МИНИСТЕРСТВО ПРОМЫШЛЕННОСТИ И ЭНЕРГЕТИКИ

МЕЖДУНАРОДНАЯ АССОЦИАЦИЯ
«СИСТЕМСЕРВИС»
приборостроение, средства автоматизации и системы управления.
Комплексные системы безопасности, информатизации и связи

Стандарт Ассоциации

КОМПЛЕКСНАЯ БЕЗОПАСНОСТЬ ЗДАНИЙ И СООРУЖЕНИЙ ОБЩИЕ ПОЛОЖЕНИЯ

СТА 25.03.014-2005

Издание официальное
2005 год

gost.e-ecolog.ru

МИНИСТЕРСТВО ПРОМЫШЛЕННОСТИ И ЭНЕРГЕТИКИ

МЕЖДУНАРОДНАЯ АССОЦИАЦИЯ
«СИСТЕМСЕРВИС»
приборостроение, средства автоматизации и системы управления.
Комплексные системы безопасности, информатизации и связи

Стандарт Ассоциации

КОМПЛЕКСНАЯ БЕЗОПАСНОСТЬ ЗДАНИЙ И СООРУЖЕНИЙ ОБЩИЕ ПОЛОЖЕНИЯ

СТА 25.03.014-2005

Издание официальное
2005 год

Группа П 77

МИНИСТЕРСТВО ПРОМЫШЛЕННОСТИ И ЭНЕРГЕТИКИ

МЕЖДУНАРОДНАЯ АССОЦИАЦИЯ
«СИСТЕМСЕРВИС»

КОМПЛЕКСНАЯ ФУНКЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ ЗДАНИЙ И СООРУЖЕНИЙ ОБЩИЕ ПОЛОЖЕНИЯ

Часть 1
СТА 25.03.014 -2005

ПРИКАЗОМ МЕЖДУНАРОДНОЙ АССОЦИАЦИИ «СИСТЕМСЕРВИС»

От .. .. 2005 года № .. срок действия установлен с «1» ноября 2005 года

1. ОБЛАСТЬ ПРИМЕНЕНИЯ

1.1. Требования настоящего стандарта распространяются на все здания, строения, сооружения, включая входящие в них машины (механизмы) и инженерное оборудование жизнеобеспечения объекта и системы, связанные с обеспечением безопасности, кроме предназначенных для федеральных государственных нужд (оборонный заказ), составляющих государственную тайну, охраняемых в соответствии с законодательством Российской Федерации. Постановлениями Российской Федерации устанавливаются перечни объектов, относящиеся к

различным категориям, в зависимости от характера опасностей (угроз), условий и источников их возникновения, тяжести последствий при их реализации и имеющихся ресурсов по снижению риска до уровня допустимого риска.

1.2. Виды зданий, строений, сооружений, на которые распространяется требования данного стандарта, приведены в приложении 1.

1.3. Виды машин (механизмов) и инженерного оборудования жизнеобеспечения объекта, на которые распространяются требования настоящего стандарта, приведены в приложении 2.

1.4. Виды систем безопасности, на которые распространяются требования настоящего стандарта, приведены в приложении 3.

Издание официальное Перепечатка воспрещена

2. НОРМАТИВНЫЕ ССЫЛКИ

В настоящем стандарте использованы ссылки на следующие нормативно-технические документы:

Федеральный закон РФ «О борьбе с терроризмом» от 25.06.1998 г. №130-ФЗ.

Федеральный закон РФ «О безопасности» от 5.04.1992 г. №2446-1-ФЗ.

Федеральный закон РФ «О промышленной безопасности опасных производственных объектов» от 21.07.1997 г. № 116-ФЗ.

Федеральный закон РФ от 09.01.1996 «О радиационной безопасности населения и территории от чрезвычайных ситуаций природного и техногенного характера» от 21.12.1994 г. №8-ФЗ.

Федеральный закон РФ «О техническом регулировании» от 27.12.2002 г. №184-ФЗ.

Федеральный закон РФ «О противодействии экстремистской деятельности» от 25.06.2002 г. №14-ФЗ.

Гражданский Кодекс Российской Федерации от 25.06.2002 г. №14-ФЗ.

Федеральный закон «О пожарной безопасности» от 21 декабря 1994 (изм.6 августа 2001г.)

Закон г. Москвы «О защите населения и территории города от чрезвычайных ситуаций природного и техногенного характера» от 5.11.1997 г. №46.

ГОСТ Р 22.3.09 Безопасность в чрезвычайных ситуациях. Защита помещений. Основные положения.

МЭК 61508-0: 2005 – Функциональная безопасность электрических и/или электронных, и/или программируемых электронных систем, связанных с функциональной безопасностью. Часть 0. Общее руководство.

МЭК 61508-1: 1998 – Функциональная безопасность электрических и/или электронных, и/или программируемых электронных систем, связанных с функциональной безопасностью. Часть 1. Общие требования.

МЭК 61508-2: 2000 – Функциональная безопасность электрических и/или электронных, и/или программируемых электронных систем, связанных с функциональной безопасностью. Часть 2. Требования к электрическим /электронным / программируемым электронным системам, связанным с безопасностью.

МЭК 61508 -3: 1998 – Функциональная безопасность электрических и/или электронных, и/или программируемых электронных систем, связанных с функциональной безопасностью. Часть 3. Требования к программному обеспечению.

МЭК 61508-4: 1998 – Функциональная безопасность электрических и/или электронных, и/или программируемых электронных систем, связанных с функциональной безопасностью. Часть 4. Определения и сокращения.

МЭК 61508-5: 1998 – Функциональная безопасность электрических и/или электронных, и/или программируемых электронных систем, связанных с функциональной безопасностью. Часть 5. Примеры методов для определения уровней полноты безопасности.

МЭК 61508-6: 2000 – Функциональная безопасность электрических и/или электронных, и/или программируемых электронных систем, связанных с функциональной безопасностью. Часть 6. Руководящие указания по применению стандартов МЭК 61508-2 и МЭК 61508-3.

МЭК 61508-7: 1998 Функциональная безопасность электрических и/или электронных, и/или программируемых электронных систем, связанных с функциональной безопасностью. Часть 7. Обзор методов и средств измерения.

Руководство ИСО/МЭК 51: 1999 - Аспекты безопасности. Руководящие указания по включению их в стандарты.

ИСО/МЭК 15408-1-99. Информационные технологии». Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий.

Часть 1. Введение и общая модель.

Часть 2. Функциональные требования безопасности.

Часть 3. «Требования доверия к безопасности».

3. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Для целей настоящего стандарта использованы следующие термины, определения и аббревиатуры, гармонизированные с терминологией МЭК и ИСО:

строительный объект – отдельное здание (строение, сооружение) или группа зданий, включая входящие в него (них) машины (механизмы) и инженерное оборудование жизнеобеспечения объекта, системы, связанные с безопасностью, и прилегающую территорию;

ущерб – физическое повреждение (травма) или вред, нанесённый жизни или здоровью человека (людей) либо прямо, либо косвенно в результате вреда, нанесённого имуществу, окружающей среде, жизни и здоровью животных и растений;

опасность – потенциальный источник ущерба;

опасная ситуация – обстоятельства, при которых человек (люди), имущество, или окружающая среда, животные и растения подвергаются опасности;

опасное событие – опасная ситуация, которая приводит к ущербу;

вызывающее ущерб событие – событие, при котором опасная ситуация приводит к ущербу;

риск – сочетание вероятности нанесения ущерба жизни или здоровью граждан, имуществу физических или юридических лиц, государственному или муниципальному имуществу, ок-

ружающей среде, жизни или здоровью животных и растений с учётом тяжести этого ущерба.

допустимый риск – риск, который общепринят в данных обстоятельствах на основе существующих в данное время ценностей общества Российской Федерации;

безопасность – отсутствие недопустимого риска, связанного с причинением вреда жизни или здоровью людей, имуществу физических или юридических лиц, государственному или муниципальному имуществу, окружающей среде, жизни или здоровью животных и растений;

комплексная безопасность – безопасность в условиях совокупного воздействия различных видов опасности;

защитная мера – мера, используемая для уменьшения риска, которая может снижать риск за счёт безопасных в своей основе проектов, защитных устройств, персонального защитного оборудования, за счёт информации по установке и применению, а также за счёт обучения;

остаточный риск – риск, оставшийся после принятия защитных мер;

анализ риска – систематическое использование имеющейся информации для выявления опасностей и оценивания риска;

оценивание риска – основанная на анализе рынка процедура проверки, не превышен ли допустимый риск;

общая оценка риска – полный процесс анализа риска и оценивания риска;

предназначенное использование – использование строительного объекта, с входящими в его состав машинами (механизмами), системами, в соответствии с информацией, предоставленной поставщиком строительного объекта или поставщиком услуг по его использованию;

предназначенное использование - использование строительного объекта, с входящими в его состав машинами (механизмами), системами, в соответствии с информацией, предостав-

ленной поставщиком строительного объекта или поставщиком услуг по его использованию;

возможное предсказуемое неправильное использование - использование строительного объекта, с входящими в его состав машинами (механизмами), системами, в условиях и для целей, не предусмотренных поставщиком строительного объекта или поставщиком услуг по его использованию, но которое может быть следствием предсказуемого поведения человека;

оборудование, находящееся под управлением – одна из мер, используемых для уменьшения *риска,* которая заключается в автоматическом управлении оборудованием с помощью электрических и/или электронных, и/или электронных программируемых (Э/Э/ЭП) систем, связанных с безопасностью;

система, связанная с безопасностью (ССБ) – система, выполняющая функцию или функции безопасности

(Примечание 1. В зависимости от характера опасности или назначения функции безопасности различают системы пожарной сигнализации, охранной сигнализации, системы пожартушения, системы контроля и управления доступом, охранные системы и т.п.

Примечание 2. Человек может входить в состав системы, связанной с безопасностью, как один из элементов этой системы);

надежное состояние - состояние оборудования, находящегося под управлением, при котором достигается безопасность;

функция безопасности - функция, которая предназначена для достижения или поддержания надежного состояния оборудования, находящегося под управлением, для определенного опасного события;

(Примечание. Функция безопасности характеризуется двумя составляющими: назначением, которое определяет, что выполняется для снижения риска, и полнотой безопасности - вероятностью удовлетворительного выполнения *функции безопасности при заданных условиях в заданном интервале времени*);

полнота безопасности – вероятность удовлетворительного выполнения функции безопасности системой, связанной с

безопасностью, при конкретных условиях и в пределах конкретного периода времени;

уровень полноты безопасности – дискретный уровень (один из возможных четырех) для определения требований, предъявляемых к функции безопасности, которые должны быть выполнены системами, связанными с безопасностью;

внешнее средство сокращения риска - отдельное средство для сокращения или смягчения риска, которое отличается от Э/Э/ПЭ систем, связанных с безопасностью, и не использует их, либо иная система, связанная с безопасностью (например, ров, дамба, ограда, брандмауэр и т.п.);

функциональная безопасность - часть безопасности, относящаяся к оборудованию, находящемуся под управлением (далее именуемому ОПУ), и системам управления ОПУ, которая зависит от Э/Э/ПЭ систем, связанных с безопасностью, других технических систем, относящихся к безопасности, и внешних средств сокращения риска;

комплексная система безопасности (КСБ) – система, связанная с безопасностью, одновременно выполняющая несколько функций безопасности, снижающих риски, связанные с различными видами опасностей

группа безопасности (строительного объекта) – идентификационный признак строительного объекта, характеризующийся частотой обращения к действиям систем, связанных с безопасностью: для группы с низкой частотой обращения «L» (от английского Low - низкая) частота обращения к действиям этих систем не больше, чем один раз в год и не больше, чем два раза за период регламентных испытаний; для группы с высокой частотой обращения (или с непрерывным обращением) «H» (от английского High - высокая) к действиям систем, связанных с безопасностью, больше, чем один раз в год и больше, чем два раза за период регламентных испытаний;

категория безопасности (строительного объекта) – идентификационный признак строительного объекта (один из четырех в каждой из групп безопасности), характеризующийся минимально требуемой вероятностью опасных сбоев в системах, связанных с безопасностью, для достижения полноты безопасности, обеспечивающей допустимый риск;

проектировщик – юридическое или физическое лицо, несущее в соответствии с законодательством Российской Федерации ответственность за соблюдение требований технических регламентов при проектировании строительного объекта;

застройщик - юридическое или физическое лицо, несущее в соответствии с законодательством Российской Федерации ответственность за соблюдение требований технических регламентов при строительстве строительного объекта;

поставщик – юридическое или физическое лицо, несущее в соответствии с законодательством Российской Федерации ответственность за соблюдение требований технических регламентов передаваемых в эксплуатацию либо в пользование законченных строительством строительных объектов или их частей;

эксплуатант - юридическое или физическое лицо, несущее в соответствии с законодательством Российской Федерации ответственность за соблюдение требований безопасности при эксплуатации строительного объекта (включая эксплуатацию машин (механизмов), оборудования и систем, в него входящих) и требований технических регламентов (в части эксплуатации);

пользователь - юридическое или физическое лицо, несущее в соответствии с законодательством Российской Федерации ответственность за соблюдение требований безопасности при пользовании приобретенным в собственность, арендуемым или предоставленным ему в пользование строительным объ-

ектом, либо его части в соответствии с информацией, предоставленной ему застройщиком или поставщиком;

орган по сертификации - юридическое лицо или индивидуальный предприниматель, аккредитованные в установленном порядке для выполнения работ по сертификации в области строительства и комплексной безопасности строительных объектов;

испытательная(ый) лаборатория (центр) - юридическое лицо или индивидуальный предприниматель, аккредитованные в установленном порядке на компетентность и независимость для проведения исследований (испытаний), измерений и (или) расчетов, подтверждающих (опровергающих) соответствие строительных объектов требованиям технических регламентов и/или положениям стандартов, и/или условиям договоров области строительства и комплексной безопасности строительных объектов;

оценка соответствия - прямое или косвенное определение соблюдения соответствия строительного объекта требованиям технических регламентов, положениям стандартов или условиям договоров;

подтверждение соответствия - документальное удостоверение соответствия строительного объекта требованиям технических регламентов и/или положениям стандартов, и/или условиям договоров;

форма подтверждения соответствия - определенный порядок документального удостоверения соответствия строительных объектов требованиям технических регламентов и/или положениям стандартов и/или условиям договоров;

сертификация - форма осуществляемого органом по сертификации подтверждения соответствия строительного объекта положениям стандартов или условиям договоров;

система сертификации - совокупность правил выполнения работ по сертификации, ее участников и правил функционирования системы сертификации в целом;

сертификат соответствия – выданный органом по сертификации документ, удостоверяющий соответствие объекта требованиям технических регламентов и/или положениям стандартов и/или условиям договоров;

заявитель – зарегистрированное в соответствии с законодательством Российской Федерации на ее территории юридическое лицо или физическое лицо, в качестве индивидуального предпринимателя, или являющееся застройщиком, продавцом, поставщиком строительного объекта, или услуг по его использованию, либо лицо, выполняющее функции иностранного застройщика, продавца, поставщика строительного объекта или услуг по его использованию на основании договора с ним в части обеспечения соответствия строительного объекта, требованиям технических регламентов и в части ответственности за несоответствие строительного объекта требованиям технических регламентов, предоставляющее для регистрации федеральным органом исполнительной власти по техническому регулированию оформленную надлежащим образом декларацию о соответствии или заключающее договор с органом по сертификации о сертификации строительного объекта на соответствие требованиям настоящего технического регламента;

декларирование соответствия – форма подтверждения соответствия строительных объектов требованиям технических регламентов, положениям стандартов или условиям договоров путем принятия заявителем декларации о соответствии на основе собственных доказательств или на основании доказательств, полученных с участием третьей стороны (органа по сертификации, испытательной лаборатории, испытательного центра);

декларация о соответствии – оформленный в установленном порядке заявителем самостоятельно или с привлечением третьей стороны документ, подтверждающий соответствие строительного объекта требованиям технических регламентов;
орган государственного контроля (надзора) – подведомственное федеральному органу исполнительной власти, органу исполнительной власти субъекта Российской Федерации государственное учреждение, уполномоченное на проведение государственного контроля (надзора) в области строительства и безопасности в соответствии с законодательством Российской Федерации;
ИСО – Международная организация по стандартизации (членом которой является Российская Федерация);
МЭК – Международная электротехническая комиссия (членом которой является Российская Федерация);

4. ОБЩИЕ ТРЕБОВАНИЯ КОМПЛЕКСНОЙ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

4.1. Все строительные объекты должны быть категорированы по группам и категориям комплексной функциональной безопасности с учетом их назначения, характеристик, важности, степени опасности производств, местных условий, тяжести последствий приводящих к ущербу событий

4.2. Защитные меры, технические средства и системы безопасности, применяемые в зданиях и сооружениях, должны быть направлены на уменьшение риска до уровня допустимого риска.

4.3. Все требования безопасности должны основываться на анализе и оценке рисков, которые учитывают как вероятность нанесения ущерба, так и тяжесть этого ущерба в случае реализации опасного события.

4.4. При анализе и общей оценке рисков нанесения вреда должна быть учтена вся совокупность приводящих к ущер-

бу событий. Перечень источников и характера опасностей (угроз), которые следует учитывать в этом случае, приведен в приложении 4.

4.5. Анализ и общая оценка рисков должны проводиться на всех стадиях жизненного цикла зданий и сооружений: в период разработки концепции и проектирования, проведения строительных, монтажных и пуско-наладочных работ, ввода в эксплуатацию, эксплуатации, вывода из эксплуатации и утилизации.

5. МЕРЫ, СРЕДСТВА И СИСТЕМЫ СНИЖЕНИЯ РИСКОВ

5.1. В качестве основных средств снижения рисков в период эксплуатации зданий и сооружений следует использовать системы, связанные с безопасностью и внешние средства снижения рисков.

5.2. В качестве автоматических систем снижения риска должны быть использованы электрические и/или электронные, и/или электронные программируемые (Э/Э/ЭП) системы, связанные с безопасностью, которые, воздействуя на оборудование, находящееся под управлением (ОПУ), выполняют функции безопасности.

5.3. Мерами по снижению рисков служат исполнение требований по безопасности федеральных законов Российской Федерации, международных соглашений с участием Российской Федерации, технических регламентов Российской Федерации, национальных стандартов Российской Федерации, стандартов международных организаций по стандартизации ИСО и МЭК, которые приняты с согласия Российской Федерации.

5.4. Мерой по снижению рисков является также информация, связанная с безопасностью, доведенная до приоб-

ретателя, эксплуатанта и пользователя зданиями и сооружениями.

6. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ОТДЕЛЬНЫХ КАТЕГОРИЙ ЛИЦ

6.1. Завершённые строительством, либо находящиеся в эксплуатации и использовании здания и сооружения должны быть безопасны как в случае предназначенного использования, так и в случае прогнозируемого неправильного их использования, в том числе отдельными категориями физических лиц (детьми, людьми преклонного возраста, людьми с ограниченными возможностями) в случае, когда имеется свободный доступ к входящим в здания и сооружения машинам (механизмам) и инженерному оборудованию.

6.2. Здания и сооружения должны быть безопасны как в случае предназначенного использования, так и в случае прогнозируемого неправильного их использования операторами (представителями эксплуатанта), с учётом их профессиональных обязанностей, в случае, когда ограниченный доступ к входящим в здания и сооружения машинам (механизмам) и инженерному оборудованию.

6.3. Застройщики, поставщики зданий и сооружений и услуг несут ответственность за непредставление информации по безопасной эксплуатации этих объектов или их пользовании приобретателям, представителям эксплуатанта и пользователям в соответствии с действующим законодательством Российской Федерации.

7. ГРУППЫ И КАТЕГОРИИ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ ЗДАНИЙ И СООРУЖЕНИЙ

7.1. Строительные объекты в зависимости от допустимого риска при их эксплуатации, пользовании, обслуживании, ремонте и утилизации делятся на две группы (группу с низкой необходимой частотой обращения к системам, связанным с безопасностью «L» и группу с высокой необходимостью частотой обращения к системам, связанным с безопасностью «H») по четыре категории (1,2,3,4) в каждой из групп.

7.2. Категории безопасности объектов, относящихся к группе «H», и минимальные требуемые значения вероятности (p) опасных сбоев в течение одного часа в системах, связанных с безопасностью, для достижения допустимого уровня безопасности объекта соответствующей категории указаны в таблице 1.

Высокая частота обращения к системам – группа «H»

Категория безопасности	Диапазон вероятности сбоев в системах, связанных с безопасностью в 1 час
4	$10^{-9} \le p < 10^{-8}$
3	$10^{-8} \le p < 10^{-7}$
2	$10^{-7} \le p < 10^{-6}$
1	$10^{-6} \le p < 10^{-5}$

7.3. Категории безопасности объектов, относящихся к группе «L», и минимальные требуемые значения вероятности (p) опасных сбоев в течение одного часа в системах, связанных с безопасностью, для достижения допустимого уровня безопасности объекта соответствующей категории указаны в таблице 2.

Низкая частота обращения к системам – группа «L»

Категория безопасности	Диапазон вероятности сбоев в системах, связанных с безопасностью в 1 час
4	$10^{-5} \le p < 10^{-4}$
3	$10^{-4} \le p < 10^{-3}$
2	$10^{-3} \le p < 10^{-2}$
1	$10^{-2} \le p < 10^{-1}$

8.4. Ранжирование зданий и сооружений по группам и категориям определяется Федеральным органом исполнительной власти в зависимости от вида, типа, назначения, важности строительного объекта с учетом местных условий. Перечень ранжированных зданий и сооружений, а равно и перечень угроз и их характеристик, которые учитываются для анализа и общей оценки риска для каждого из ранжированных зданий и сооружений, утверждаются постановлением Правительства и опубликовывается в печати в установленном порядке.

8. ПРОЦЕДУРЫ И МЕТОДЫ ОЦЕНКИ РИСКА И БЕЗОПАСНОСТИ ЗДАНИЙ И СООРУЖЕНИЙ

8.1. Общие методы и процедуры анализа и оценки риска, которыми следует руководствоваться при оценке полноты безопасности, приведены в приложениях 5-9 к настоящему стандарту.

Детали оценки и расчета полноты безопасности приведены в части 2 стандарта «Комплексная функциональная безопасность зданий и сооружений».

8.2. Оценка полноты безопасности здания или сооружения может осуществляться путем измерений (испытаний) систем и средств, связанных с безопасностью, непосредственно на объекте после их установки и комплексной настройки, при

сдаче объекта в эксплуатацию, в период эксплуатации, а также проводиться расчетным путем.

8.3. В случае проведения оценки расчетным путем должны быть учтены природные, климатические и иные местные условия, все взаимные связи систем, связанных с безопасностью, влияние смежных и окружающих систем, включая силовые электрические системы и системы телекоммуникаций.

ПРИЛОЖЕНИЯ

ПРИЛОЖЕНИЕ 1
ПЕРЕЧЕНЬ ВИДОВ СТРОИТЕЛЬНЫХ ОБЪЕКТОВ, НА КОТОРЫЕ РАСПРОСТРАНЯЕТСЯ ДЕЙСТВИЕ НАСТОЯЩЕГО СТАНДАРТА

Перечень видов строительных объектов, на которые распространяется действие настоящего стандарта приведен в таблице П1.

Таблица П1.

№	Вид строительного объекта
1	Здания складские
2	Здания архивов уникальных изданий, отчетов, рукописей и другой документации особой ценности
3	Здания и сооружения для автомобилей
4	Здания высотой более 28 м
5	Здания высотные и комплексные, высотой от 75 до 400 м
6	Многофункциональные комплексы
7	Жилые здания
8	Гостиницы
9	Здания общественного назначения
10	Здания общественного административно-бытового назначения
11	Здания предприятий торговли
12	Здания специализированных предприятий торговли по продаже легковоспламеняющихся и горючих жидкостей
13	Автозаправочные станции
14	Культовые здания и комплексы
15	Здания учреждений культуры и искусства (театры, концертные, выставочные залы, музеи, библиотеки)
16	Здания и сооружения физкультурно-оздоровительного и

	спортивного назначения
17	Здания учреждений народного образования (дошкольные учреждения, общеобразовательные школы, школы-интернаты, внешкольные учреждения, средние специальные и профессионально-технические учебные заведения, высшие учебные заведения)
18	Здания лечебных учреждений (стационары всех типов, поликлиники, амбулатории, станции скорой помощи, санатории, дома отдыха)
19	Склады и хранилища ядовитых и наркотических веществ
20	Вокзалы всех типов, аэропорты
21	Здания организаций и учреждений управления, проектных предприятий и организаций, НИИ, кредитно-финансовых, юридических учреждений, предприятий связи
22	Здания и сооружения атомных реакторов, объектов ядерного цикла
23	Здания и сооружения ракетно-космических комплексов
24	Здания и сооружения химических и биотехнологических комплексов
25	Здания и сооружения гидро- и теплоэнергетических комплексов
26	Здания и сооружения металлургических комплексов
27	Транспортные комплексы
28	Сооружения магистральных газо-и нефтепроводов
29	Уникальные инженерные сооружения
30	Склады и хранилища ядовитых и наркотических веществ
31	Склады и хранилища радиоактивных веществ
32	Хранилища газа, нефти и нефтепродуктов
33	Емкостные сооружения для хранения легко воспламеняющихся и горючих жидкостей
34	Склады и хранилища легко воспламеняющихся, горючих

	и взрывчатых веществ и материалов
35	Компрессорные станции и продуктопроводы
36	Закрытые галереи для транспортирования горючих веществ
37	Шлюзовые здания и сооружения, сооружения разводных мостов
38	Вокзалы всех видов транспорта, аэропорты
39	Здания и сооружения комплексов водоснабжения
40	Станции и тоннели метрополитена, другого вида подземного транспорта

ПРИЛОЖЕНИЕ 2

ПЕРЕЧЕНЬ ВИДОВ МАШИН (МЕХАНИЗМОВ), ИНЖЕНЕРНОГО ОБОРУДОВАНИЯ И СИСТЕМ ЖИЗНЕОБЕСПЕЧЕНИЯ СТРОИТЕЛЬНЫХ ОБЪЕКТОВ, НА КОТОРЫЕ РАСПРОСТРАНЯЕТСЯ ДЕЙСТВИЕ НАСТОЯЩЕГО СТАНДАРТА

Виды систем жизнеобеспечения машин (механизмов), инженерного оборудования строительных объектов, на которые распространяется действие настоящего стандарта, перечислены в таблице П2.

Таблица П2.

№	Вид системы
1	Система энергоснабжения
2	Система бесперебойного электропитания
3	Система гарантированного питания
4	Система освещения, включая аварийное освещение
5	Система холодного водоснабжения
6	Система горячего водоснабжения
7	Система сброса сточных вод, включая системы бытовой, ливневой канализаций и канализации подвала
8	Система теплоснабжения
9	Система отопления
10	Система газоснабжения
11	Система тепловых завес
12	Система общеобменной вентиляции
13	Система холодоснабжения
14	Система фанкойлов
15	Система прецизионного кондиционирования
16	Система водоподготовки бассейна
17	Система лифтов, подъемников, движущихся дорожек
18	Система телекоммуникаций и связи
19	Система управления помещением
20	Система сервисной диспетчеризации
21	Система энергосбережения

ПРИЛОЖЕНИЕ 3

ПЕРЕЧЕНЬ ВИДОВ СИСТЕМ БЕЗОПАСНОСТИ, НА КОТОРЫЕ РАСПРОСТРАНЯЕТСЯ ДЕЙСТВИЕ НАСТОЯЩЕГО СТАНДАРТА

Виды систем безопасности, на которые распространяется действие настоящего стандарта, перечислены в таблице П3.

Таблица П3.

№	Вид системы
1	Система пожарной сигнализации
2	Система пожаротушения
3	Система дымоудаления
4	Система оповещения
5	Система помещения спасения
6	Система пожарных лифтов и подъемников
7	Система контроля целостности конструкции
8	Система контроля и управления доступом
9	Система охранно-тревожной сигнализации
10	Система охраны периметра
11	Система телевизионного наблюдения
12	Система управления эвакуацией людей
13	Система физической защиты
14	Система экстренной связи
15	Система комплексной безопасности

ПРИЛОЖЕНИЕ 4

ПЕРЕЧЕНЬ ИСТОЧНИКОВ И ХАРАКТЕРА ОПАСНОСТЕЙ (УГРОЗ), КОТОРЫЕ ДОЛЖНЫ БЫТЬ УЧТЕНЫ ПРИ АНАЛИЗЕ И ОБЩЕЙ ОЦЕНКЕ РИСКА

	Группа	Группа «L»				Группа «H»			
	Категория	1	2	3	4	1	2	3	4
	Природные опасности:								
	Землетрясения (в сейсмоопасных зонах)	-	v	v	v	v	v	v	v
	Наводнения (в зонах опасности наводнений)	-	-	-	v	v	v	v	v
	Сели (в селеопасных зонах)	-	-	-	v	v	v	v	v
	Оползни (в зонах опасности оползней)	-	-	-	v	v	v	v	v
	Лавины (в лавиноопасных зонах)	-	-	-	v	v	v	v	v
	Грозы (в зонах повышенной грозовой активности)	-	-	-	-	v	v	v	v
	Ураганы (в зонах опасности ураганов)	-	-	-	v	v	v	v	v
	Обледенения (в зонах опасности обледенений)	-	-	-	-	-	v	v	v
	Техногенные опасности (угрозы):								
	Опасность излучений (при наличии источников излучений)	-	v	v	v	v	v	v	v
	Биологическая опасность (при наличии источников опасности)	-	v	v	v	v	v	v	v
	Опасность взрыва (при наличии взрывоопасных веществ и материалов)	-	-	v	v	v	v	v	v
	Опасность нарушения устойчивости и обрушения	-	-	-	v	v	v	v	v
	Опасность пожара	-	v	v	v	v	v	v	v
	Промышленная опасность (для потенциально опасных производств и технологий)	-	-	v	v	v	v	v	v
	Химическая опасность (для химических производств, складов хранилищ)	-	-	-	v	v	v	v	v
	Электрическая опасность	-	v	v	v	v	v	v	v

	Группа	Группа «L»				Группа «H»			
	Категория	1	2	3	4	1	2	3	4
	Ядерная и радиационная опасность (для ядерных объектов, производств и хранилищ ядерных материалов)	-	v	v	v	v	v	v	v
	Опасности (угрозы) исходящие от людей:								
	Вызванные прогнозируемым неправильным использованием строительного объекта и его составляющих								
	обслуживающим персоналом	-	-	-	-	v	v	v	v
	обывателями	-	-	-	v	v	v	v	v
	Вызванные злонамеренными действиями:								
	саботаж	-	-	-	-	v	v	v	v
	хищение	-	v	v	v	v	v	v	v
	диверсия	-	-	-	-	v	v	v	v
	нападение	-	-	v	v	v	v	v	v
	терроризм	-	-	-	-	-	v	v	v

ПРИЛОЖЕНИЕ 5

РИСК И ПОЛНОТА БЕЗОПАСНОСТИ – ОСНОВНАЯ КОНЦЕПЦИЯ

1. Общие положения

Риск и полнота безопасности служат мерами безопасности системы или объекта для сравнения с допустимым уровнем безопасности.

Методы и процедуры оценки риска, предусмотренные настоящим техническим регламентом, гармонизированы с методами и процедурами, изложенными в стандартах Международной электротехнической комиссии: МЭК 61508-0, МЭК 61508-1, МЭК 61508-2, МЭК 61508-3, МЭК 61508-4, МЭК 61508-5, МЭК 61508-6, МЭК 61508-7, а также в Руководстве ИСО/МЭК 51.

Относящихся к функциональной безопасности, снижение риска вызывающих ущерб событий осуществляется с помощью Э/Э/ЭП систем, связанных с безопасностью (ССБ), которые реализуют функции безопасности, благодаря чему достигается допустимый уровень безопасности.

Для определения полноты безопасности для Э/Э/ЭП ССБ, ССБ, действующих на основе других технологий, и внешних средств снижения риска могут быть использованы количественные и качественные методы которые приведены в последующих приложениях. Выбор метода зависит от конкретного строительного объекта и конкретных условий, связанных с его составом, структурой и функционированием.

Необходимое сокращение риска – это снижение риска до такого уровня, при котором достигается допустимый риск для определенной ситуации (который может быть установлен качественно[1] или количественно[2]). Цель определения допусти-

---

[1] При достижении допустимого риска должно быть установлено необходимое сокращение риска. Приложения 7 и 8 к настоящему стандарту опи-

мого риска для данного приводящего к ущербу события состоит в установлении, что является приемлемым с учетом как частоты (или вероятности) опасного события, так и его специфических последствий.

Допустимый риск зависит от множества факторов (например, серьезности травмы, числа людей, подверженных опасности, частоты, с которой человек или люди подвергаются опасности и времени нахождения в состоянии опасности). Важным фактором являются восприятие и оценка обществом (общественный резонанс) незащищенности людей от опасного события. При определении допустимого риска учитывается ряд входящих факторов. Они включают:

- руководящие принципы соответствующего органа власти, осуществляющего регулирование в области безопасности;
- договоры и соглашения между сторонами, вовлеченными в использование (применение) продукции, процесса или услуги;
- промышленные стандарты и руководства;
- международные договоры и соглашения (в достижении допустимого риска для специфических применений все большая роль отводится национальным и международным стандартам);
- высококомпетентный независимый промышленный экспертный и ученый совет консультативных органов;
- юридические требования, а также общие и частные требования, относящиеся к данному применению.

сывают качественные методы, поскольку в приведенных примерах необходимое сокращение риска установлено скорее неявно, чем явно.

[2] Например, что приводящее к ущербу событие, влекущее определенные последствия, должно происходить с частотой не более чем один раз в 10^8 часов.

2. Э/Э/ЭП системы, связанные с безопасностью

Э/Э/ЭП системы, связанные с безопасностью, вносят вклад в необходимое сокращение риска для достижения допустимого риска.

Система, связанная с безопасностью (ССБ),

- реализует требуемые функции безопасности для достижения безопасного состояния оборудования, находящегося под управлением (ОПУ), или поддержания безопасного состояния ОПУ и

- предназначена для достижения необходимой полноты безопасности для требуемых функций безопасности с помощью собственной или иной Э/Э/ЭП системы, связанной с безопасностью, систем, основанных на других технологиях, или внешних средств снижения риска.

Примечание 1 – Первая часть определения означает, что система, связанная с безопасностью, должна выполнять функции безопасности, которые должны были бы быть определены в спецификации требований к функциям безопасности. Например, спецификация требований функций безопасности может устанавливать, что когда температура достигает значения *x*, клапан *y* должен открыться, чтобы позволить воде поступать в сосуд.

Примечание 2 – Вторая часть определения означает, что функции безопасности могут быть выполнены системами, связанными с безопасностью, со степенью доверия (достоверности), соответствующей применению.

Человек может быть рассмотрен как составная часть Э/Э/ЭП системы, связанной с безопасностью. Например, человек может получить информацию о состоянии ОПУ на экране дисплея и предпринять действия, основанные на этой информации.

Э/Э/ЭП системы, связанные с безопасностью, могут работать в режиме низкой частоты запросов (обращений), высокой частоты запросов и в режиме непрерывных запросов.

3. Полнота безопасности

Полнота безопасности определяется как вероятность удовлетворительного выполнения требуемых функций безопасности при всех установленных условиях в течение установленного периода времени. Полнота безопасности относится к работе системы при выполнении функций безопасности (функций безопасности, подлежащие выполнению, должны быть определены в спецификации требований к функциям безопасности).

Рассматриваемая полнота безопасности содержит два элемента.

- *Аппаратная полнота безопасности.* Эта часть полноты безопасности относится к случайным отказам в опасном режиме отказов. Достижение определенного уровня полноты безопасности аппаратной части, относящейся к безопасности, может быть оценено с приемлемым уровнем точности, и требования, таким образом, могут быть распределены между подсистемами с использованием обычных правил для комбинации вероятностей. Может оказаться, что для достижения достаточной полноты безопасности необходимо использовать избыточную архитектуру.

- *Систематическая полнота безопасности.* Эта часть полноты безопасности относится к систематическим отказам в опасном режиме отказов. Несмотря на то, что средняя частота отказов, вносящих вклад в систематические отказы, может быть оценена, информация об отказах, получаемая из анализа отказов и общих случаев отказов, означает, что распределение отказов может оказаться трудным предсказуемым. Это вносит неопределенность в расчеты вероятности отказов для специфической ситуации (например, вероятности отказов системы защиты, относящейся к безопасности). Таким образом, целесообразно выбрать другой метод для минимизации этой неопределенности. Заметим, что нет необходимости доказывать, что меры по снижению вероятности случайных отказов долж-

ны соответственно влиять на вероятность систематических отказов. Такие технические средства, как избыточные каналы идентичных аппаратных средств, имеют большое влияние на случайные отказы управляющих (управляемых) аппаратных средств.

Требуемая полнота безопасности Э/Э/ЭП систем, связанных с безопасностью, систем, связанных с безопасностью, действующих на основе других технологий, и внешних средств снижения риска должна иметь такой уровень, чтобы гарантировать

- достаточно низкую частоту отказов систем, связанных с безопасностью, для предотвращения приводящего к ущербу события, которая необходима для достижения допустимого риска, и/или
- преобразование последствий отказов систем, связанных с безопасностью, до пределов, необходимых для достижения допустимого риска.

Рисунок 1 иллюстрирует основную концепцию снижения риска. Основная модель предполагает, что

- имеется ОПУ и система управления ОПУ;
- учтено влияние человеческого фактора;
- защитные средства безопасности включают:

внешние средства сокращения риска,

Э/Э/ЭП системы, связанные с безопасностью,

средства, связанные с безопасностью, основанные на других технологиях.

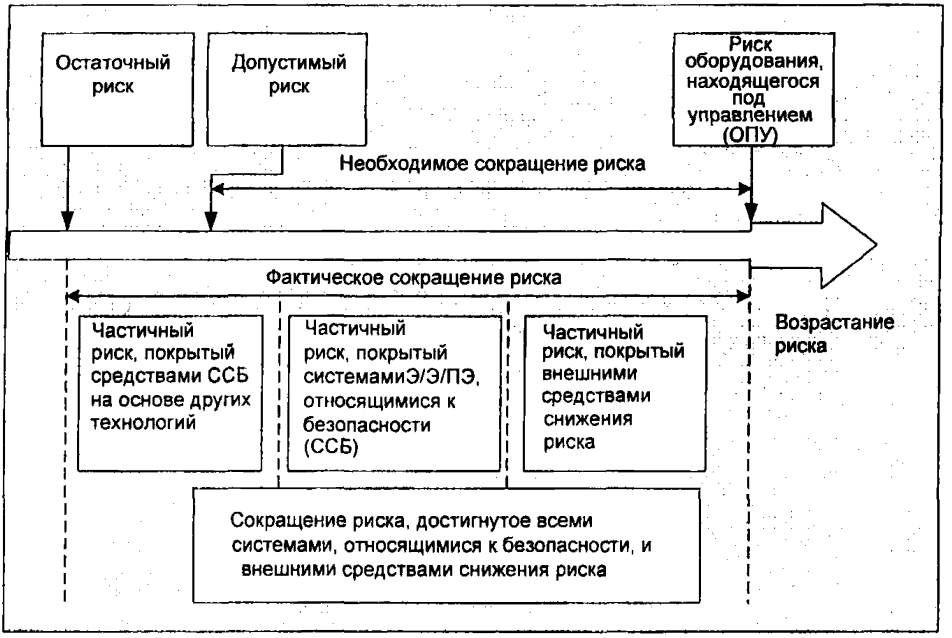


Рис. 1. Сокращение риска: основная концепция.

Примечание – На рисунке 1 изображена обобщенная модель для иллюстрации общих принципов. Модель риска для конкретных применений нуждается в развитии с учетом специфических условий (специфического поведения, способов, действий) при которых реально достигается допустимый риск с помощью Э/Э/ЭП систем, связанных с безопасностью, систем, связанных с безопасностью, основанных на других технологиях, внешних средств снижения риска. Таким образом, результирующая модель может отличаться от модели, изображенной на рис. 1.

На рис. 1. обозначены следующие риски:

- риск ОПУ: имеющийся для определенных опасных событий для ОПУ, системы управления ОПУ и дополнительного человеческого фактора – при определении этого риска не учитываются никакие разработанные защитные меры;

- допустимый риск: риск, который приемлем в данном контексте на основе текущего состояния развития общества;

- остаточный риск: в контексте стандарта – это такой риск, который остается для определенных приводящих к ущербу событий для ОПУ, систем управления ОПУ, с учетом влияния человеческого фактора, но с добавлением внешних средств снижения риска, Э/Э/ЭП систем, связанных с безопасностью, систем, связанных с безопасностью, основанных на других технологиях.

Риск ОПУ является функцией риска, связанной с собственно ОПУ, но с учетом уменьшения риска, достигаемого с помощью системы управления ОПУ. Для предотвращения необоснованных требований стандарты, упомянутые в пункте 1 настоящего приложения, содержит ограничения на такие требования.

Необходимое снижение риска достигается с помощью комбинации всех защитных средств безопасности. На рис.1 показано необходимое снижение риска для достижения определенного допустимого риска, начиная от начальной точки риска ОПУ.

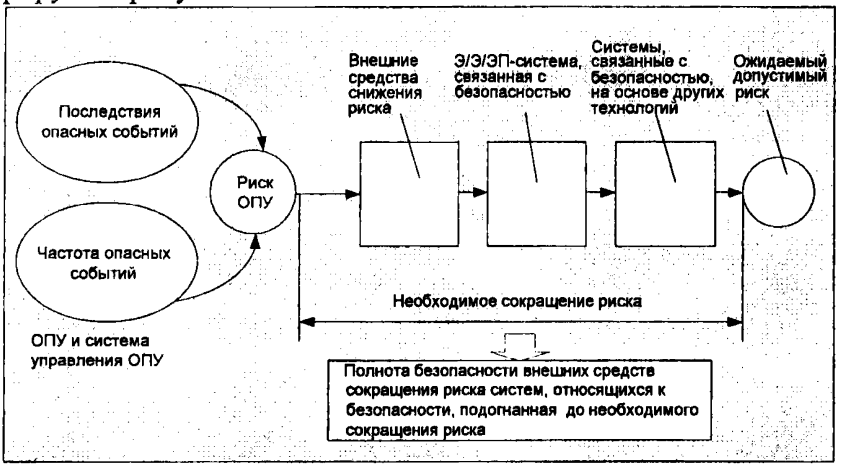
4. Риск и полнота безопасности

Различия между риском и полнотой безопасности следующие. Риск – это мера вероятности и последствий определенного случающегося приводящего к ущербу события. Он может быть оценен для различных ситуаций (риск ОПУ, риск, требуемый для достижения допустимого риска, фактический риск (см. рис. 1)). Допустимый риск определяется на социальной основе с учетом социальных и политических факторов. Полнота безопасности относится исключительно к Э/Э/ЭП системам, связанным с безопасностью, системам, связанным с безопасностью, основанным на других технологиях, и вешним средствам снижения риска. Она является мерой вероятности удовлетворительного достижения этими системами и средствами необходимого сокращения риска при реализации определенных (заданных) функций безопасности. Однажды уста-

новленный допустимый риск и оцененное необходимое сокращение риска позволяют распределить требования к полноте безопасности систем, связанных с безопасностью.

Примечание – Распределение требует итеративности для оптимизации разработки в целях удовлетворения различных требований.

Роль, которую играют системы, связанные с безопасностью, в достижении необходимого сокращения риска, иллюстрируется рисунками 1 и 2.



Примечание 1 – Требования полноты безопасности связываются с каждой функцией безопасности до распределения.

Примечание 2 – Функция безопасности может быть распределена на более чем одну систему, связанную с безопасностью.

Рис. 2. Риск и концепция полноты безопасности.

В настоящем стандарте для каждой из групп («L» и «H») определено четыре уровня полноты безопасности (см. раздел 7 настоящего стандарта), где уровень полноты безопасности 4 является наивысшим уровнем, а уровень полноты безопасности 1 – наинизшим уровнем.

В таблицах 1 и 2 статьи раздела 7 настоящего стандарта определены ожидаемые (планируемые) диапазоны величины

отказов для четырех уровней полноты безопасности в группах «L» и «H». Одни системы действуют в режиме низкой частоты обращения к системам «L» (от английского Low), а другие – в режиме высокой частоты обращений «H» (от английского High) или непрерывных обращений.

Примечание – Для систем, связанных с безопасностью, действующих в режиме низкой частоты обращения, в отношении величины полноты безопасности представляет интерес вероятность отказов при выполнении функций безопасности по запросам. Для систем, действующих в режиме высокой частоты обращения (запросов) или систем с непрерывными обращениями (запросами), в качестве величины полноты безопасности представляет интерес среднее число отказов в час.

6. Распределение требований безопасности

Распределение требований безопасности (как требований к функциям безопасности, так и требований к полноте безопасности), предъявляемых к Э/Э/ЭП системам, связанным с безопасностью, системам, связанным с безопасностью, действующим на основе других технологий, и внешним средствам снижения риска показано на рис. 3.

Методы, используемые для распределения требований полноты безопасности по Э/Э/ЭП системам, связанным с безопасностью, системам, действующим на основе других технологий, и внешним средствам снижения риска, изначально зависят от того, в какой форме требуется однозначно определять необходимое сокращение риска – в количественной форме или в качественной форме. Эти подходы названы количественным и качественным методами, соответственно (см. приложения 6, 7, 8 и 9).

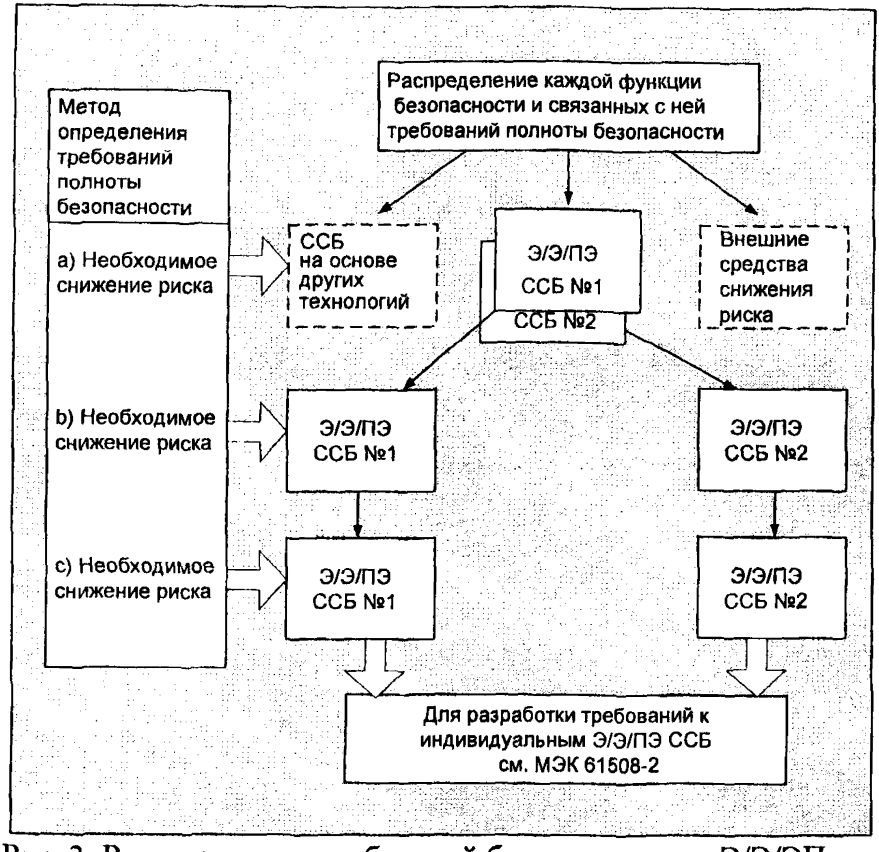


Рис. 3. Распределение требований безопасности по Э/Э/ЭП системам, связанным с безопасностью (ССБ), ССБ на основе других технологий и внешних средств снижения риска.

ПРИЛОЖЕНИЕ 6

КОНЦЕПЦИЯ РАЗУМНОЙ ДОСТАТОЧНОСТИ И ДОПУСТИМОГО РИСКА

1. Модель разумной достаточности

1.1. Основные тесты, которые применяют при управлении промышленными рисками, могут показывать, что в результате деятельности:

a) риск является настолько большим, что его нужно совершенно отвергнуть, или

b) риск является, или был сделан настолько малым, что его не следует принимать во внимание, или

c) риск попадает между двумя позициями, указанными выше в (a) и (d) и уменьшен до самого низкого реального уровня, с учетом полученных от этого выгод и учетом затрат на любое дальнейшее его сокращение.

Принцип разумной достаточности (c) требует, чтобы любой риск был уменьшен настолько, насколько это реально разумно, либо был приведен к уровню, который является столь же низким, как и реально разумный. Если риск попадает в зону между этими двумя границами, (то есть зоной недопустимого риска, и зоной вполне приемлемого риска), и применяется принцип разумной достаточности, то остаточный риск является допустимым для данного конкретного применения. Этот трехзонный подход показан на рис. 1.

Выше некоторого уровня риск расценивается, как недопустимый риск и не может быть оправдан ни при каких обычных обстоятельствах.

Ниже этого уровня имеется зона допустимого риска, где допускается деятельность, если относящиеся к ней риски сделаны настолько низкими, насколько это реально разумно. Допустимый риск отличается от приемлемого риска: он указывает готовность жить с риском, чтобы обеспечить некоторые выгоды, в то же самое время надеясь на то, что риск будет нахо-

диться под наблюдением и будет уменьшен, как только это станет возможным. Здесь требуется явная или неявная оценка стоимости выгоды для взвешивания стоимости и необходимости мер по обеспечению безопасности. Чем выше риск, тем пропорционально больше ожидаемые затраты для его уменьшения. В пределе допустимости, расходы будут непропорционально большими, чтобы выгода была оправдана. В этом случае риск должен быть существенным по определению, чтобы значительные усилия, потраченные для достижения крайнего его сокращения, были бы объективно оправданы.

В нижней части зоны допустимости риска, где риски меньше существенных, пропорционально уменьшается потребность в затратах на его сокращение, и удовлетворяется баланс между затратами и выгодой.

Ниже зоны допустимости риска, уровни риска расцениваются как настолько незначительные, что тот, кто управляет рисками, не должен добиваться дальнейшего его снижения.

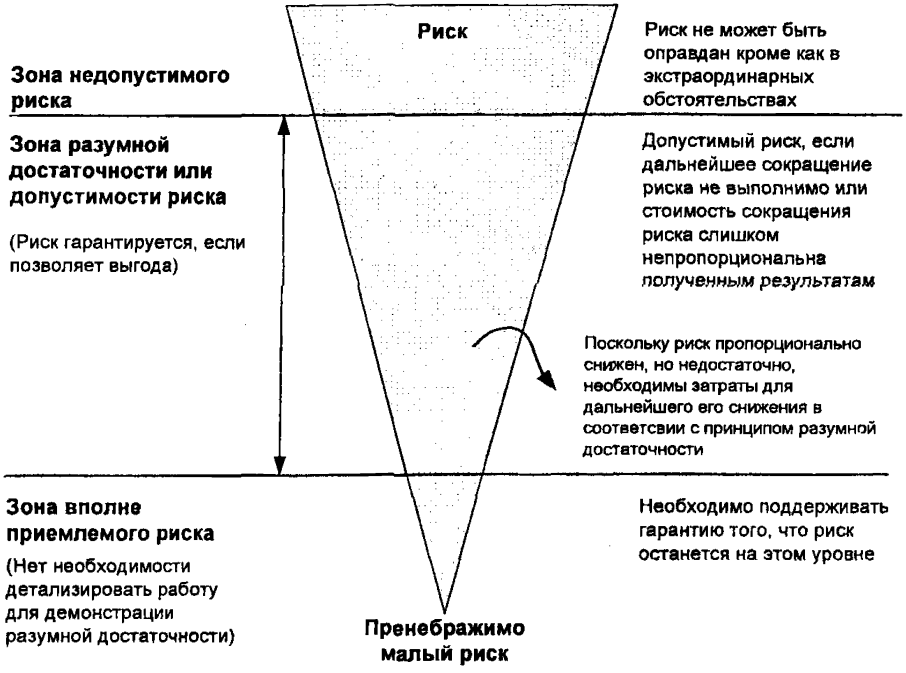


Рис. 1. Допустимый риск и разумная достаточность.

Это – область вполне приемлемого риска, где риски малы по сравнению с каждодневными рисками, которые все мы испытываем. Хотя в области вполне приемлемого риска нет никакой необходимости в доказательстве разумной достаточности, следует, однако, внимательно следить за тем, чтобы риск оставался на этом уровне.

2. Планирование допустимого риска

Один из путей получения плана риска состоит в определении для ряда последствий распределения частот, которые соответствуют присущим им допустимым рискам. Приведение в соответствие последствий и допустимых частот должно быть предметом обсуждений и соглашений между заинтересованными сторонами (например, органами власти, осуществляющими регулирование в области безопасности, теми, кто

производит риск (например, владельцами химических предприятий), и теми, кто подвергается риску (людьми, обществом, общественной организацией, представляющей их интересы). В соответствии с настоящим стандартом согласованные значения допустимых рисков определяет Комиссии по допустимым уровням комплексной безопасности.

Принимая во внимание концепцию разумной достаточности (разумной реальности), соответствие между последствиями и частотами может быть дано в виде классов риска. В таблице 1 в качестве примера показано четыре класса рисков (I, II, III и IV) для ряда последствий и частот. В таблице 2 приведена интерпретация каждого из классов риска с использованием концепции разумной достаточности. То есть, дано описание каждого из четырех классов риска на основании рис. 1. Риски в рамках определений этих классов рисков являются рисками после принятия мер по их снижению. В соответствии с рис. 1 имеются следующие классы рисков:

- риск класса I находится в зоне недопустимого риска;
- риски классов II и III лежат в зоне разумной достаточности, причем риск класса II находится у самой границы зоны разумной достаточности (разумной реальности);
- риск класса IV находится в зоне вполне приемлемого риска.

Для каждой определенной ситуации или сопоставимой отрасли промышленности, либо строительных объектов могли бы быть разработаны таблицы, подобные таблице 1, с учетом социальных, политических и экономических и иных факторов. Каждому последствию должна бы быть поставлена в соответствие частота, и таблица была бы заполнена классами риска. Например, частота в таблице 1 могла бы обозначать частоту события (которое считается возможным на основании продолжительного опыта), которая могла бы быть заданной, как частота больше, чем 10 раз в год. Критическим последствием

могла бы быть смерть одного человека и/или многочисленные серьезные повреждения, либо несколько профессиональных заболеваний.

Таблица 1 – Пример классификации рисков опасных событий (несчастных случаев, аварий, катастроф)

Частота опасных событий	Последствия			
	Катастрофические	Критические	Крайне малые	Несущественные
Частые	I	I	I	II
Возможные	I	I	II	III
Редкие	I	II	III	III
Отдельные	II	III	III	IV
Маловероятные	III	III	IV	IV
Невозможные	IV	IV	IV	IV

Примечание 1 – Реальное заполнение таблицы классами рисков I, II, III и IV должно зависеть от зоны, а также от того, какая реальная частота их появления, от вероятности и т.п. Следовательно, эта таблица скорее должна рассматриваться как пример того, как таблица должна заполняться, а не как спецификация для дальнейшего применения.

Примечание 2 – Определение уровней полноты безопасности для позиций, встречающихся в таблице, кратко описано в приложении 6.

Таблица 2 – Интерпретация классов риска

Класс риска	Интерпретация
Класс I	Недопустимый риск
Класс II	Нежелательный риск, и допустимый только, если снижение риска не осуществимо или если затраты чрезвычайно непропорциональны полученному выигрышу
Класс III	Допустимый риск, если затраты на снижение риска не превышают полученную выгоду
Класс IV	Пренебрежимо малый риск

ПРИЛОЖЕНИЕ 7

КОЛИЧЕСТВЕННЫЙ МЕТОД ОПРЕДЕЛЕНИЯ ПОЛНОТЫ БЕЗОПАСНОСТИ

1. Условия применения

Количественный метод удобно применять, когда:

- допустимый риск может быть определен в численной форме (например, определенное последствие не должно произойти чаще, чем один раз в 10^4 лет);

- заданы численные планируемые (ожидаемые) значения полноты безопасности для систем, связанных с безопасностью.

Метод, в частности, применим, когда модель риска соответствует моделям, показанным на рис. 1 и 2 приложения 5 к настоящему стандарту.

2.Общий метод

Модель, используемая для иллюстрации общих принципов, показана на рис. 1 приложения 5. Ключевые шаги в методе, которые должны быть выполнены для каждой функции безопасности, которая будет выполняться Э/Э/ЭП системой, связанной с безопасностью, следующие:

- определение допустимого риска из таблицы, такой как табл. 1 приложения 6;

- определение риска оборудования, находящегося под управлением (ОПУ);

- определение необходимого снижения риска для достижения допустимого риска;

- распределение необходимого снижения риска по Э/Э/ЭП системам, связанным с безопасностью, системам, связанным с безопасностью, основанным на других технологиях, и внешним средствам снижения риска.

Таблица 1 приложения 6 к настоящему стандарту, заполненная частотами возникновения риска, позволяет определить планируемый (ожидаемый) допустимый риск (F_t).

Частота, связанная с риском, который существует для ОПУ, включая систему управления ОПУ и человеческий фактор (риск ОПУ), в отсутствие любых защитных мер, может быть оценена с использованием численных методов оценки риска. Это частота, с которой может происходить опасное событие в отсутствие защитных мер ($F_{пр}$), - является одним из двух компонентов риска ОПУ. Другой компонент риска – последствие опасного случая. $F_{пр}$ - может быть определен с помощью

- анализа частоты (коэффициента) отказов в сопоставимых ситуациях;
- данных из уместных баз данных;
- расчетов с применением соответствующих методов прогноза.

Стандарты, указанные в приложении 5 к настоящему стандарту, содержат ограничения на минимальные частоты отказов, которые могут потребоваться для систем управления ОПУ. Если требуется, чтобы система управления ОПУ имела частоту отказов меньшую, чем минимальная частота отказов, то система управления ОПУ будет рассматриваться как система, связанная с безопасностью, и на нее будут распространяться все требования настоящего стандарта для систем, связанных с безопасностью.

3. Пример расчета

На рис. 1 показан пример расчета планируемой (ожидаемой) полноты безопасности для одиночной системы, связанной с безопасностью. Для этой ситуации

$PFD_{avg} \leq F_t / F_{пр}$,

где

PFD_{avg} - средняя вероятность отказа по требованию (по обращению) защитной системы (системы защиты), связанной с безопасностью, работающей в режиме низкой частоты обращений (см. раздел настоящего 7 стандарта);

F_t - частота допустимого риска;

$F_{пр}$ - частота риска при наличии защитных мер.

Можно заметить, что определение $F_{пр}$ для ОПУ важно из-за его отношения к PFD_{avg} и, следовательно, к уровню полноты безопасности системы, связанной с безопасностью.

Необходимые шаги в получении уровня полноты безопасности (когда последствия С остаются постоянными, как на рис. 1) для ситуации, где полное необходимое сокращение риска достигнуто единственной системой защиты, связанной с безопасностью, которая должна уменьшить частоту опасных событий, как минимум, с $F_{пр}$ до F_t, следующие:

- определение частоты событий риска без каких-либо дополнительных защитных мер ($F_{пр}$);

- определение последствий С без добавления каких-либо дополнительных мер безопасности;

- определение (с использованием табл. 1 приложения 6), достигнут ли для частоты $F_{пр}$ и последствий С допустимый риск. Если на основании таблицы 1 это приводит к риску класса I, то требуется дальнейшее сокращение риска. Риски классов IV или III были бы допустимыми рисками. Риск класса II потребовал бы дополнительного изучения;

Примечание – Таблица 1 приложения 6 используется для проверки, требуются ли или нет дальнейшие меры по снижению риска до тех пор, пока не окажется возможным достижение допустимого риска без каких-либо дополнительных защитных мер.

- определение вероятности отказа по запросу (отказа по требованию) для системы защиты, связанной с безопасностью, (PFD_{avg}) для достижения необходимого сокращения риска (ΔR). Для постоянных последствий в определенной описанной ситуации, $PFD_{avg} = (F_t / F_{пр}) = \Delta R$;

- для $PFD_{avg} = (F_t / F_{пр})$ уровень полноты безопасности может быть получен из таблицы 2, приведенной в разделе 7 настоящего стандарта (например, для $PFD_{avg} = 10^{-2} - 10^{-3}$, уровень полноты безопасности равен 2).

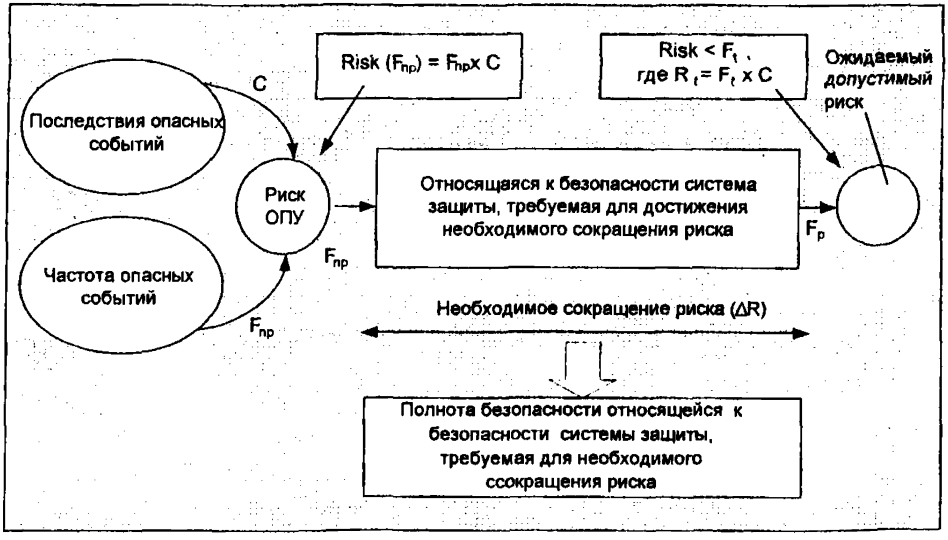


Рис. 1. Распределение полноты безопасности: пример системы защиты, относящейся к безопасности

ПРИЛОЖЕНИЕ 8

КАЧЕСТВЕННЫЙ МЕТОД ОПРЕДЕЛЕНИЯ ПОЛНОТЫ БЕЗОПАСНОСТИ – МЕТОД ГРАФА РИСКА

1. Условия применения

Настоящее приложение описывает графический метод оценки риска (метод графа риска), который является качественным методом, и который позволяет определить уровень полноты безопасности системы, относящейся к безопасности, исходя из знаний факторов риска, связанных с ОПУ и системой управления ОПУ. Его удобно применять, когда модель риска такая, как показано на рис. 1 и 2 приложения 5.

В случаях, когда для упрощения рассмотрения вопросов безопасности принимают качественный подход, вводят ряд параметров, которые вместе описывают природу опасной ситуации, когда система, связанная с безопасностью, отказывает или находится вне доступа. Из каждого из четырех наборов выбирают один параметр, и выбранные параметры затем объединяют, чтобы определить место положения систем, связанных с безопасностью. Эти параметры

- позволяют сделать градуировку рисков по значению и
- содержат ключевые факторы оценки риска.

2. Синтез графа риска

Нижеследующие упрощенные процедуры основаны на выражении

$R = f \times C$,

где

R - риск в отсутствие системы, связанной с безопасностью;

f - частота приводящего к ущербу события в отсутствие системы, связанной с безопасностью;

C - последствия приводящего к ущербу события (последствие должно быть отнесено к ущербу, связанному с здоровь-

ем и безопасностью или ущербом, нанесенным окружающей среде).

Частота приводящих к ущербу событий f в этом случае определяется тремя влияющими факторами

- частотой и временем пребывания в опасной зоне;
- вероятностью избежания приводящего к ущербу события;
- вероятностью наступления приводящего к ущербу события в отсутствие какой-либо системы, относящейся к безопасности, (но имеющей в наличии внешние средства снижения риска) – ее называют вероятностью нежелательного события.

Она производит четыре следующих параметра

- последствие приводящего к ущербу события (C);
- частоту и время подтверждения воздействию в опасной зоне (F);
- вероятность неудачи в избежании приводящего к ущербу события (P)
- вероятность нежелательного события (W).

3. Другие возможные параметры риска

Полагается, что определенные выше параметры риска являются в достаточной степени родовыми, чтобы их можно было распространять на широкий диапазон применений. Могут, однако, быть применения, которые требуют введения дополнительных параметров. Например, использование новых технологий (технических средств) в ОПУ и системах управления ОПУ. Назначение дополнительных параметров состояло бы в более точной оценке необходимого сокращения риска (см. рис. 1 приложения 5).

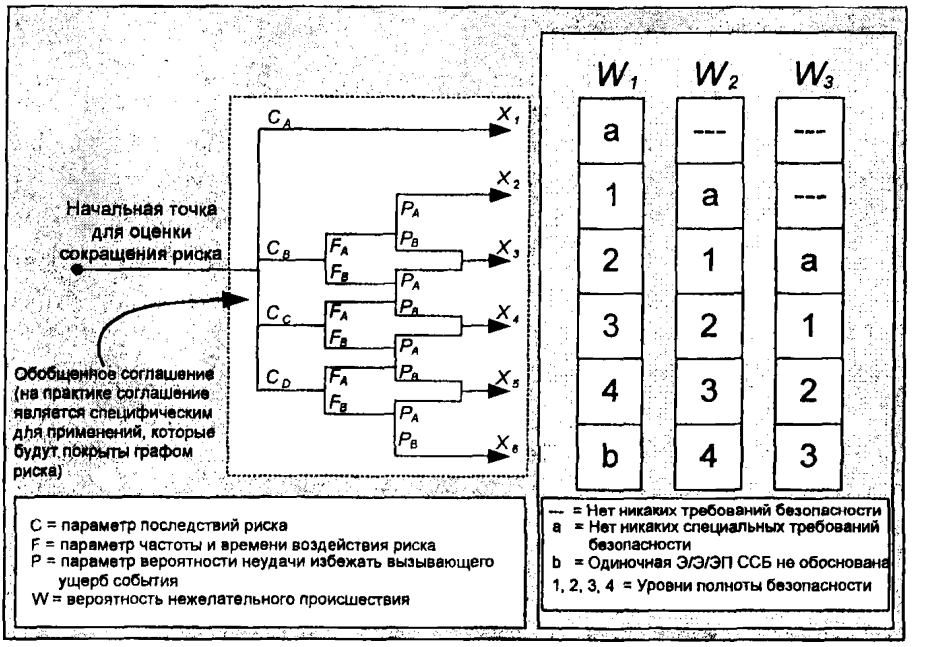


Рис. 1 – Граф риска: Общая схема

4. Выполнение графа риска

Комбинация параметров риска, описанных выше, позволяет получить граф риск в виде, показанном на рис. D.1: $C_A < C_B < C_C < C_D$; $F_A < F_B$; $P_A < P_B$; $W_1 < W_2 < W_3$. Толкование этого графа риска следующее:

- Использование параметров риска C, F и P приводит к ряду исходов X_1, X_2, X_3,... X_n (точное число зависит от области применения, чтобы быть покрытой графом риска). Рис D.1 показывает ситуацию, при которой не обеспечивается никакой дополнительный вклад для более серьезных последствий. Каждый из этих исходов отображается на одной из трех шкал (W_1, W_2 или W_3). Каждая точка этих шкал обозначает необходимую полноту безопасности, которая должна быть достигнута с помощью рассматриваемой Э/Э/ЭП системы, связанной с

безопасностью. На практике будут ситуации, когда для специфических последствий одиночная Э/Э/ЭП система, связанная с безопасностью, не позволит достичь необходимого снижения риска.

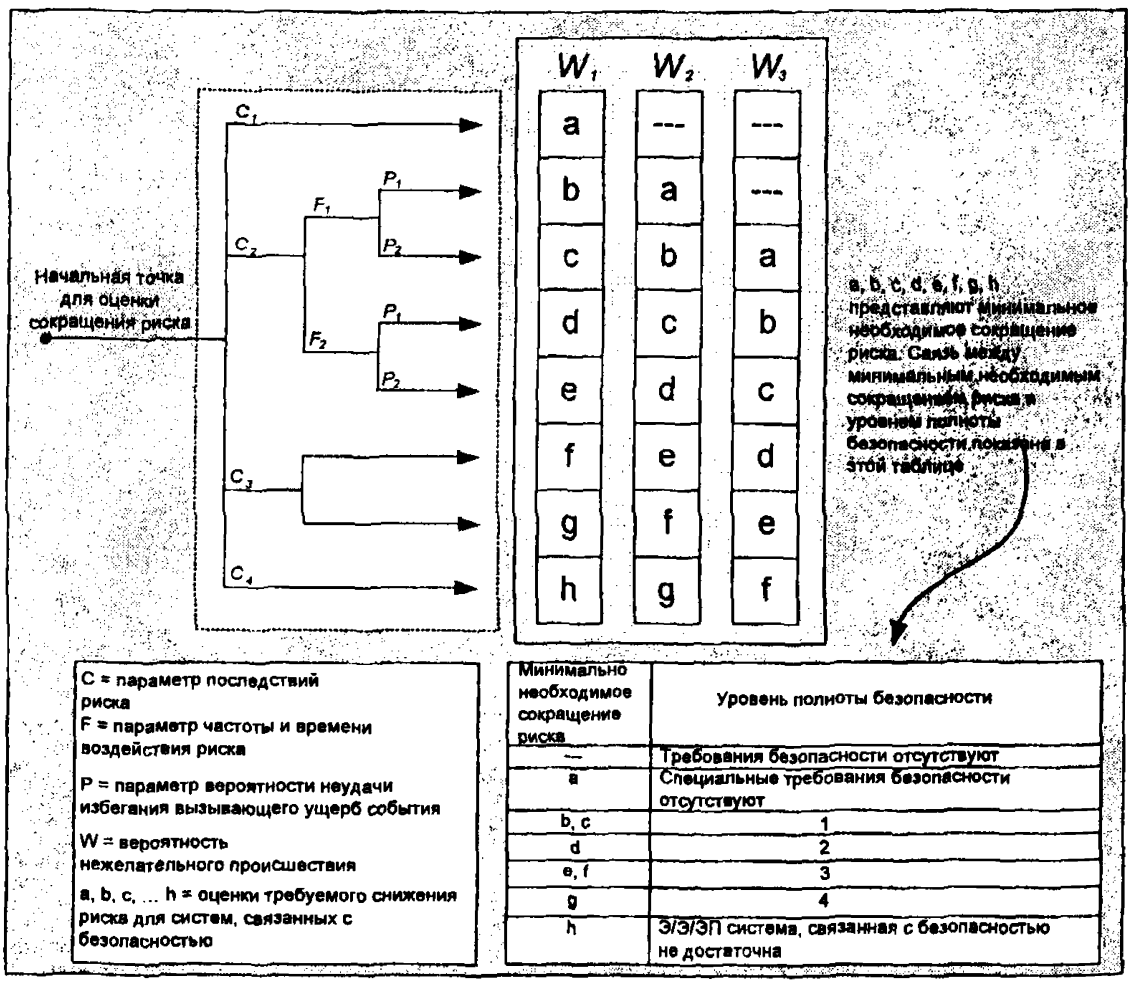
- Отображение на шкалах W_1, W_2 или W_3 позволяет ввести для использования другие меры снижения риска. То есть, шкала W_3 предусматривает минимальное снижение риска, внесенное другими средствами (то есть, самую высокую вероятность имеющего место нежелательного происшествия), шкала W_2 предусматривает средний вклад, и шкала W_1 – максимальный вклад. Для специфических промежуточных точек графа риска (например, X_1, X_2... или X_6) или для специфической шкалы W (например, W_1, W_2 или W_3) финальный выход (исход) графа риска дает уровень полноты безопасности Э/Э/ЭП системы, связанной с безопасностью (например, 1, 2, 3 или 4) и требуемые средства снижения риска для этой системы. Это снижение риска, вместе со снижением риска, достигаемым с помощью других мер (например, с помощью систем, связанных с безопасностью, основанных на других технологиях, и внешних средств снижения риска), которые принимаются в расчет с помощью механизма W-шкал, дает необходимое снижение риска для специфической ситуации.

Параметры, обозначенные на Рис. 1 (C_A, C_B, C_C, C_D, F_A, F_B, P_A, P_B, W_1, W_2, W_3), и их содержимое должны были бы точно определены для каждой конкретной ситуации или сопоставимой отрасли промышленности.

5. Пример графа риска

Выполнение графа риска, основанного на данных таблицы 1 приложения 6, показано на рис. 2. Использование параметров риска C, F, и P приводит к одному из восьми выходов (исходов). Каждый из этих выходов (исходов) обозначается на одной из трех шкал (W_1, W_2 и W_3). Каждая точка на этих шка-

лах (a, b, c, d, e, g и h) является обозначением необходимого сокращения риска, который должен быть достигнут системой, связанной с безопасностью.



Минимально необходимое сокращение риска	Уровень полноты безопасности
—	Требования безопасности отсутствуют
a	Специальные требования безопасности отсутствуют
b, c	1
d	2
e, f	3
g	4
h	Э/Э/ЭП система, связанная с безопасностью не достаточна

Рис. 2 – Граф риска: пример (иллюстрирует лишь основные принципы)

Таблица 1

Данные к примеру графа риска (рис. 2)

Параметр риска		Классификация	Комментарии
1	2	3	4
Последствия (С)	C_1 C_2 C_3 C_4	Несущественный ущерб Серьезный долговременный (permanent) ущерб одному лицу или большему числу лиц; Сметь одного лица, смерть нескольких лиц; Гибель очень большого числа людей	1 Система классификации была разработана для рассмотрения вопроса нанесения вреда здоровью и жизни людей. Для рассмотрения нанесения вреда окружающей среде или материального ущерба должны бы быть разработаны другие схемы классификации. 2 Для интерпретации C_1, C_2, C_3 и C_4 должны быть приняты во внимание катастрофа (несчастный случай) и нормальное спасение
Частота и время воздействия опасности в опасной зоне (F)	F_1 F_2	От редкого до более частого подтверждения опасности в опасной зоне Частое или непрерывное подтверждение опасности в опасной зоне	3 См. комментарий 1 (выше)
Вероятность избегания (избежания) опасного события (Р)	P_1 P_2	Возможно при некоторых условиях Почти невозможно	4 Этот параметр учитывает (принимает в расчет) - режим процесса (контролируемый (например, квалифицированным или неквалифицированным лицом) или неконтролируемый); - скорость развития приводящего к ущербу события (например, неожиданно, быстро или медленно);

			- легкость распознавания опасности (например, обнаруживается немедленно, обнаруживается техническими средствами или обнаруживается без технических средств); - избежание (избегание, уклонение от) опасного события (например, возможны запасные пути, не возможно или возможно при некоторых условиях); - имеющийся реальный опыт спасения (такой опыт может иметь место в идентичном ОПУ или похожем ОПУ, либо может отсутствовать)
Вероятность нежелательных происшествий (W)	W_1 W_2 W_3	Очень небольшая вероятность того, что нежелательное происшествие произойдет, и только несколько нежелательных происшествий возможно Небольшая вероятность того, что нежелательное происшествие произойдет, и несколько нежелательных происшествий возможно Относительно высокая вероятность того, что нежелательное происшествие произойдет, и возможны частые нежелательные происшествия	5 Назначение (цель) W-фактора состоит в приблизительной оценке частоты появления нежелательного происшествия без применения каких-либо систем, относящихся к безопасности (Э/Э/ЭП систем или систем, основанных на других технологиях), но с использованием любых внешних средств снижения риска. 6 Если имеется небольшой или отсутствует опыт применения ОПУ или систем управления ОПУ, либо подобных ОПУ и систем управления ОПУ, приблизительная оценка W-фактора может быть сделана путем расчета. В этом случае должен быть использован наихудший прогноз.

ПРИЛОЖЕНИЕ 9

КАЧЕСТВЕННЫЙ МЕТОД ОПАРЕДЕЛЕНИЯ ПОЛНОТЫ БЕЗОПАСНОСТИ – МАТРИЦА КРИТИЧНОСТИ СОБЫТИЙ

1. Условия применения

Численный (количественный) метод, описанный в приложении 6, не применим, когда риск (или частота его появления) не могут быть определены количественно. Настоящее приложение описывает метод матрицы серьезности (критичности) приводящих к ущербу событий, который относится к качественному методу и позволяет определить уровень полноты безопасности Э/Э/ЭП системы, связанной с безопасностью (ССБ), на основании знаний факторов риска, связанных с оборудованием, находящимся под управлением (ОПУ), и системой управления ОПУ. Он практически применим, когда модель риска такая, как показано на рис. 1 и 2 приложения 5.

Схема, приведенная в настоящем приложении, предполагает, что каждая система, связанная с безопасностью (ССБ), и внешние средства снижения риска являются независимыми.

2. Матрица серьезности (критичности) приводящих к ущербу событий

В основу матрицы положены следующие обязательные требования:

a) системы, связанные с безопасностью (ССБ), (Э/Э/ЭП или ССБ, основанные на других технологиях), вместе с внешними средствами снижения риска являются независимыми;

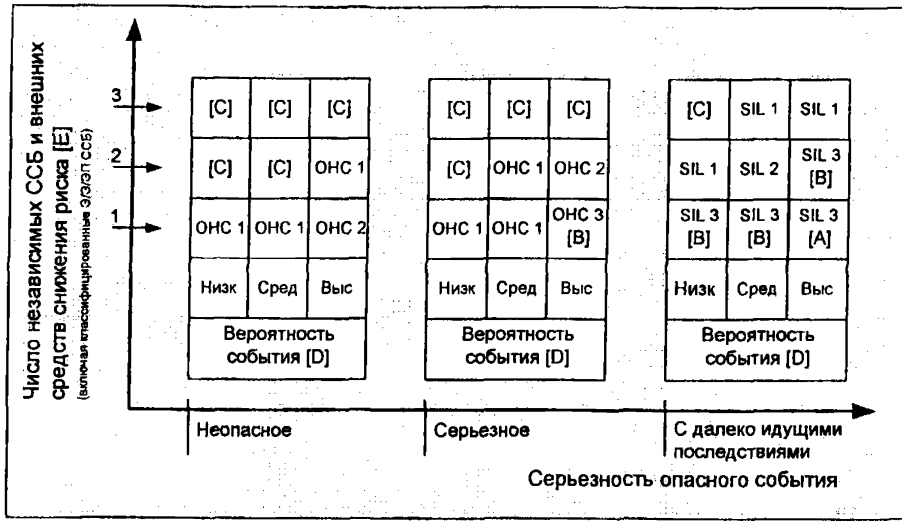
b) каждая система, связанная с безопасностью (Э/Э/ЭП или ССБ, основанная на другой технологии), вместе с внешними средствами снижения риска рассматриваются как слои защиты, которые обеспечивают по своим собственным правилам (возможностям) частичные сокращения риска, как показано на рис..1 приложения 5.

Примечание – Это допущение справедливо только, если выполняются регулярные контрольные испытания слоев защиты.

c) увеличение уровня полноты безопасности достигается тогда, когда добавляется один слой защиты (b), см. выше);

d) используется только одна Э/Э/ЭП система, связанная с безопасностью, (но она может быть объединена с системой, связанной с безопасностью, основанной на другой технологии, и/или с внешним средством снижения риска).

Приведенные выше рассуждения подводят к матрице серьезности приводящих к ущербу событий, показанной на рис. 1. Следует отметить, что матрица заполнена примерными данными для иллюстрации общих принципов. Для каждой конкретной ситуации или сектора сопоставимой отрасли промышленности может быть построена своя матрица, подобная матрице, изображенной на рис. 1.



[A] - Один одиночный независимый слой (ОНС) 3 Э/Э/ЭП ССБ не обеспечивает достаточное снижение риска на этом уровне риска. Требуется дополнительные меры сокращения риска.

[B] - Один ОНС 3 Э/Э/ЭП ССБ может не обеспечить достаточное снижение риска на этом уровне риска. Требуется анализ источников опасности и риска для определения, необходимы ли дополнительные меры сокращения риска.

[C] - Независимая Э/Э/ЭП система, связанная с безопасностью (ССБ), вероятно, не требуется.

[D] - Вероятность события – это вероятность того, что приводящие к ущербу события происходят в отсутствие каких-либо ССБ или внешних средств снижения риска.

[E] - ССБ = система, связанная с безопасностью. Вероятность события и общее число независимых слоев защиты определяется в соответствии со специфическим применением.

Рис. 1. Матрица серьезности приводящих к ущербу событий: *пример (иллюстрирует лишь основные принципы).*

Разработан и внесён:
Техническим комитетом по стандартизации Госстандарта Российской Федерации, ТК 439 «Средства автоматизации и системы управления»
Любимов М.М. – президент МА «Системсервис» - доктор технических наук, профессор; Матвеев В.Ф. – вице-президент ВАНКБ, доктор технических наук, профессор; Соломанидин Г.Г. – проректор по науке Университета КСБ и ИО, доктор технических наук, Щербина В.И. – проректор - заведующий кафедрой Университета КСБ и ИО, кандидат технических наук; Пузыревская Е.И. – главный эксперт Всемирной академии наук комплексной безопасности, Кокшин В.В. – директор Московского представительства «Аргус-спектр» кандидат технических наук, профессор; Антоненко А.А. – гл. специалист НПО «Мосспецавтоматика», кандидат технических наук, профессор

Издательство УКСБ и ИО

119602, г. Москва, ул. Академика Анохина, дом 30,
корп. 2, подъезд 3, офис 128
Тел.: (095) 735-6314, 430-1061, 430-2771, 203-9870
Факс: 437-9149; E-mail:info@systemservice.ru

Печать офсетная.
Тир. 1000 экз.

gost.e-ecolog.ru