команд будут выполнены за указанный интервал времени;

– программный и аппаратный контроль тайм-аутов, исключающий сохранение активного состояния выходов в случае зависания вычислительных каналов.

Такая многоуровневая защита позволяет гарантировать переход в защитное состояние систем ЖАТ при любых нарушениях доступности критической информации. Таким образом можно сделать вывод, что методы обеспечения функциональной безопасности позволяют в полной мере решить задачи информационной безопасности по обеспечению доступности информации в АСУ ТП в том объеме, который позволит исключить опасное влияние таких угроз на работу АСУ ТП.

Нарушение целостности и конфиденциальности данных тоже нужно рассматривать по нескольким направлениям:

– случайное (непреднамеренное) искажение информации (в том числе конфигурационной);

– преднамеренное искажение информации посредством внешних систем передачи информации. Сюда можно отнести такие угрозы, как несанкционированный доступ, вредоносное ПО, целевые атаки, уязвимости в протоколах передачи данных;

– преднамеренное искажение информации посредством использования уязвимостей в ПО, в том числе недекларированных возможностей.

Случайное нарушение целостности информации (искажения, добавления или удаления) являются предметом функциональной безопасности. Концепция обеспечения безопасности, принятая разработчиками, должна исключать опасное влияние таких нарушений на безопасность системы в целом. Для этих целей разработан и успешно применяется ряд методов, таких как избыточное кодирование, дублирование с последующим сравнением, диверсификация способов кодирования и форматов хранения информации, защита с помощью контрольных сумм и т. д. [10].

Защита систем ЖАТ от преднамеренного нарушения целостности информации через внешние системы передачи информации осуществляется в соответствии с ГОСТ Р МЭК 62280 «Железные дороги. Системы связи, сигнализации и обработки данных. Требования к обеспечению безопасной передачи информации» [11]. В данном стандарте рассмотрены возможные угрозы нарушения целостности данных, такие как случайные отказы аппаратных средств, систематические отказы (ошибки) программного обеспечения, внешние физические воздействия и преднамеренные действия злоумышленника. Выделены основные типы нарушения целостности: повтор, удаление, вставка, переупорядочивание, повреждение (искажение), задержка и подмена сообщений.

В стандарте также определены необходимые меры для защиты от опасных последствий этих нарушений: использование меток времени в сообщениях, избыточных кодов и криптографических методов. Рассмотренные в стандарте угрозы и меры защиты охватывают все возможные угрозы информационной безопасности и являются достаточными для их нейтрализации.

Защита систем ЖАТ от систематических отказов (ошибок) программного обеспечения осуществляется в соответствии с ГОСТ Р МЭК 62279 «Железные дороги. Системы связи, сигнализации и обработки данных. Программное обеспечение систем управления и защиты на железных дорогах» [12]. Стандарт охватывает все этапы жизненного цикла программного обеспечения и регламентирует порядок разработки, документирования, верификации и внесения изменений в программное обеспечение. Рассмотрены вопросы организации разработки ПО, определены типовые роли, их компетенции, возможность совмещения разных ролей одним человеком. Рекомендован независимый аудит аккредитованной лабораторией на всех стадиях разработки, позволяющий обнаруживать ошибки на ранних этапах жизненного цикла.

В стандарте приведены методы, позволяющие получить программное обеспечение, соответствующее требованиям функциональной безопасности с УПБ4. Например, при разработке архитектуры ПО стандартом рекомендовано применять следующий набор методов: защищенное программирование, многовариантное (диверситетное) программирование, полностью определенный интерфейс, структурная методология, а также один из следующих методов: коды с обнаружением ошибок, программирование с проверкой ошибок, сохранение достигнутых состояний или моделирование.

Статический анализ кода, который является обязательным элементом верификации ПО, позволяет контролировать не только корректную реализацию спецификации, но и убедиться в отсутствии недекларируемых возможностей.

Таким образом, выполнение всех мероприятий по защите от систематических отказов по ГОСТ Р МЭК 62279 позволяет получить программное обеспечение, соответствующее не только требованиям функциональной безопасности, но и требованиям информационной безопасности.

Этапы жизненного цикла, связанные с функциональной и информационной безопасностью. Структура жизненного цикла определена стандартами по функциональной безопасности [13], которые рекомендуют использовать V-образный жизненный цикл. По нисходящей ветви жизненного цикла выполняется разработка системы, а по восходящей ветви – интеграция, сопровождаемая процедурами верификации и валидации на соответствие требованиям. Этапы жизненного цикла объекта железнодорожного транспорта представлены на рисунке 2.

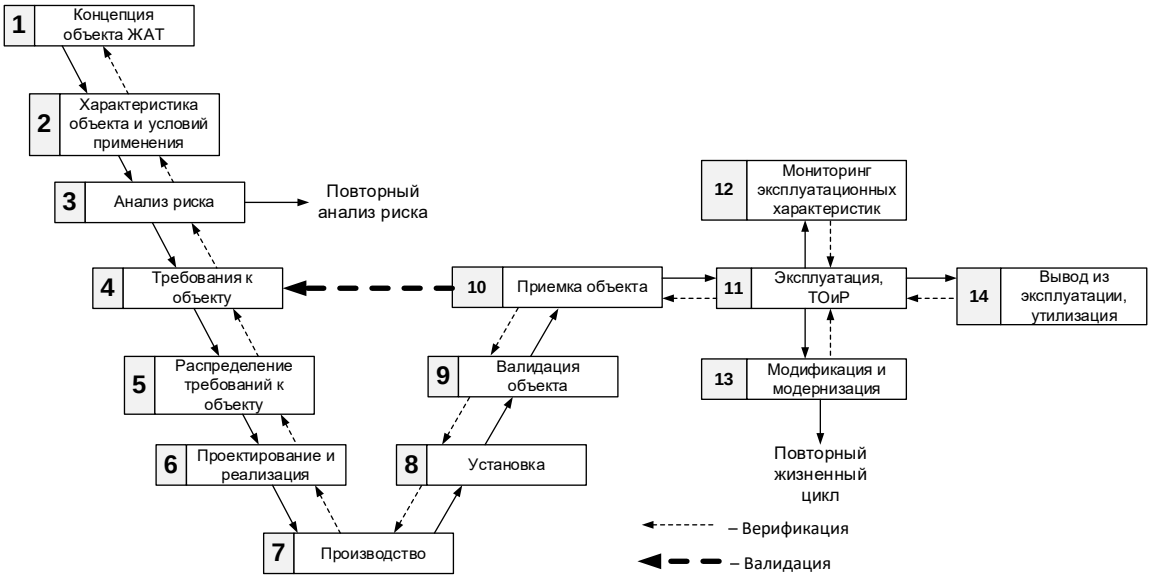

Рисунок 2 – Этапы жизненного цикла объекта железнодорожного транспорта

Согласно МЭК 61508 предметная область функциональной безопасности должна быть охвачена менеджментом функциональной безопасности. В свою очередь предметная область информационной безопасности в соответствии с МЭК 62443 должна быть охвачена менеджментом информационной безопасности.

Задачи, связанные с обеспечением информационной безопасности, можно интегрировать в жизненный цикл функциональной безопасности на ранних этапах разработки. Подробное описание такого подхода с перечнем задач функциональной и информационной безопасности, решаемых на каждом этапе жизненного цикла, приведено в [9, 14]. Взаимодействие функциональной и информационной безопасности в процессе реализации жизненного цикла представлено на рисунке 3.

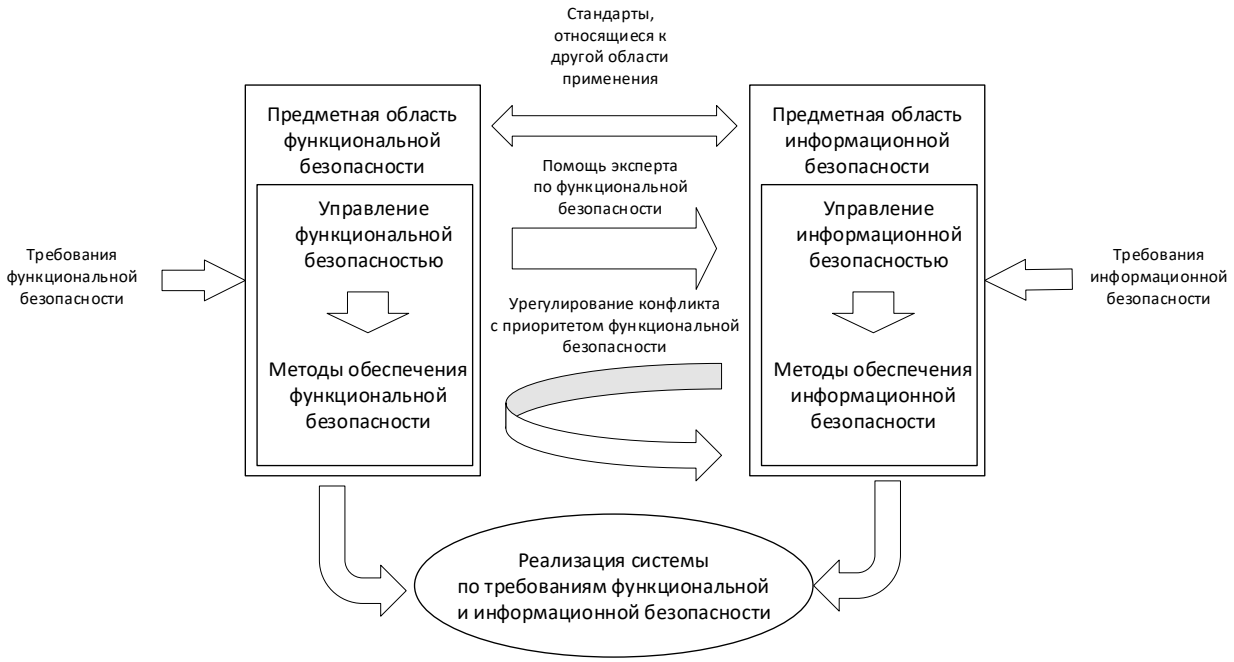

Рисунок 3 – Взаимодействие функциональной и информационной безопасности

На этих этапах разработчик должен привлекать специалистов в области как функциональной, так и информационной безопасности. При этом в случае возникновения конфликтной ситуации выполнение требований функциональной безопасности должно иметь приоритет над требованиями информационной безопасности [9].

При таком подходе при проектировании и реализации объекта ЖАТ будут в равной мере учтены требования как функциональной, так и информационной безопасности. Разработчик сможет применять наиболее эффективные методы на различных уровнях защиты, что позволит не только повысить уровень защищенности системы от выявленных опасностей, но и исключить дублирование средств защиты.

На этапах жизненного цикла, связанных с валидацией и приемкой объекта, возникает задача подтверждения соответствия требованиям функциональной и информационной безопасности. Учитывая глубокую интеграцию

методов защиты, реализованной на ранних этапах жизненного цикла, такие работы желательно проводить в одной испытательной лаборатории, аккредитованной в области как функциональной, так и информационной безопасности.

Выводы. Использование методов функциональной безопасности позволяет в полном объеме решить задачи информационной безопасности для систем ЖАТ. Для всех угроз информационной безопасности существуют эффективные методы защиты, базирующиеся на стандартах по функциональной безопасности.

Для эффективного использования методов функциональной безопасности в целях обеспечения информационной безопасности необходимо выполнять эту работу на ранних стадиях разработки АСУ ТП, начиная с технического задания. При этом для исключения дублирования работ подтверждение соответствия требованиям функциональной и информационной безопасности желательно проводить в одной организации, аккредитованной в этих областях.

Список литературы

1 О Концепции информационной безопасности Республики Беларусь [Электронный ресурс] : постановление Совета безопасности Респ. Беларусь, 18 марта 2019 г., № 1 // ЭТАЛОН Online. Законодательство Республики Беларусь / Нац. центр правовой информации Респ. Беларусь. – Минск, 2019.

2 **ТР ТС 003/2011.** Технический регламент Таможенного союза «О безопасности инфраструктуры железнодорожного транспорта» (в редакции Решения Совета Евразийской экономической комиссии от 14 сентября 2021 г. № 90). – Минск : БелГИСС, 2022. – 38 с.

3 **ГОСТ Р МЭК 61508-4–2012.** Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Ч. 4. Термины и определения. – М. : Стандартинформ, 2014. – 28 с.

4 **Бочков, К. А.** Микропроцессорные системы автоматики на железнодорожном транспорте : учеб. пособие / К. А. Бочков, А. Н. Коврига, С. Н. Харлап. – Гомель : БелГУТ, 2013. – 254 с.

5 **Харлап, С. Н.** Применение диверситета в автоматизированных системах управления опасными технологическими процессами для повышения устойчивости к систематическим отказам / С. Н. Харлап // Известия Транссиба. – 2020. – № 3 (43). – С. 148–157.

6 **ГОСТ 33433–2015.** Безопасность функциональная. Управление рисками на железнодорожном транспорте. – М. : Стандартинформ, 2016. – 36 с.

7 **Надеждин, Ю.** Безопасность АСУ ТП критически важных объектов / Ю. Надеждин [Электронный ресурс]. – Режим доступа : http://lib.secuteck.ru/articles2/security-director/bezopasnost-asu-tp-kriticheski- vazhnyh-obektov. – Дата доступа : 19.04.2022.

8 **Мальнев, А.** Противодействие реальным угрозам АСУ ТП / А. Мальнев // Information Security/ Информационная безопасность. – 2015. – № 4. – С. 26–28.

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

10 **ГОСТ IEC 61508-3–2018.** Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Ч. 3. Требования к программному обеспечению. – М. : Стандартинформ, 2014. – 107 с.

11 **ГОСТ Р МЭК 62280–2017.** Железные дороги. Системы связи, сигнализации и обработки данных. Требования к обеспечению безопасной передачи информации. – М. : Стандартинформ, 2017. – 49 с.

12 **ГОСТ Р МЭК 62279–2016.** Железные дороги. Системы связи, сигнализации и обработки данных. Программное обеспечение систем управления и защиты на железных дорогах. – М. : Стандартинформ, 2017. – 96 с.

13 **ГОСТ 33432–2015**. Безопасность функциональная. Политика, Программа обеспечения безопасности. Доказательство безопасности объектов железнодорожного транспорта. – М. : Стандартинформ, 2016. – 22 с.

14 **Скляр, В. В.** Обеспечение безопасности АСУ ТП в соответствии с современными стандартами : метод. пособие / В. В. Скляр. – М. : ИнфраИнженерия, 2018. – 384 с.

Получено 27.09.2022

K. A. Bochkov, S. N. Kharlap, A. N. Kovriga. Ensuring information security of microelectronic systems of automatics and telemechanics of railway in life cycle of functional safety.

Approaches to ensuring functional and information security within uniform life cycle of systems of railway automatics and telemechanics are considered. The possibility of use of methods of ensuring functional safety for the solution of problems of information security is proved. Examples of ensuring availability, integrity and confidentiality of information are given by methods of functional safety. Problems of functional and information security which have to be solved within uniform life cycle are formulated.