Автоматика, связь, информатика, № , 2006,
. (не опубликована! Находится в редакции журнала)

О нормировании безопасности информационно-управляющих систем

ктн Белов В.П., дтн Голяков А.Д., кфмн Талалаев Д.В.

Современный этап развития информационно-управляющих систем (ИУС), способных при функционировании нанести вред здоровью людей, причинить ущерб окружающей природной среде и привести к материальным потерям, характеризуется, как правило, жёсткими требованиями, которые предъявляются к их безопасности. При этом сами механизмы выставления тех или иных требований не имеют жесткой нормативной базы.

На наш взгляд такая ситуация обусловлена наличием двух основных проблем. Первой проблемой является отсутствие до настоящего времени научно обоснованного понятийного аппарата, обеспечивающего чёткое и однозначное понимание некоторых применяемых в теории безопасности терминов. Наиболее остро эта проблема проявляется при использовании расплывчатых понятий и терминов, которые, тем не менее, имеют вполне легальные место в законах и различного рода нормативных правовых актах, и обладают обязательной силой. Практическое применение нечётких понятий приводит не только к юридическим ошибкам. Значимость терминологической базы в области безопасности нельзя переоценить: ошибки в понимании и применении основного термина «безопасность» приводят к неправильному построению системы, что в свою очередь грозит авариями и катастрофами, которые можно было избежать, либо неоправданными материальными потерями, связанными с потребностью разработки сложных и дорогостоящих систем защиты и значительно превышающих реальную необходимость.

Вторая проблема обусловлена необходимостью нормирования безопасности, т.е. научно обоснованного установления в нормативно-технической документации количественных и качественных требований к безопасности ИУС на основе согласованных подходов и правил. Анализ действующих в настоящее время законов и других нормативно-правовых актов РФ показывает, что в большинстве случаев в определении термина «безопасность» применяется понятие типа «безопасность – это состояние защищённости какой-либо системы от совокупности тех или иных угроз». Поскольку сущность понятия «состояние защищённости» не раскрыта ни в одном известном докумен-

те или словаре, смысловые границы термина «безопасность», как нам представляется, достаточно размыты и не имеют однозначный и чётко определённый характер.

В соответствии с теорией терминологии родовым словом в определении термина «безопасность» большинства дефиниций является «состояние». Как известно, состояние системы – это способ её существования, характеризующийся определёнными значениями переменных параметров (параметров состояния). Любая система может находиться в одном из двух (трёх, четырёх и т.д.) состояниях. Переход системы из одного состояния в другое состояние происходит в результате некоторого события. Причём о наступлении события судят на основании принятого критерия.

Если базироваться на этих общепризнанных положениях и полагать, что безопасность – это состояние, то при решении практических задач разработки ИУС, в том числе и задач нормирования безопасности, естественно возникают следующие вопросы: каким образом формируется перечень параметров этого состояния; как называется противоположное состояние; какие принципы используются при установлении критериев наступления опасного события; как называется способность системы сохранять безопасность (т.е. состояние защищённости) в течение некоторого времени? Поиск ответов на эти вопросы в отечественной нормативно-правовой литературе не дал положительных результатов.

В тоже время ответы на такие и подобные им вопросы могут быть получены при реализации методологического подхода, в основе которого лежит утверждение, что безопасность – это не состояние, а свойство [1 - 3], присущее системе, которая состоит из двух взаимодействующих подсистем: объекта и субъекта безопасности. При этом под объектом безопасности понимается подсистема, которая обладает определёнными «привлекательными» (для субъекта безопасности) свойствами, нуждающимися в защите. Субъектом безопасности является подсистема, которая имеет способность к уничтожению (или завладению) не принадлежащих ей «привлекательных» свойств. Кроме того, объект безопасности имеет способность препятствовать уничтожению «привлекательных» свойств.

При изучении свойства безопасности эти подсистемы должны быть однозначно определены и не могут рассматриваться без взаимодействия между собой, в отрыве друг от друга. Результатом их взаимодействия является ущерб, который наносит субъект безопасности объекту безопасности. В том случае, когда наносимый объекту безопасности ущерб не превышает приемлемого значения, система находится в безопасном состоянии. В момент превышения ущерба приемлемого значения происходит опасное

событие – происшествие. При возникновении происшествия система переходит в опасное (небезопасное) состояние.

Способность субъекта безопасности наносить ущерб и способность объекта безопасности препятствовать нанесению ущерба зависят от пространственных и временных факторов. При таком подходе под **безопасностью понимается свойство системы сохранять безопасное состояние в течение заданного времени и в определённой области пространства.**

Поскольку способность к сохранению безопасного состояния системы определяется рядом факторов, многие из которых носят случайный характер, для количественного оценивания безопасности используются, как правило, стохастические показатели. Выбор этих показателей производится в общем случае с помощью многомерной пространственно-временной функции распределения или условной функции распределения времени наступления опасного события в установленной заданными границами области пространства. Причём в задачах нормирования безопасности системы, в которой объектом безопасности является человек, а субъектом безопасности – техногенно-производственная подсистема (техника, материалы, вещества и т.п.)[1], в качестве аргумента этих функций наибольшее распространение в настоящее время получил интервал времени, равный одному году, а в качестве происшествия – гибель человека. Возможность гибели одного человека называется индивидуальным риском. Одним из показателей индивидуального риска является вероятность гибели человека в течение года.

Наряду с функциями распределения при нормировании функциональной безопасности применяются также плотности распределения вероятностей. В этом случае показателем индивидуального риска является значение плотности распределения вероятностей, которое представляет собой частоту гибели человека за рассматриваемый промежуток времени.

Если в виде объекта безопасности выступает группа людей (более 5 – 10 человек), то при анализе безопасности системы рассматриваются, как правило, два возможных происшествия, связанных с безвозвратными людскими потерями: гибель одного человека и гибель группы людей. При этом возможность гибели группы людей получила название социального (группового) риска.

[1] В отечественных и международных документах безопасность такой системы получила название «функциональной безопасности».

Любое происшествие возникает только при появлении определённого события, называемого угрозой безопасному состоянию рассматриваемой системы[1], т.е. угроза – это предвестник опасного события [4], внешняя форма её существования [2]. Угроза безопасному состоянию системы (угроза безопасности) исходит от субъекта безопасности при его функционировании (источника опасности). Она возникает, например, при выходе определённых (критических) параметров за установленные границы, при наличии ошибок операторов, отказов критичных элементов, ошибок в программном обеспечении субъекта безопасности и т.п. Перечень этих параметров, критичных элементов и ошибок устанавливается для всей совокупности возможных угроз, которая формируется при обосновании технического задания и уточняется в процессе сертификации конкретной ИУС (источника опасности), исходя из анализа процесса её функционирования, этапа жизненного цикла, условий эксплуатации и квалификации обслуживающего персонала. Угрозы характеризуют субъект безопасности и различаются по частоте появления, своими возможными последствиями, мотивам и другим признакам.

При наличии угрозы опасное событие может произойти или не произойти. В качестве препятствия на пути угрозы стоят меры (способы, средства) защиты объекта безопасности. Благодаря средствам защиты (при условии их работоспособности в момент появления угрозы и способности к её идентификации), ИУС переводится в защитное, как правило, неработоспособное состояние. В этом состоянии вероятность происшествия, связанного с гибелью человека или группы людей, становится пренебрежимо малой величиной. Заметим, что конкретная ИУС не всегда может быть отнесена только к субъекту или только к объекту безопасности. Наличие управляющих функций может являться источником угроз, в то же время, наличие контрольных и защитных механизмов, безусловно, характеризует способность предотвращать угрозы со стороны субъекта безопасности. В этой связи рассмотрение безопасности в комплексе, а именно полноценной взаимодействующей субъект-объектной пары является принципиально необходимым условием при решении конкретных практических задач.

Кроме того, развитию процесса перехода угрозы в происшествие могут способствовать или противодействовать внешние факторы среды, в которой функционирует система (температура, влажность, шум и т.п.), а также действия (или бездействия) обслуживающего персонала. Поэтому на практике при разработке и сертификации ИУС, например, систем железнодорожной автоматики и телемеханики [5], широкое распро-

[1] Вместо термина «угроза» иногда используется термин «опасности» (причём, как правило, во множественном числе), который, по нашему мнению, вводит дополнительную путаницу в терминологической базе теории безопасности.

странение получили способы анализа безопасности, основанные на сценарном подходе, построении деревьев событий и т.п.

Расчёт оценки истинного значения вероятности наступления опасного события в определённой точке (области) пространства в течение заданного времени производится по правилам сложения и умножения вероятностей. Например, вероятность гибели человека при возникновении i-ой угрозы в некоторой точке (области) пространства в течение времени t находится из выражения

$$R_i(t) = P(A_i \cdot B_i \cdot C_i \cdot D_i, t) = P(A_i, t) \cdot P(B_i / A_i, t) \cdot P(C_i / B_i \cdot A_i, t) \cdot P(D_i / C_i \cdot B_i \cdot A_i, t),$$

где $P(A_i, t)$ - вероятность возникновения угрозы жизни человека в течение времени t;

$P(B_i / A_i, t)$ - условная вероятность того, что средства защиты не смогли противостоять угрозе A_i (в частности, вероятность отказа средства защиты от i-ой угрозы);

$P(C_i / B_i \cdot A_i, t)$ - условная вероятность присутствия человека в данной точке (области) пространства при появлении угрозы (A_i) и отказе средства защиты от i-ой угрозы (B_i);

$P(D_i / C_i \cdot B_i \cdot A_i, t)$ - условная вероятность гибели человека при условии его присутствия в данной точке (области) пространства (C_i) при появлении угрозы (A_i) и отказе средства защиты от i-ой угрозы (B_i).

Приведённое выражение может быть дополнено рядом сомножителей, в частности условными вероятностями наличия неблагоприятных факторов, которые способствуют развитию процесса, приводящему к фатальному исходу.

В большинстве случаев все события, представляющие собой пересечение событий $A_i \cdot B_i \cdot C_i \cdot D_i$ $(i = \overline{1,k})$, где k - количество угроз жизни человека, являются несовместными событиями, поскольку человек может погибнуть только один раз и, как правило, при возникновении одной угрозы. Поэтому вероятность гибели человека от k угроз определяется путём суммирования вероятностей $R_i(t)$, т.е.

$$R(t) = \sum_{i=1}^{k} R_i(t).$$

При необходимости анализа аварийных ситуаций, возникающих при совместном появлении двух и более угроз, применяется способ комплексирования каждой возможной совокупности угроз в отдельную самостоятельную угрозу. В результате этого увеличивается общее количество угроз безопасному состоянию системы при сохранении методики расчёта искомого показателя безопасности.

При использовании нескольких барьеров защиты, которые функционируют независимо друг от друга, условная вероятность $P(B_i / A_i, t)$ определяется в виде произведения вероятностей:

$$P(B_i / A_i, t) = \prod_{j=1}^{N_i} P_j(B_i / A_i, t),$$

где $P_j(B_i / A_i, t)$ - условная вероятность того, что j-ый барьер средства защиты не смог противостоять i-ой угрозе;

N_i – количество барьеров средства защиты от i-ой угрозы.

В качестве показателя индивидуального риска используется также частота гибели человека от i-ой угрозы, которая рассчитывается по формуле

$$f_{R_i}(t) = \sum_{i=1}^{k} P(A_i, t) \cdot f(B_i / A_i, t) \cdot P(C_i / B_i \cdot A_i, t) \cdot P(D_i / C_i \cdot B_i \cdot A_i, t),$$

где $f(B_i / A_i, t)$ - условная частота события, заключающегося в отсутствии способности средства защиты противостоять i-ой угрозе гибели человека, которая появилась в момент времени t.

Анализ отечественных и международных документов, посвящённых нормированию безопасности [6 - 10], свидетельствует о том, что приемлемое значение вероятности гибели одного человека в течение года (приемлемый индивидуальный риск[1]) находится в диапазоне ($10^{-5} \div 10^{-6}$). При этом значение вероятности 10^{-6} иногда называют желаемым (верхним) уровнем индивидуального риска, а значение вероятности 10^{-5} – допустимым (нижним) уровнем индивидуального риска.

Поэтому полагается, что система, у которой индивидуальный риск меньше 10^{-6} (или при использовании условной плотности распределения времени наступления происшествия в некоторой заданной области пространства при t = 1 год меньше 10^{-6} 1/год), является безопасной, и не требуются дополнительные мероприятия по снижению этой вероятности. Если индивидуальный риск системы больше 10^{-5}, то её использование по назначению является недопустимым, несмотря на получаемые при этом социально-экономические или другие выгоды[2].

Для обоснования требований к средствам защиты от угроз, обусловленных отказом оборудования или ошибками в программном обеспечении систем управления объектами повышенной опасности, в стандарте Международной электротехнической ко-

---

[1] Под приемлемым риском понимается такой риск, на который общество готово пойти ради выгод, получаемых от эксплуатации субъекта безопасности [6].

[2] В ряде случаев индивидуальный риск разделяется на две группы: индивидуальный риск населения и индивидуальный риск обслуживающего персонала. При этом допустимый уровень индивидуального риска обслуживающего персонала устанавливается, как правило, равным 10^{-4} в год.

миссии (IEC) МЭК 61508 «Функциональная безопасность программируемых электронных систем, относящихся к безопасности» [8], а также в стандарте Европейского комитета по стандартизации (CENELEC) EN 50129 «Системы безопасности электронные для сигнализации на железных дорогах» [9], реализована концепция уровней полноты (целостности) безопасности. Согласно этой концепции, которая хорошо согласуется с рассматриваемым методологическим подходом, введены четыре уровня полноты безопасности SIL (Safety Integrity Level). Каждый уровень характеризуется определённым интервалом значений условной вероятности $P(B_i / A_i, t)$ при t = 1 год:

1 уровень - $10^{-2} \le P(B_i / A_i, t) < 10^{-1}$;

2 уровень - $10^{-3} \le P(B_i / A_i, t) < 10^{-2}$;

3 уровень - $10^{-4} \le P(B_i / A_i, t) < 10^{-3}$;

4 уровень - $10^{-5} \le P(B_i / A_i, t) < 10^{-4}$.

Откуда следует, что чем выше уровень полноты безопасности, тем более жёсткие требования предъявляются к системе защиты от угроз безопасному состоянию ИУС, т.е. уровень SIL 4 является высшим, а уровень SIL 1- низшим уровнем безопасности.

Приведём пример установления уровня полноты безопасности в соответствии с МЭК 61508 и EN 50129 (числовые значения параметров в этом примере носят иллюстративный характер).

Приемлемое значение вероятности гибели человека в поезде метрополитена в результате открытия дверей вагона во время движения поезда принято равным 10^{-5} в год. Известно, что команда на открытие дверей вагона выдаётся контроллером на основе определения положения поезда с учётом сигнала от инфракрасного датчика коррекции пути, установленного на станции [5]. Интенсивность отказов этой системы управления не превышает 10^{-4} 1/час, т.е. вероятность её отказа в течение одного года непрерывной работы равна 0,583. Предположим, что вероятность того, что человек, находящийся в поезде, располагается в непосредственной близости у двери вагона, равна 0,5, а вероятность гибели человека при открытии двери вагона во время движения поезда составляет 0,8. Средством защиты человека от этой угрозы является датчик скорости и бортовая цифровая вычислительная машина (БЦВМ), которая выдаёт разрешающую команду на открытие дверей при нулевой скорости движения поезда.

Удалено:

Удалено: 4

Требуемое значение вероятности отказа средства защиты в течение одного года находится из выражения

$$P_{тр} = \frac{10^{-5}}{0{,}583 \cdot 0{,}5 \cdot 0{,}8} = 4{,}29 \cdot 10^{-5}.$$

Следовательно, на основании МЭК 61508 и EN 50129 средство защиты для обеспечения заданного значения приемлемой вероятности гибели человека должно соответствовать четвёртому уровню полноты безопасности (SIL 4).

Если интенсивность отказов средства защиты $\lambda_{сз} = 3{,}6 \cdot 10^{-5}$ 1/час (т.е. вероятность его отказа в течение одного года $P_{1к} = 0{,}27 > P_{тр}$), то необходимо ввести дополнительное оборудование, которое способно обеспечить заданные требования по безопасности, например, второй идентичный канал защиты, содержащий датчик скорости и БЦВМ. Тогда двери вагона могут открываться только при поступлении команд от двух БЦВМ. Отказ одного из каналов переводит систему управления открытием дверей в неработоспособное защитное состояние, при котором двери вагонов могут быть открыты только машинистом после остановки поезда. Если время обнаружения отказа одного из каналов системы защиты не превышает $\Delta t = 10$ с, то вероятность опасного отказа двухканальной системы защиты рассчитывается по приближённой формуле

$$P_{2к} = 2 \cdot P_{1к} \cdot l_{сз} \cdot \Delta t = 2 \cdot 0{,}27 \cdot 3{,}6 \cdot 10^{-5} \cdot 10 / 3600 = 0{,}0054 \cdot 10^{-5} < P_{тр}.$$

Следовательно, введение дополнительного канала обеспечивает заданные требования по безопасности. Однако при этом система управления процессом открытия дверей вагонов поездов метрополитена становится более дорогостоящей и менее надёжной, поскольку переход системы в неработоспособное (защитное) состояние происходит при возникновении отказа любого из двух каналов средства защиты.

Приведённый пример, а также опыт, накопленный при решении практических задач, связанных с обоснованием требований по безопасности и последующей проверкой соответствия разработанной ИУС этим требованиям, показывает необходимость скорейшего решения следующих проблем:

- формирование чёткой и понятной (как заказчикам, так и разработчикам и экспертам по сертификации) терминологической базы теории функциональной безопасности, в которой однозначно раскрыта сущность терминов «безопасность», «риск», «опасное состояние», «опасное событие» и т.п.;
- разработка научно-обоснованных перечней возможных рисков для связанных с безопасностью систем;
- установление конкретных значений нижних (минимально допустимых) границ для показателей всех рассматриваемых рисков, в том числе: индивидуального и социального рисков, а также рисков обслуживающего персонала с

учётом рекомендаций, изложенных в документах международных организаций по стандартизации.

Рассмотренный методологический подход позволяет сформулировать принципы нормирования безопасности ИУС, способных в процессе функционирования привести к гибели людей, установить в нормативно-технической документации разрабатываемых систем научно-обоснованные количественные и качественные требования к безопасности, гармонизированные с международными стандартами и способные обеспечить объективность анализа соответствия при проведении сертификации.

Литература

1. Белов П.Г., Гражданкин А.И., Махутов Н.А. Стандартизация и регламентация в сфере безопасности: реалии и перспективы // Стандарты и качество. — 2004. — № 2. – С. 26–33.

2. Белов В.П., Голяков А.Д. Терминологическая база теории безопасности // Стандарты и качество. – 2004. – №9. – С. 48 – 51.

3. Шалягин Д.В., Шубинский И.Б. Надёжность и безопасность железнодорожной автоматики // Автоматика, связь, информатика. – 2005. – №2. – С. 23 – 26.

4. Белов В.П., Голяков А.Д., Старков С.Я. О понятиях «надёжность» и «безопасность» технических систем с позиции разработчиков // Методы менеджмента качества. – 2003. – №10. – С. 46 – 49.

5. Антонов Ю.В., Белов В.П., Голяков А.Д. и др. Надёжность и безопасность информационно-управляющих систем: методы оценивания и контроля. – С-Пб.: ОАО «НИИ ТМ», 2004. – 324 с.

6. Лисанов М.В. О техническом регулировании и критериях приемлемого риска // Безопасность труда в промышленности. – 2004. – №5. – С. 11–14.

7. Лесных В.В. Нормирование риска: зарубежный и отечественный опыт. hazard.fromru.com/Seminar/6/Lsnh_txt.htm.

8. IEC 61508: 1-6. Functional safety of electrical/electronic/programmable electronic safety-related systems. 1998 – 2000.

9. EN 50129. Railway applications. Safety related electronic systems for signaling. 2003.

10. ГОСТ Р 12.3.047-98. ССБТ. Пожарная безопасность технологических процессов. Общие требования. Методы контроля.

Удалено:
Удалено:
Удалено:
Удалено:
Удалено:
Удалено:
Удалено:
Удалено:
Удалено:
Удалено:
Удалено:
Удалено:
Удалено:
Удалено:
Удалено:
Удалено:
Удалено:
Удалено:
Удалено:
Удалено:
Удалено:
Удалено:
Удалено:
Удалено:
Удалено:
Удалено: