УДК 681.5
ББК 32.965

ктн Антонов Ю.В., ктн доцент Белов В.П., дтн профессор Голяков А.Д.

Научно-исследовательский институт точной механики, г. Санкт-Петербург

МЕТОДИКА ОБОСНОВАНИЯ ТРЕБОВАНИЙ К ТЕХНИЧЕСКИМ СРЕДСТВАМ ЗАЩИТЫ ПОТЕНЦИАЛЬНО ОПАСНЫХ ОБЪЕКТОВ

В современных условиях одной из важнейших задач отечественной промышленности является повышение конкурентоспособности производимых изделий. Центральное место при этом, наряду с обеспечением высоких показателей назначения, надёжности, экономичности и т.п., занимает безопасность. Особую значимость проблема обеспечения заданных показателей безопасности приобретает при эксплуатации объектов, относящихся к категории потенциально опасных. Отказы аппаратных средств, ошибки в программном обеспечении систем управления потенциально опасных объектов представляют собой угрозы безопасному состоянию [1] таких объектов. Эти события способны привести к гибели людей, нанести материальный и экологический ущерб, т.е. угрозы являются предвестником происшествий [2].

Для борьбы с угрозами используются различные меры защиты, которые могут носить административный или технический характер. Административные меры направлены на предотвращение ошибок обслуживающего персонала, а также на предоставление сведений населению о наличии источника опасности. К административным мерам относятся различного рода инструкции, предупреждающие плакаты, знаки, сигналы, а также другие организационные и правовые мероприятия. Наибольшую значимость и жёсткость они принимают тогда, когда технические средства либо отсутствуют, либо не могут противодействовать угрозам и обеспечить требуемую степень безопасности. Административные меры применяются на всех этапах жизненного цикла потенциально опасных объектов, но не всегда имеют высокую эффективность.

Основным и наиболее эффективным способом борьбы с угрозами безопасному состоянию потенциально опасного объекта является использование технических мер защиты, которые классифицируются по ряду признаков, в частности, по возможности прекращения процесса функционирования объекта при возникновении угрозы. По этому признаку технические средства защиты различаются на пассивные (заграждения, замки и т.п.) и активные (предохранительные устройства, системы самоблокировки и т.п.). С помощью пассивных средств защиты достигается снижение возможности реализации соответствующего типа угрозы без потери работоспособности потенциально опасного объекта. При использовании активных средств защиты обеспечивается обнаружение (идентификация) угрозы, оповещение обслуживающего персонала о появлении угрозы и проведение необходимых операций (действий) для перевода потенци-

ально опасного объекта в, так называемое, защитное (не работоспособное) состояние, из которого переход в опасное состояние маловероятен (практически исключён).

Пассивные средства защиты отличаются, как правило, сравнительно простым исполнением и высокой надёжностью. Однако в ряде случаев они не способны обеспечить необходимый уровень защиты от всей совокупности возможных угроз. Поэтому широкое распространение в настоящее время получили активные (в том числе аппаратно-программные) средства защиты, способные к самоорганизации и саморегулированию [2, 3].

Для решения задачи обоснования требований к количественным и качественным показателям безопасности технических средств защиты разработана методика, которая построена на концепции уровней полноты безопасности. Эта концепция положена в основу рекомендаций международной электротехнической комиссии (МЭК), которые изложены в широко используемом в настоящее время международном стандарте IEC 61508 [4, 5]. Концепция уровней полноты безопасности применяется также Европейским комитетом по стандартизации (CENELEC), который выпустил серию стандартов по вопросам безопасности систем, в том числе систем, построенных на базе программируемых логических контроллеров (EN 50126, EN 50128, EN 50129, EN 50159).

Согласно этим рекомендациям требования к показателям безопасности технических средств защиты задаются в зависимости от частоты угроз источника опасности. При этом все источники угроз разделены на две группы. В первую группу входят источники с «высокой» частотой угроз, а во вторую группу – с «низкой» частотой угроз. В качестве граничного значения частоты появления угроз $\left(f_{гр}(t)\right)$международным стандартом IEC 61508 определена частота, равная одной угрозе в год, т.е. $f_{гр}(t) = 1{,}14 \cdot 10^{-4}\ 1/\text{час}$.

Следовательно, если угрозой безопасности при функционировании потенциально опасного объекта является, например, опасный отказ какого-либо критического элемента его системы управления, то при частоте таких отказов $f_{у}(t) > f_{гр}(t)$ требования к средству защиты от этой угрозы соответствуют первой группе. В противном случае, т.е. при выполнении условия $f_{у}(t) \le f_{гр}(t)$, полагается, что угрозы появляются с «низкой» частотой. Для таких систем управления применяется требования к средству защиты, которые относятся ко второй группе.

Заметим, что частоту отказов следует отличать от интенсивности отказов, которая является одним из широко применяемых показателей надёжности отечественных систем и представляет собой условную плотность распределения времени наступления отказов. Интенсивность отказов $\left(l(t)\right)$ зависит от закона распределения отказов, т.е.

$$f(t) = P(t)\, l(t),$$

где $P(t)$ - вероятность безотказной работы системы.

Поэтому при выполнении условия $P(t) \approx 1$ справедливо приближённое равенство этих параметров, т.е. $f(t) \approx l(t)$.

Каждая группа источников угроз в соответствии с рекомендациями стандарта IEC 61508 имеет четыре уровня полноты (целостности) безопасности SIL (Safety Integrity Level), которые определяют требования к техническим средствам защиты. Эти требования задаются в виде условной частоты ($f_{сз}(t)$ - первая группа) или в виде условной вероятности ($P_{сз}(t)$ - вторая группа) наступления события, заключающегося в том, что средство защиты не способно противостоять соответствующей угрозе при условии её появления в течение времени t. Конкретные значения уровней SIL приведены в таблице 1 [5].

Таблица 1

Уровни полноты безопасности (SIL) по IEC 61508

Номер уровня SIL	Частота появления угроз от источника опасности	
	высокая $\left(f_у(t) > f_{гр}(t)\right)$	низкая $\left(f_у(t) \le f_{гр}(t)\right)$
4	$10^{-9}(1/\text{час}) \le f_{сз}(t) < 10^{-8}(1/\text{час})$	$10^{-5} \le P_{сз}(t = 1\ \text{год}) < 10^{-4}$
3	$10^{-8}(1/\text{час}) \le f_{сз}(t) < 10^{-7}(1/\text{час})$	$10^{-4} \le P_{сз}(t = 1\ \text{год}) < 10^{-3}$
2	$10^{-7}(1/\text{час}) \le f_{сз}(t) < 10^{-6}(1/\text{час})$	$10^{-3} \le P_{сз}(t = 1\ \text{год}) < 10^{-2}$
1	$10^{-6}(1/\text{час}) \le f_{сз}(t) < 10^{-5}(1/\text{час})$	$10^{-2} \le P_{сз}(t = 1\ \text{год}) < 10^{-1}$

Анализ значений показателей, приведённых в таблице 1, свидетельствует о том, что чем выше уровень полноты безопасности, тем более жёсткие требования предъявляются к системе защиты от угроз безопасному состоянию системы, т.е. уровень SIL 4 является высшим, а уровень SIL 1 – низшим уровнем безопасности. Для расчёта показателей, характеризующих конкретные значения SIL, используется сценарный подход.

Предлагаемая методика обоснования требований к техническим средствам защиты потенциально опасных объектов разработана с использованием концепции уровней полноты безопасности в рамках рекомендаций международного стандарта IEC 61508. Сущность этой методики, которая построена на основе субъектно-объектной природы свойства безопасности, заключается в следующем.

1. Определяется объект безопасности, нуждающийся в защите (например, человек, группа людей, обслуживающий персонал и т.п.).
2. Формируется перечень возможных угроз безопасности, и определяются источники этих угроз.
3. Расчётным, экспериментальным или расчётно-экспериментальным методом [6 – 8] оценивается частота появления угроз каждого источника опасности.
4. В соответствии с принятым критерием (путём сравнения оценки частоты угрозы с граничным значением) определяется группа, к которой относится источник угроз.
5. Устанавливается предельно допустимое значение вероятности происшествия (например, гибели человека в течение одного года), на которое общество (или

эксплуатирующая организация) готово пойти ради выгод, получаемых от эксплуатации потенциально опасного объекта (показатель риска)[1].

6. Определяется вклад, который вносит каждая угроза в возможность наступления происшествия. Этот вклад характеризуется значением коэффициента нормирования, сумма которых равна единице. Коэффициент нормирования вводится при необходимости оценивания вероятности гибели группы людей, т.е. социального риска. Если в качестве происшествия принимается гибель человека в определённой области пространства в течение заданного времени (например, одного года), то, как правило, полагается, что каждая угроза вносит равнозначный вклад в возможность наступления фатального события.

7. Оцениваются вероятности возникновения происшествия при условии появления угрозы, присутствия объекта безопасности в рассматриваемой области пространства и в течение заданного времени. При необходимости расчёта территориального риска полагается, что объект безопасности (например, человек) находится в выбранной для анализа области пространства, т.е. условная вероятность этого события принимается равной единице.

8. Рассчитываются значения частоты или вероятности событий, заключающиеся в том, что средства защиты не способны противостоять всем угрозам из принятого перечня.

9. С помощью таблицы 1 определяется требуемый уровень полноты безопасности технического средства защиты.

Для практического применения настоящей методики необходимы следующие исходные данные:

категория объекта безопасности, подлежащего защите от угроз, и характеристика вреда (ущерба), который может быть ему нанесён (например, объект безопасности – человек, наносимый вред от угроз – гибель человека);

перечень угроз и частота их появления;

минимально допустимое значение вероятности нанесения ущерба в течение заданного времени (например, вероятность гибели человека 10^{-6} в год);

значения условных вероятностей расположения объекта безопасности в заданной области пространства и в заданное время при появлении угрозы;

значения условных вероятностей нанесения ущерба объекту безопасности при появлении угроз в заданное время и в заданной области пространства.

В докладе приведён пример обоснования требований к уровню полноты безопасности технического средства защиты пассажира поезда метрополитена. В качестве происшествий приняты гибель пассажира при открытии дверей вагона во время движения поезда и при столкновении двух поездов. С помощью примера показано, что при использовании одноканальной системы защиты желаемый уровень индивидуального риска не достигается. Введение дублированной системы обеспечивает требования по безопасности. При этом сделан вывод о том, что с ростом требований к безопасности пассажиров метрополитена

[1] В ряде европейских стран (Голландия, Великобритания и др.) значение этой вероятности выбирается из диапазона $10^{-6} \div 10^{-5}$ для населения и $10^{-5} \div 10^{-4}$ для обслуживающего персонала.

снижаются характеристики надёжности системы управления движением поезда, поскольку отказ любого из каналов средства защиты переводит систему в защитное (неработоспособное) состояние, выход из которого возможен только после проведения восстановительных работ, связанных с ремонтом (заменой) отказавшего оборудования. Кроме того, внедрение средств защиты с высоким уровнем SIL приводит к росту стоимости систем, предназначенных для обеспечения безопасности движения поездов метрополитена.

Предлагаемая методика позволяет установить в нормативно-технической документации разрабатываемых систем управления потенциально опасных объектов научно-обоснованные количественные и качественные требования к безопасности технических средств защиты, гармонизированные с международными стандартами и способные обеспечить объективность анализа соответствия при проведении сертификации.

Литература

1. Белов В.П., Голяков А.Д. Терминологическая база теории безопасности // Стандарты и качество. – 2004. – №9. – С. 48 – 51.
2. 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.
3. Статистические методы анализа безопасности сложных технических систем: Учебник / Л.Н. Александровская, И.З. Аронов, А.И. Елизарова и др.; Под ред. В.П. Соколова - М.: Логос, 2001. – 232 с.
4. IEC 61508: 1-6. Functional safety of electrical/electronic/programmable electronic safety-related systems. 1998 – 2000.
5. Смит Д., Симпсон К. Функциональная безопасность (Простое руководство по применению стандарта МЭК 61508 и связанных с ним стандартов). – М.: Изд. Дом «Технологии», 2004. – 208 с.
6. Антонов Ю.В., Белов В.П., Голяков А.Д. Аналитическое и экспериментальное оценивание технических систем повышенной опасности / В Сб. докладов на 3 НТК «Перспективы использования новых технологий и научно- технических решений в изделиях ракетно-космической техники разработки ГКНПЦ им. М.В. Хруничева», Москва, 2003, С. 41– 43.
7. Антонов Ю.В., Белов В.П., Голяков А.Д. и др. Надёжность и безопасность информационно-управляющих систем (методы оценивания и контроля). – СПб.: ОАО «НИИ ТМ», 2004. – 326 с.
8. Белов В.П., Голяков А.Д. Анализ методов оценивания безопасности технических систем / Сб. трудов 23 МНТК «Проблемы обеспечения эффективности и устойчивости функционирования сложных технических систем». – Серпухов, 2004, С. 242 – 246.