Гапанович В.А., Розенберг Е.Н., Шубинский И.Б.

НЕКОТОРЫЕ ПОЛОЖЕНИЯ ОТКАЗОБЕЗОПАСНОСТИ И КИБЕРЗАЩИЩЕННОСТИ СИСТЕМ УПРАВЛЕНИЯ

Приводятся определения опасного отказа и отказобезопасности, обсуждается взаимосвязь и принципиальные различия между функциональной надежностью и функциональной безопасностью, анализируются альтернативы обеспечения отказобезопасности систем управления.
Рассматриваются основные угрозы киберзащищенности, способы реализации кибератак, предлагается концепция обеспечения гарантированного уровня киберзащищенности системы управления.

Ключевые слова: *надежность, отказ, опасный отказ, функциональная безопасность, отказобезопасность, кибератака, киберпространство, киберзащищенность.*

1. Отказобезопасность

Согласно [1] «опасность – ситуация, потенциально оказывающая вред человеку». Это, конечно, относится не только к человеку, но и к ущербам, которые могут быть причинены материальным ценностям или окружающей среде. Не каждая опасность всегда переходит в угрозу. Для этого необходимо, чтобы случилось инициирующее событие. Потом из угрозы может развиваться цепочка нежелательных событий, которая, в конечном счете, сведет к опасному событию, к аварии. Опасное состояние (событие) – это неисправное состояние объектов информационной системы, при котором возникают превышающие допустимые уровни риски причинения вреда жизни и здоровью граждан, имуществу физических и юридических лиц, государственному и муниципальному имуществу, окружающей среде, жизни и здоровью животных и растений.

Итак, безопасность – отсутствие неприемлемого риска. Риск – это комбинация ущерба и вероятности возникновения [2]. В зависимости от последствий можно отдельно рассматривать:

а) функциональную надежность системы, если она выполняет свою функцию (т.е. не теряет определенных свойств) в цепочке всех тех систем, которые участвуют в реализации данной функции;

б) функциональную безопасность, если последствия не сведут к неприемлемым рискам.

Рис. 1 показывает, что со стороны последствий функциональная надежность плавно переходит в функциональную безопасность, если критичность последствий возрастает. Отсюда и понятно, что информационные системы управления, у которых интенсивность отказов в выполнении функ-

ции должна быть не выше 10^{-6} 1 / час, можно толковать с позиций функциональной безопасности [3]. Такие системы часто называют потенциально опасными системами. Для них *опасный отказ* определяется как событие, в результате которого система переходит из исправного, работоспособного или частично работоспособного в опасное состояние.

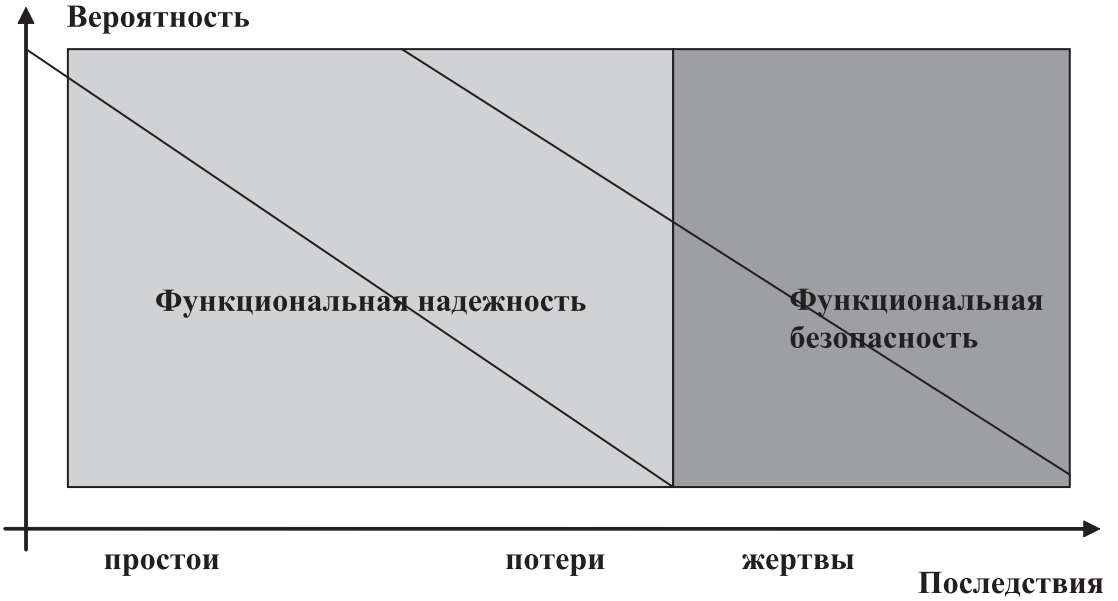

Рис. 1. Функциональная надежность и функциональная безопасность

Отказобезопасность – способность системы управления сохранять безопасное состояние и (или) обеспечивать безопасность управления подчиненными объектами в случае опасных отказов самой системы или ее составных частей.

Проблема обеспечения функциональной безопасности систем управления состоит в исключении влияния их отказов и ошибок в функционировании на объекты управления и окружающую среду, т.е. в исключении так называемых опасных отказов (рис. 2). В результате выдачи неправильных команд управления возможны столкновения поездов, разгерметизация цистерн, пожары, взрывы и т.д. В итоге возникают экономические и экологические ущербы, человеческие жертвы и даже катастрофы.

Полностью исключить влияние отказов и ошибок систем на окружающую среду принципиально невозможно – всегда существует некоторая вероятность возникновения подобных событий. Задача заключается в достижении минимально допустимых значений этих вероятностей. Одним из ключевых направлений в достижении этих целей остается обеспечение высокого уровня надежности систем. Однако возможности резкого повышения надежности известными технологическими, алгоритмическими, структурными и др. методами ограничены, главным образом из-за неприемлемых экономических потерь.

С позиций безопасности не может быть другой альтернативы кроме как прекратить функционирование системы или понизить до предусмотренных пределов ее производительность при недопустимой вероятности возникновения в ней опасного отказа. Отсюда следует необходимость создания технологий гарантированного и достоверного обнаружения отказов в системах. Если правильно реализована технология обеспечения функциональной безопасности, то обеспечивается своевременное обнаружение и блокирование опасных состояний системы.

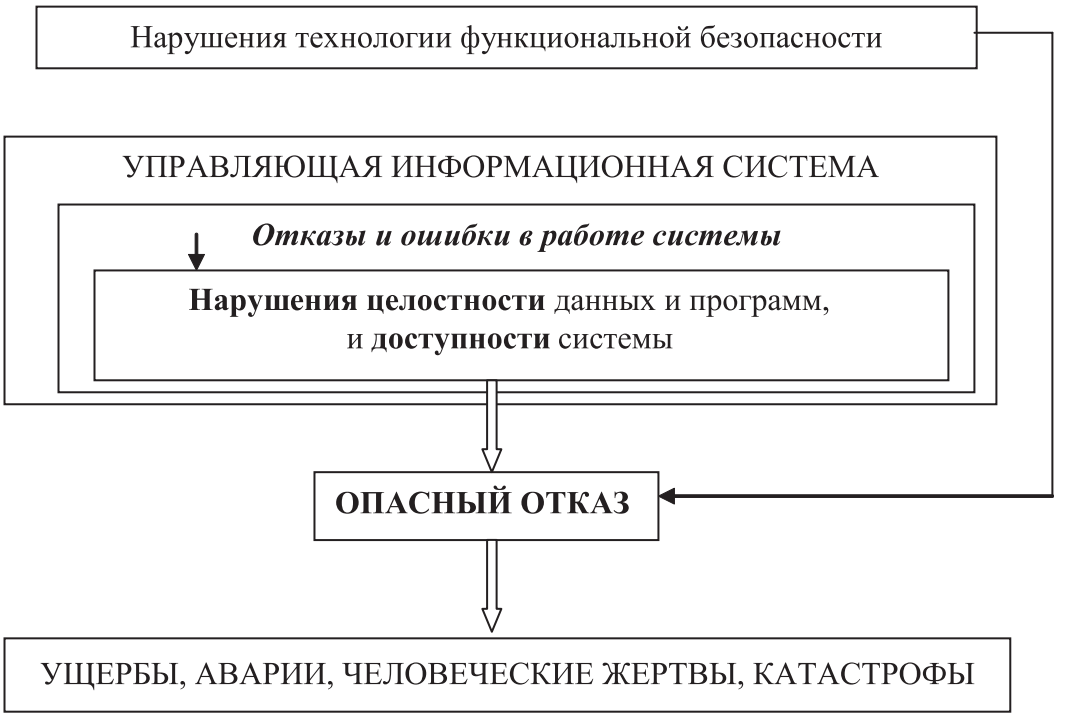

Рис. 2. Угрозы безопасности в управляющих информационных системах

Высокая эффективность обнаружения опасных состояний в ИС достигается с помощью технологий обнаружения отказов, основанных на построении двух, трех и более параллельных каналов управления. Параллельное формирование и сравнение выдаваемых команд управления обеспечивает уверенность в обнаружении опасных состояний при условии построения безопасных алгоритмов или устройств сравнения (так называемых компараторов), обеспечения независимости каналов и данных, несимметричности отказов каналов и при выполнении целого ряда других условий. Вместе с тем, для реализации указанной технологии обнаружения отказов дополнительно требуется включение в состав системы значительного объема аппаратных и программных средств, что приводит к снижению ее надежности.

Из указанных положений следует:

– между содержанием безопасности и надежности систем имеют место принципиальные различия – если ненадежность приводит к неприемлемым уровням готовности, технического использования, безотказности и стоимости технического обслуживания, то недостаточная безопасность приводит к авариям и человеческим жертвам;

– между целями обеспечения надежности и функциональной безопасности систем существуют противоречия, устранение которых возможно на основе компромисса, требования к надежности и функциональной безопасности должны быть между собой сбалансированы;

– в критически важных, потенциально опасных объектах, или объектах, представляющих повышенную опасность, приоритеты отдаются задачам обеспечения безопасности, а требуемые уровни надежности должны задаваться с учетом ограничений по стоимости после выполнения требований по безопасности.

Для обеспечения отказобезопасности систем нужно проделать тот же путь, что и для обеспечения отказоустойчивости, т.е. создать условия для наблюдаемости и управляемости системы. На основе принципа приемлемости остаточного риска при имеющихся ограничениях в затратах средств необходимо в полной мере реализовать возможности по обеспечению отказоустойчивости и функциональной безопасности.

2. Киберзащищенность

Проблема обеспечения отказобезопасности в системах управления неразрывно связана с вопросами обеспечения их информационной защищенности, в первую очередь, от кибератак. Термин *кибер* определяется как «имеющий отношение к информационным технологиям» [4]. Информационные технологии реализуются в так называемом *киберпространстве*, под которым понимается «среда, созданная при помощи физических и не физических компонентов, характеризуемая использованием компьютеров и электромагнитного диапазона для хранения, изменения и обмена данными при помощи компьютерных сетей» [4]. Использование кибернетических возможностей, с целью достижения задач в киберпространстве или при помощи использования киберпространства определяется как «кибероперация». Теперь мы вплотную подошли к определению понятия *кибератака* – это кибероперация как наступательная, так и оборонительная, которая приводит к телесным повреждениям или человеческим потерям, или нанесению ущерба, или разрушению объектов.

Опираясь на приведенные выше понятия, можно определить **киберзащищенность, как способность системы управления успешно выполнять предусмотренные задачи при сохранении безопасного состояния в условиях кибератак, направленных на нанесение ущерба критически важным или потенциально опасным объектам, или объектам, представляющим повышенную опасность для жизни и здоровья граждан, имуществу физических или юридических лиц, экономике, окружающей среде.**

Основными угрозами нарушения киберзащищенности в информационно-управляющих системах являются (рис. 3):

- Информационные атаки (в первую очередь кибератаки);
- Недекларированные возможности в программах и устройствах систем;
- Отказы и ошибки в работе систем, в том числе аппаратные и программные сбои и ошибки, ошибки операторов, ошибки данных.

На рис. 2. показано, что киберзащищенность системы зависит как от возможностей несанкционированного доступа к системе (НСД) вероятного противника, так и от недекларированных возможностей (НДВ), которые имеют место в программных и аппаратных средствах. Несанкционированный доступ реализуется путем информационных атак (кибератак) на систему.

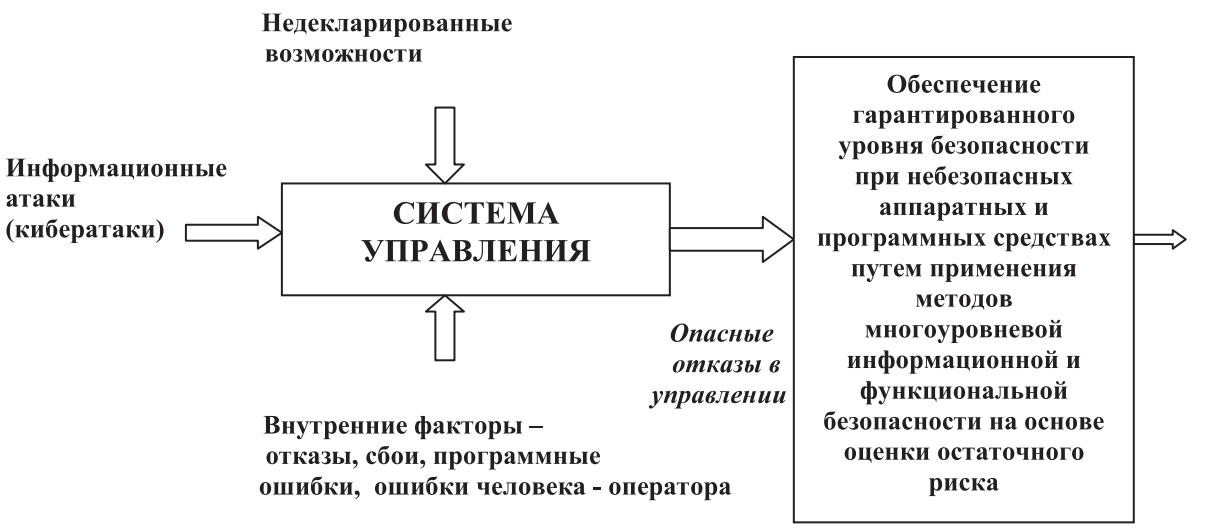

Рис. 3. Концепция обеспечения гарантированного уровня киберзащищенности системы управления

Полное устранение опасных отказов в управлении теоретически возможно, но практически неосуществимо, поскольку потребует экономических затрат, заведомо больших, чем ожидаемый ущерб от воздействия опасных отказов. Реальный путь – это определение допустимого уровня риска от кибератак и создание эффективной защиты от опасных отказов.

Рассмотрим более подробно перечисленные угрозы.

Результатом успешной кибератаки может стать нарушение целостности или доступности информации. В качестве целей атаки могут рассматриваться серверы, рабочие станции пользователей или коммуникационное оборудование информационной системы. При организации кибератак злоумышленники часто используют специализированное ПО, позволяющее автоматизировать действия, выполняемые на различных стадиях атаки.

В общем случае в любой кибератаке можно выделить четыре стадии:

Рекогносцировка. На этой стадии нарушитель старается получить как можно больше информации об объекте атаки, чтобы на ее основе спланировать дальнейшие этапы вторжения. Этим целям может служить, например, информация о типе и версии операционной системы; список пользователей, зарегистрированных в системе; сведения об используемом прикладном ПО и т.д.

Вторжение. На этом этапе нарушитель получает несанкционированный доступ к тем ресурсам, на которые совершается атака.

Атакующее воздействие. На данной стадии реализуются те цели, ради которых и предпринималась атака, – например, нарушение работоспособности системы, удаление или модификация данных и т.д. При этом атакующий часто выполняет операции, направленные на удаление следов его присутствия в системе. Всякая атака основана на наличии в системе управления уязвимостей и «правильное» использование хотя бы одной из них открывает злоумышленнику вход в систему.

Развитие атаки. После атакующего воздействия нарушитель стремится перевести атаку в фазу дальнейшего развития. Для этого в систему обычно внедряется вредоносная программа, с помощью которой можно организовать атаку на другие средства системы. Основные угрозы киберзащищенности информационным системам (ИС) создают следующие группы вредоносных программ: ***DoS-атака*** (от англ. Denial of Service, отказ в обслуживании) – атака на информационную систему, с целью довести её до отказа, то есть создание таких условий, при которых легитимные (правомерные) пользователи системы не могут получить доступ к предоставляемым системой ресурсам (серверам), либо этот доступ затруднён. Отказ «вражеской» системы может быть одним из шагов к овладению системой (если во внештатной ситуации ПО выдаёт какую-либо критическую информацию – например, версию, часть программного кода и т. д.); ***троянские программы –*** после внедрения в систему нарушают целостность данных и программ или рассаживают вирусы в системе. Они также могут собрать сведения о хранящихся на компьютере профилях пользователей, паролях и другую конфиденциальную информацию и затем переслать ее в руки злоумышленников; ***программы несанкционированного управления компьютерами ИС (****загрузочные вирусы, программные вирусы, сетевые черви и др.)*

Недекларированные возможности – функциональные возможности программных или аппаратных средств, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение доступности, целостности, а также конфиденциальности обрабатываемой информации. Реализацией недекларированных возможностей, в частности, являются программные или аппаратные закладки.

В результате реализации указанных угроз возникают опасные отказы, которые приводят к недопустимым ущербам объектам, которые для хозяйствующего субъекта относятся к категории объектов с повышенной опасностью или к категории потенциально опасных объектов, а на уровне

государственных или региональных органов опасные отказы могут приводить к недопустимым ущербам критически важных объектов. Последнее обстоятельство объясняется тем, что ответственность за защиту критически важных объектов возлагается на государственные или региональные органы.

Угрозы нарушения киберзащищенности систем управления аналогичны угрозам нарушения отказобезопасности. Принципиальное различие в том, что кибератаки – это специфический класс информационных атак, направленный на нанесение ущерба или разрушение объекта управления, который относится к одной из отмеченных выше трех групп важных объектов.

В вопросах обеспечения киберзащищенности, также как и в вопросах обеспечения отказоустойчивости и отказобезопасности, целесообразно опираться на следующие основные **постулаты***:*

1. Не существует абсолютной киберзащищенности (отказоустойчивости, отказобезопасности) систем управления.

2. Чем более сложная система, чем больше задач она выполняет, тем ниже ее киберзащищенность.

3. Необходимым условием повышения киберзащищенности системы является введение избыточности в сочетании с организацией эффективного контроля.

4. Киберзащищенность системы управления должна обеспечиваться на всех этапах жизненного цикла.

5. Уровень киберзащищенности системы ограничен экономическими рисками заказчика и эксплуатирующей организации.

Абсолютной киберзащищенности невозможно достичь, поскольку устранение одних уязвимостей в системе не исключает возможности появления новых. Проблема обеспечения киберзащищенности – это проблема совершенствования щита от нападения меча. Одновременно с повышением уровня защиты совершенствуются средства нападения и не факт, что эффективность средств защиты в определенные отрезки времени сколь угодно выше эффективности средств нападения.

Кардинальное решение задачи состоит в том, чтобы обеспечить **гарантированный уровень киберзащищенности при небезопасных аппаратных и программных средствах путем применения многоуровневой информационной и функциональной системы защиты на основе оценки остаточного риска** (рис. 3).

Примерами реализации принципов многоуровневой безопасности на железнодорожном транспорте могут быть [5]:

● ***многоуровневое обеспечение безопасности каждого автономного устройства управления.*** Пусть в этом программно-аппаратном устройстве предусматривается *несколько* функций безопасности. Одна или одновременно несколько функций безопасности в случае возникновения отказа выполняют задачу перевода устройства в неопасное состояние, – это могут быть состояния допустимых пониженных функциональных возможностей или защитные состояния, когда блокируется выдача управляющих воздействий;

● ***многоканальная безопасная многоуровневая система (МС) из разнотипных устройств или систем.*** Суть в том, что два или более устройств (систем) управления выполняют на определенном участке дороги аналогичные функции управления, которые реализуются разными способами и алгоритмами. Результаты каждого управления проверяются на непротиворечивость. Если это условие выполняется, то осуществляется управление. В противном случае осуществляется дополнительная проверка и принимается решение о введении защитного отказа одного из устройств или о продолжении его работы в составе МС, но с пониженной производительностью. Если в произвольный момент времени функции управления не противоречивы, то МС продолжает выполнять функции управления с заданной производительностью.

● ***система с выбором более запрещающего сигнала.*** В многоуровневую систему вводится устройство принятия решения, которое реализует следующее правило: если функции управления не противоречивы, но не совпадают по уровням градации опасности управления, то выбирается менее опасное управление. Например, если на выходе первого устройства железнодорожной автоматики и телемеханики сформировано управление светофором *«красный»*, а на выходе второго устройства – «*красно-желтый*», то на выходе системы формируется сигнал управления светофором *«красный»*.

● ***создание системных функций безопасности в развивающихся многоуровневых системах.*** Развивающаяся многоуровневая система – это система, которая обладает возможностями и способностями формировать новые свойства управления и/или новые функции безопасности. В дальнейшем будем рассматривать развивающуюся систему, которая формирует только новые функции безопасности. Суть принципа в следующем: в системе вместе с устройством принятия решения (или вместо него) вводится подсистема поддержки принятия решения (ППР). Кроме того, для каждого составного устройства или составной системы железнодорожной автоматики и телемеханики вводится дополнительный логический контроль состояний безопасности, который осуществляется путем запоминания, анализа, корреляции с указаниями составных устройств логических последовательностей смены состояний напольного оборудования автоматики и телемеханики. Путем совместной обработки в ППР команд управления с выходов этих устройств или систем и данных логического контроля формируются их дополнительные функции безопасности.

3. Заключение

Для обеспечения отказобезопасности систем управления нужно создать условия для наблюдаемости и управляемости системы.

На основе принципа приемлемости остаточного риска при имеющихся ограничениях в затратах средств необходимо в полной мере реализовать возможности по обеспечению отказоустойчивости и функциональной безопасности.

Для обеспечения киберзащищенности системы управления целесообразно комплексно реализовать меры по обеспечению информационной защищенности, надежности, и, особенно, функциональной безопасности. Кардинальное решение задачи состоит в том, чтобы обеспечить гарантированный уровень киберзащищенности при небезопасных аппаратных и программных средствах путем применения многоуровневой информационной и функциональной безопасности на основе оценки остаточного риска.

Литература

1. ИСО 9126 ГОСТ Р ИСО/МЭК 9126-93, Оценка программной продукции, характеристика качества и руководства по их применению, 28.12.93

2. ГОСТ Р/МЭК 61508. Функциональная безопасность электрических/ электронных/ программируемых электронных систем безопасности. – 2010.

3. **Шубинский И.Б., Шебе Х.** О понятии функциональной надежности. – Надежность, – 2012, № 4, – С. 74-84.

4. Таллиннский справочник по международному праву, применимому к кибернетическим способам ведения военных действий. – 2013.

5. **Rozenberg E.N, Shubinskiy I.B.** Functional Safety of RailwayAutomation Systems: Methods and Models. Moscow: VNIIAS MPS UIC, 2005.- 155 p.