3 **Коновалов, Г. В.** Моделирование способов передачи сигналов времени при частотно-временном обеспечении телекоммуникаций / Г. В. Коновалов, Е. О. Новожилов // Молодые ученые – 2008 : материалы V Междунар. науч.-техн. школы-конф. Ч. 4. – М. : Энергоатомиздат, 2008. – С. 205–208.

4 **Васильев, Д. Н.** Опыт построения системы точного времени на сети оператора электросвязи / Д. Н. Васильев // Современные проблемы частотно-временного обеспечения сетей электросвязи : сб. тр. междунар. науч.-техн. конф. – М. : ФГУП ЦНИИС, 2010. – С. 206–219.

5 Передача времени по сети связи общего пользования / А. В. Рыжков [и др.] // Электросвязь. – 2010. – № 12. – С. 42–47.

6 **Рыжков, А. В.** Частота и время в телекоммуникациях XXI века / А. В. Рыжков. – М. : МАС, 2006.

УДК 656.25

ПРИМЕНЕНИЕ МЕТОДОВ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ ДЛЯ РЕШЕНИЯ ЗАДАЧ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЖАТ

К. А. БОЧКОВ, С. Н. ХАРЛАП
Белорусский государственный университет транспорта, г. Гомель

В настоящее время наблюдается активное использование информационных технологий в автоматизированных системах управления технологическими процессами (АСУ ТП). При этом возникла проблема взаимного влияния функциональной и информационной составляющих на безопасность таких систем, что отражено, в частности, в ГОСТ Р 59505-2021 / IEC TR 63069:2019 «Измерение, управление и автоматизация промышленного процесса. Основные принципы обеспечения функциональной безопасности и защиты информации». Особенно ярко эта проблема проявляется в автоматизированных системах управления ответственными технологическими процессами (АСУ ОПТ), типовым представителем которых являются микроэлектронные системы железнодорожной автоматики и телемеханики (ЖАТ), которые должны соответствовать самому высокому уровню полноты безопасности УПБ4 по ГОСТ Р МЭК 61508. Особенностью систем ЖАТ является то, что в первую очередь данные системы должны выполнять требования функциональной безопасности и только во вторую очередь все остальные требования, включая требования информационной безопасности. При этом методы и средства построения безопасных микроэлектронных систем ЖАТ могут успешно применяться и для решения новых задач, связанных с нарушением информационной безопасности.

Для того, чтобы оценить возможность 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 № 31 ФСТЭК России от 14.03.2014 целью мер по обеспечению информационной безопасности в первую очередь является обеспечение доступности и целостности обрабатываемой в АСУ ТП информации. Таким образом, основной упор делается на защиту информации с целью недопущения ее искажения, т. е. объектом защиты является сама информация. Цели функциональной безопасности заключаются в отсутствии неприемлемого риска здоровью людей, их собственности или окружающей среде со стороны АСУ ТП при нарушении ее правильного функционирования, т. е. объектом защиты являются функции безопасности, а именно возможность их выполнения в любой момент времени. При этом для таких систем вводятся понятия опасного и защитного состояний, а для опасных отказов формулируются критерии опасного отказа со статистическими показателями. 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.

Сравнение критериев значимости объектов в нормативных документах по информационной и функциональной безопасности позволяет сделать вывод, что требования функциональной безопасности гораздо жёстче, чем требования информационной безопасности. Так, например, ГОСТ 33433-2015 «Безопасность функциональная. Управление рисками на железнодорожном транспорте», относит к наивысшему, катастрофическому уровню последствий, аварийную ситу-

ацию, повлекшую гибель одного или более людей. В то время как согласно Перечню показателей критериев значимости объектов критической информационной инфраструктуры, утвержденному Постановлением Правительства РФ от 8 февраля 2018 № 127, если инцидент на объекте критической инфраструктуры приведет к гибели от одного до пятидесяти человек, то такой объект относят к низшей, третьей категории.

Объектами защиты в микроэлектронных системах ЖАТ как с точки зрения функциональной безопасности, так и с точки зрения информационной безопасности являются:

– технические средства;

– программное обеспечение;

– информация о параметрах или состоянии управляемого объекта или процесса.

Однако при рассмотрении вопросов информационной безопасности внимание концентрируют на конфиденциальности, доступности и целостности информации, а технические средства и программное обеспечение рассматривают только как источники 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 этого 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.

Сравнение типичных угроз информационной и функциональной безопасности позволяет сделать вывод о том, что 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.

Рассмотрим более подробно угрозы информационной безопасности применительно к основной цели – обеспечение конфиденциальности, доступности и целостности информации.

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

Доступность – способность компонента выполнять требуемую функцию при заданных условиях в заданный интервал времени, если предоставлены внешние ресурсы.

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.

Все рассмотренные угрозы информационной безопасности 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.

Парирование последствий нарушения доступности информации можно выполнять по двум направлениям:

1) сохранение доступности информации. В этом случае решение сводится к задаче повышения 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, ограничение времени жизни команд, контроль последовательности выполнения процедур в программном обеспечении, 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 микроэлектронных 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 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.

Защита микроэлектронных 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». 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». В стандарте приведены методы, позволяющие получить программное обеспечение, соответствующее требованиям функциональной безопасности с УПБ4.

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

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.

Таким образом, 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.