ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 56205— 2014 IEC/TS 62443-1-1:2009

СЕТИ КОММУНИКАЦИОННЫЕ ПРОМЫШЛЕННЫЕ Защищенность (кибербезопасность) сети и системы

Часть 1-1 Терминология, концептуальные положения и модели

IEC/TS 62443-1-1:2009
Industrial communication networks — Network and system security — Part 1-1: Terminology, concepts and models
(IDT)

Издание официальное

Москва
Стандартинформ
2014

Предисловие

1 ПОДГОТОВЛЕН Негосударственным образовательным частным учреждением «Новая Инженерная Школа» (НОЧУ «НИШ») на основе аутентичного перевода на русский язык указанного в пункте 4 стандарта, который выполнен Российской комиссией экспертов МЭК/ТК 65, и Федеральным государственным унитарным предприятием «Всероссийский научно-исследовательский институт стандартизации и сертификации в машиностроении» (ВНИИНМАШ)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 306 «Измерение и управление промышленных процессах»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 10 ноября 2014 г. № 1493-ст

4 Настоящий стандарт идентичен международному документу IEC/TS 62443-1-1:2009 «Промышленные коммуникационные сети. Защищенность сети и системы. Часть 1-1. Терминология, концептуальные положения и модели» (IEC/TS 62443-1-1:2009, «Industrial communication networks — Network and system security — Part 1-1: Terminology, concepts and models»).

Перечень терминов, используемых в настоящем стандарте, приведен в дополнительном приложении ДА.

При применении настоящего стандарта рекомендуется использовать вместо ссылочных международных стандартов соответствующие им национальные стандарты, сведения о которых приведены в дополнительном приложении ДБ.

5 Некоторые элементы настоящего стандарта могут быть предметом патентных прав

6 ВВЕДЕН ВПЕРВЫЕ

Правила применения настоящего стандарта установлены в ГОСТ Р 1.0—2012 (раздел 8). Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (gost.ru)

© Стандартинформ, 2014

В Российской Федерации настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения 1
1.1 Общие положения 1
1.2 Включенная функциональность 1
1.3 Системы и интерфейсы 2
1.4 Критерии, основанные на действиях 2
1.5 Критерии, основанные на имущественных объектах 2
2 Нормативные ссылки 3
3 Термины, определения и сокращения 3
3.1 Общие сведения 3
3.2 Термины и определения 3
3.3 Сокращения 14
4 Ситуация 15
4.1 Общие положения 15
4.2 Существующие системы 15
4.3 Текущие тенденции 16
4.4 Потенциальные воздействия 17
5 Базовые концепции 17
5.1 Общие положения 17
5.2 Цели безопасности 17
5.3 Основные требования 18
5.4 Эшелонированная защита 19
5.5 Контекст безопасности 19
5.6 Оценка угроз и рисков 20
5.7 Степень завершенности программ безопасности 28
5.8 Политики безопасности 34
5.9 Зоны безопасности 39
5.9.2 Определение требований 40
5.10 Тракты 40
5.11 Уровни безопасности 42
5.12 Жизненный цикл уровня безопасности 46
6 Модели 50
6.1 Общие положения 50
6.2 Базовые модели 50
6.3 Объектные модели 54
6.4 Базовая архитектура 58
6.5 Зональная и трактовая модель 59
6.6 Взаимосвязи моделей 68
Приложение ДА (справочное) Алфавитный указатель терминов 70
Приложение ДБ (справочное) Сведения о соответствии ссылочных международных стандартов национальным стандартам Российской Федерации 73
Библиография 74

Введение

Международный стандарт МЭК 61443-1-1:2009 разработан Техническим комитетом МЭК 65 «Автоматизация, измерение и управление производственными процессами».

Объектом стандартизации настоящего стандарта является безопасность систем промышленной автоматики и контроля.

Понятие «системы промышленной автоматики и контроля» (IACS) охватывает системы управления, используемые на производственно-технологических предприятиях и установках, системы контроля климата в помещениях, управление в территориально рассредоточенных службах, такие как коммунальные ресурсы (т. е. электроэнергию, газ и воду), трубопроводы и объекты по производству и распределению нефти, и другие отрасли и задачи промышленности, такие как транспортные сети, в которых задействованы автоматизированные или дистанционно управляемые или отслеживаемые объекты имущества.

Под термином «безопасность» в настоящем стандарте понимается предотвращение незаконного или нежелательного проникновения, умышленного или неумышленного вмешательства в штатную и запланированную работу, или получения ненадлежащего доступа к конфиденциальной информации в IACS. Кибербезопасность, являющаяся частным объектом настоящего стандарта, распространяется на компьютеры, сети, операционные системы, приложения и другие программируемые конфигурируемые компоненты системы.

Пользователями настоящего стандарта являются: пользователи IACS (включая отделы эксплуатации установок, обслуживания, конструирования и корпоративные компоненты пользовательских организаций), производители, поставщики, правительственные организации, которые занимаются или которых затрагивает кибербезопасность систем управления, специалисты-практики по системам управления и специалисты-практики по безопасности.

Взаимопонимание и взаимодействие между информационно-техническими, эксплуатационными, конструкторскими и производственными организациями важны для общего успеха любой инициативы в сфере безопасности, поэтому настоящий стандарт является также справочным материалом для тех, кто отвечает за интеграцию IACS и корпоративных сетей.

Настоящий стандарт устанавливает:

a) область применения безопасности систем промышленной автоматики и контроля;

b) потребность и требования к системе безопасности, используя единую терминологию;

c) базовые концепции, составляющие основу для дальнейшего анализа процесссов, свойств систем, а также действий, необходимых для создания систем управления, надежных в плане электроники;

d) каким образом можно группировать или классифицировать компоненты системы промышленной автоматики и контроля в целях определения и управления безопасностью;

e) цели кибербезопасности для различных сфер применения систем управления;

f) определение и систематизацию кибербезопасности для различных сфер применения систем управления.

Каждый из этих вопросов подробно рассмотрен в разделах настоящего стандарта.

В наименование стандарта, в отличие от наименования IEC/TS 62443-1-1:2009 включено слово «кибербезопасность» с целью отражения содержания стандарта, в котором установлены требования к кибербезопасности и, соответственно, используется термин «кибербезопасность».

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

СЕТИ КОММУНИКАЦИОННЫЕ ПРОМЫШЛЕННЫЕ
Защищенность (кибербезопасность) сети и системы

Часть 1-1
Терминология, концептуальные положения и модели

Industrial communication networks. Network and system security. Part 1-1. Terminology, concepts and models

Дата введения — 2016—01—01

1 Область применения

1.1 Общие положения

Настоящий стандарт устанавливает терминологию, определяет концептуальные положения и модели применительно к безопасности систем промышленной автоматики и контроля (далее — IACS) и является основой для остальных стандартов серии МЭК 62443.

Чтобы четко сформулировать наименования всех систем и компонентов, рассматриваемых в стандартах серии МЭК 62443, область применения может быть определена и представлена на основе нескольких аспектов, в числе которых:

a) диапазон включенной функциональности;

b) специальные системы и интерфейсы;

c) критерии отбора включенных действий;

d) критерии отбора включенных имущественных объектов.

Каждый из этих аспектов рассмотрен в подразделах 1.2 —1.5.

1.2 Включенная функциональность

Предметная область применения настоящего стандарта может быть описана с позиции диапазона функциональности в пределах информационных и автоматизированных систем организации. Такую функциональность обычно описывают в контексте одной или более моделей.

Объектом настоящего стандарта является в первую очередь промышленная автоматика и контроль, как описано в базовой модели (см. раздел 6). В рамках настоящего стандарта системы бизнес-планирования и материально-технического обеспечения не рассматриваются, но определено понятие целостности данных, пересылаемых от бизнессистем к промышленным системам и наоборот.

Промышленная автоматика и контроль включают в себя элементы диспетчерского контроля, которые, как правило, встречаются в перерабатывающих отраслях промышленности. Они включают в себя и системы SCADA (системы диспетчерского контроля и сбора данных), которые обычно используются организациями, занятыми в отраслях инфраструктуры жизнеобеспечения. Такие отрасли включают в себя:

a) передачу и распределение электроэнергии;

b) сети распределения газа и воды;

c) добычу нефти и газа;

d) трубопроводы газа и жидкости.

Данный список неполный. Системы SCADA могут встречаться также в других критических и некритических отраслях инфраструктуры.

Издание официальное

1.3 Системы и интерфейсы

Настоящий стандарт применяется к IACS, которые могут влиять или воздействовать на безопасное, защищенное и надежное функционирование промышленных процессов. Такие системы включают в себя, как правило:

a) системы управления, используемые в промышленности, и ассоциированные с ними коммуникационные сети[1)], включая распределенные системы управления (DCS), программируемые логические контроллеры (PLC), пульты дистанционного управления (RTU), интеллектуальные электронные устройства, системы SCADA, объединенные системы электронного детектирования и контроля, системы учета и сдачи-приемки, а также системы мониторинга и диагностики. (В данном контексте промышленные системы управления наделены базовыми функциями систем управления процессами и автоматизированных систем безопасности (SIS), которые могут быть как физически отделены друг от друга, так и объединены друг с другом);

b) ассоциированные системы уровня 3 или ниже базовой модели, описанной в разделе 6. Например, системы упреждающего или многосвязного регулирования, оптимизаторы реального времени, специальные мониторы к оборудованию, графические интерфейсы, серверы-архиваторы, автоматизированные системы управления производственными процессами, системы обнаружения утечек из трубопроводов, системы управления производством работ, системы управления отключениями и системы управления электроэнергией;

c) ассоциированные внутренние, пользовательские, сетевые, программные, машинные или приборные интерфейсы, используемые для обеспечения управления, защиты и функциональности производственных или дистанционных операций в ходе непрерывных, периодических, дискретных и прочих процессов.

1.4 Критерии, основанные на действиях

Критерии для определения действий, относящихся к производственным операциям, установлены в МЭК 62443-2-1, аналогичный перечень критериев определен для настоящего стандарта. Систему следует считать подпадающей под область применения стандартов серии МЭК 62443, если действия, выполняемые системой, необходимы для достижения любой из следующих целей:

a) прогнозируемое функционирование процесса;
b) безопасность процессов или персонала;
c) надежность или доступность процессов;
d) эффективность процессов;
e) оперативность процессов;
f) качество продукции;
g) защищенность окружающей среды;
h) нормативно-правовое соответствие;
i) сбыт продукции или передача ее потребителю.

1.5 Критерии, основанные на имущественных объектах

Область применения настоящего стандарта включает в себя те системы среди имущественных объектов, которые удовлетворяют любым из следующих критериев или безопасность которых важна для защиты других имущественных объектов, удовлетворяющих этим критериям:

a) объект имеет хозяйственную ценность для процесса производства или эксплуатации;

b) объект выполняет функцию, необходимую для процесса производства или эксплуатации;

c) объект представляет собой интеллектуальную собственность, относящуюся к процессу производства или эксплуатации;

[1)] Понятие «коммуникационные сети» включает в себя все типы средств коммуникации, в том числе разного рода беспроводной коммуникации. Подробное описание использования беспроводной коммуникации в системах промышленной автоматики выходит за рамки настоящего стандарта. Технологии беспроводной коммуникации упоминаются особо лишь в случаях, если их использование или задействование может изменить характер действующей или требуемой безопасности.

d) объект необходим для осуществления и обеспечения безопасности процесса производства или эксплуатации;

e) объект необходим для защиты персонала, подрядчиков и посетителей, участвующих в процессе производства или эксплуатации;

f) объект необходим для защиты окружающей среды;

g) объект необходим для защиты населения от событий, спровоцированных процессом производства или эксплуатации;

h) объект представляет собой правовое требование, направленное, в частности, на обеспечение безопасности процесса производства или эксплуатации;

i) объект необходим для восстановления после чрезвычайных происшествий;

j) объект необходим для регистрации данных о событиях безопасности.

Область применения включает в себя системы, нарушение безопасности которых может поставить под угрозу здоровье или безопасность населения или работников, привести к потере доверия со стороны общественности, нарушению регламентных норм, утечке или потере достоверности служебной или конфиденциальной информации, загрязнению окружающей среды и/или экономическому ущербу, или отразиться на каком-либо субъекте или локальной/национальной безопасности.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты. Для недатированных ссылок применяют последнее издание ссылочного документа (включая любые изменения).

МЭК 62264-1 Интеграция систем управления предприятием. Часть 1. модели и терминология (IEC 62264-1, Enterprise-control system integration — Part 1: Models and terminology)

ИСО/МЭК 15408-1 Информационная техника. Технологии безопасности. Критерии оценки безопасности информационной техники. Часть 1. Введение и общая модель (ISO/IEC 15408-1, Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model)

3 Термины, определения и сокращения

3.1 Общие сведения

В настоящем стандарте часть определений заимствована из устоявшихся источников, относящихся к традиционным отраслям промышленности, а некоторые определения следуют из более общих определений, используемых в области информационных технологий.

Алфавитный перечень терминов приведен в приложении ДА.

3.2 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.2.1 **доступ** (access): Возможность и средства для обмена сообщениями или иного взаимодействия с системой в целях использования ресурсов системы.

Примечание — Доступ может предполагать физический доступ (физическая авторизация, предоставляемая для доступа в участок, наличие механического замка, ПИН-код, или карта доступа, или биометрические признаки, обеспечивающие доступ) или логический доступ (авторизация для входа в систему и программу, осуществляемая путем комбинации логических и физических средств).

3.2.2

управление доступом (access control): Защита ресурсов системы от неавторизованного доступа; процесс, при котором использование ресурсов системы регулируется политикой безопасности и разрешено только авторизованным субъектам (пользователям, программам, процессам или другим системам), авторизованным в соответствии с этой политикой.

[RFC 2828, изменен]

3.2.3 **отслеживаемость** (accountability): Свойство системы (в том числе всех ее ресурсов), позволяющее однозначно отследить действия какого-либо из субъектов в системе до субъекта, который мог быть ответственным за его действия.

3.2.4 **приложение** (application): Программа, которая осуществляет специальные действия, инициируемые командой пользователя или событием процесса, и может быть реализована без обращения к системному управлению и мониторингу или административным привилегиям системы.

3.2.5 **участок** (area): Подмножество физической, географической или логической группы имущественных объектов, расположенных на территории производственного объекта.

Примечание — Участок может содержать производственные линии, технологические ячейки и единицы оборудования. Участки могут быть соединены между собой локальной вычислительной сетью объекта и содержать системы, связанные с операциями, которые осуществляются на данном участке.

3.2.6 **имущественный объект** (объект) (asset): Физический или логический объект, который принадлежит организации или относится к ней иным способом, представляя для нее ощущаемую или реальную ценность.

Примечание — В случае систем промышленной автоматики и контроля физические объекты имущества, имеющие наибольшую ценность, измеримую непосредственно, представляют, например, оборудование, которым управляют.

3.2.7 **ассоциация** (association): Совместные отношения между субъектами системы, обычно в целях обмена информацией между ними.

3.2.8 **уверенность** (assurance): Свойство системы, обеспечивающее доверие к тому, что система работает таким образом, что обеспечивается выполнение ее политики безопасности.

3.2.9 **атака** (attack): Посягательство на систему, которое является следствием продуманного планирования, т. е. умышленного действия, представляющее собой продуманную попытку (особенно в плане метода или стратегии) обойти сервисы безопасности и нарушить политику безопасности системы [10].

Примечание – Существуют различные общепризнанные типы атак:

- «активная атака» имеет целью преобразовать ресурсы системы или воздействовать на ее работу;
- «пассивная атака» имеет целью заполучить или использовать информацию системы без воздействия на ресурсы системы;
- «внутренняя атака» — атака, инициированная субъектом в пределах периметра безопасности («инсайдером»), т. е. субъектом, который наделен правами на получение доступа к ресурсам системы, но использует их в целях, не одобренных теми, кто предоставил эти права;
- «внешняя атака» — атака, инициированная за пределами периметра безопасности неавторизованным или неуполномоченным пользователем системы (им может быть и инсайдер, атакующий за пределами периметра безопасности). Потенциальными злоумышленниками, осуществляющими внешнюю атаку, могут быть как простые любители пошутить, так и организованные преступные группы, международные террористы и враждебные правительства.

3.2.10 **схема атаки** (attack tree): Формальный методический путь нахождения способов нарушения безопасности системы.

3.2.11 **аудит** (audit): Независимое исследование и проверка записей и действий для оценки адекватности мер по управлению системой, обеспечения их соответствия установленным политикам и рабочим процедурам и подготовки рекомендаций к необходимым корректировкам управления, политик или процедур (см. 3.2.101).

Примечание – Существуют три формы аудита:

- внешние аудиты — проводятся сторонами, которые не являются сотрудниками или подрядчиками организации;
- внутренние аудиты — проводятся отдельной организационной единицей, которая специализируется на внутреннем аудите;
- самостоятельные проверки управления — проводятся сотрудниками организации, занимающими аналогичные должности в области автоматизации процессов.

3.2.12 **выполнять аутентификацию** (authenticate): Проверять идентификационную информацию пользователя, устройства на стороне пользователя или другого субъекта, или целостность дан-

ных, сохраняемых, передаваемых или подверженных иным образом риску несанкционированного преобразования в информационной системе, или устанавливать правомерность передачи данных.

3.2.13 **аутентификация** (authentication): Мера безопасности, запроектированная на установление правомерности передачи, самого сообщения, или его источника, а также средство проверки авторизационных данных индивидуального пользователя для получения определенных категорий информации.

3.2.14 **авторизация** (санкционирование, санкция, наделение правами, авторизационные данные) (authorization): Право или разрешение, предоставляемое субъекту системы для получения доступа к ресурсу системы [10].

3.2.15 **автоматизированный подвижный объект** (automated vehicle): Мобильное устройство, снабженное системой управления, которая обеспечивает его функционирование в автономном режиме или режиме дистанционного управления.

3.2.16 **доступность (работоспособность)** (availability): Способность компонента выполнить требуемое действие при заданных условиях в заданный момент времени или в продолжение заданного интервала времени, если предоставлены необходимые внешние ресурсы.

Примечание 1 — Эта способность зависит от следующих аспектов, рассматриваемых в совокупности: надежности, удобства сопровождения и качества технической поддержки.

Примечание 2 — Необходимые внешние ресурсы, отличные от ресурсов техниче ского обслуживания, не влияют на показатель доступности компонента.

Примечание 3 — Во французском языке используется также термин «disponibilité» в значении «текущая доступность».

3.2.17 **граница** (border): Предел или рамки физической или логической зоны безопасности.

3.2.18 **ботнет** (botnet): Совокупность программных роботов или ботов, которые функционируют автономно.

Примечание — Создатель ботнета может дистанционно управлять работой группы объектов, зачастую в неблаговидных целях.

3.2.19 **ограничение доступа** (boundary): Программный, аппаратный или другой физический барьер, который ограничивает доступ к системе или ее части.

3.2.20 **канал** (channel): Особая связная линия, созданная внутри связующего тракта (см. 3.2.27).

3.2.21 **криптограмма, (за)шифрованный текст** (ciphertext): Данные, преобразованные путем шифрования таким образом, чтобы их семантическая информация (т. е. смысл) была непонятна или непосредственно недоступна.

3.2.22 **клиент** (client): Устройство или приложение, получающие или запрашивающие сервисы или информацию с приложения сервера [11].

3.2.23 **коммуникационный путь** (communication path): Логическая связь между источником информации и одним или более адресатами, которыми могут быть устройства, физические процессы, элементы данных, команды или программные интерфейсы.

Примечание — Коммуникационный путь не сводится к проводным или беспроводным сетям и может включать в себя другие средства коммуникации, такие как обращения к памяти, вызовы процедур, структура материальной основы, портативные носители информации и взаимодействия между людьми.

3.2.24 **безопасность коммуникации** (communication security):

a) меры, реализующие и гарантирующие работоспособность сервисов безопасности в коммуникационной системе, в частности — сервисов, которые обеспечивают конфиденциальность и целостность данных, а также аутентификацию субъектов, участвующих в передаче информации.

b) режим, достигнутый за счет реализации сервисов безопасности, в частности — состояние конфиденциальности и целостности данных, а также успешной аутентификации субъектов, участвующих в передаче информации.

Примечание — Данное понятие обычно распространяется на криптографические алгоритмы, а также методы и процессы управления шифрованием, устройства для их реализации, и управление жизненным циклом шифруемого материала и средств шифрования. Однако криптографические алгоритмы, а также методы и процессы управления шифрованием, могут быть не применимы к некоторым приложениям систем управления.

3.2.25 **коммуникационная система** (communication system): Конфигурация аппаратного обеспечения, программного обеспечения и среды прохождения сигналов, обеспечивающая передачу информационных сообщений от одного приложения к другому [9].

3.2.26 **утечка информации** (compromise): Несанкционированное рассекречивание, изменение, замещение или использование информации (в том числе криптографических ключей к открытому тексту и других важнейших параметров безопасности) [12].

3.2.27 **тракт** (conduit): Логическое объединение коммуникационных объектов, обеспечивающее безопасность содержащихся в них каналов.

Примечание — Схожим образом механический кабелепровод защищает кабели от физического повреждения.

3.2.28 **конфиденциальность** (confidentiality): Гарантия того, что информация не будет раскрыта неавторизованным лицам, процессам или устройствам.

3.2.29 **центр управления** (control center): Центральный пункт управления группой имущественных объектов.

Примечание 1 — На предприятиях промышленной инфраструктуры обычно используется один или более центров управления для контроля или координации процессов, происходящих на предприятии. Если центров управления несколько (например, имеется резервный центр на отдельной территории объекта), то они, как правило, связаны между собой глобаль ной вычислительной сетью. Центр управления включает в себя систему диспетчерского контроля и сбора данных (SCADA), хосткомпьютеры и соответствующие средства отображения информации для операторов, а также вспомогательные информационные системы, такие как сервер архивных данных.

Примечание 2 — В некоторых отраслях промышленности может больше употребляться термин «пульт управления».

3.2.30 **управляющее оборудование** (control equipment): Класс оборудования, который включает в себя распределенные системы управления, программируемые логические контроллеры, системы SCADA, соответствующие пульты операторов, а также периферийные датчики и исполнительные механизмы, используемые для управления и регулирования процесса.

Примечание — Термин распространяется также на промышленные сети, где логика и алгоритмы управления реализованы на интеллектуальных электронных устройствах, координирующих операции между собой, а также на системы для мониторинга процесса и на системы, используемые для сопровождения процесса.

3.2.31 **управляющая сеть** (control network): Сеть с жестким временным режимом, которая обычно связана с оборудованием, управляющим физическим процессом (см. 3.2.97).

Примечание — Управляющая сеть может быть подразделена на зоны, при этом в одной организации или на одном объекте может быть множество отдельных управляющих сетей.

3.2.32 **издержки** (cost): Величина измеримых расходов для организации или лица.

3.2.33 **контрмера** (countermeasure): Действие, устройство, процедура или стратегия, которые ослабляют угрозу, уязвимость или противодействуют атаке путем ее отражения или предотвращения, или минимизации ущерба, который она

способна нанести, или путем ее обнаружения и сообщения о ней, чтобы могло быть предпринято корректирующее действие.

Примечание — В некоторых контекстах для описания этого понятия используется также термин «мера защиты» (control). Применительно к настоящему стандарту выбран термин «контрмера» во избежание путаницы с термином «управление» (control), относящимся к управлению процессами [10].

3.2.34 **криптографический алгоритм** (cryptographic algorithm): Алгоритм на базе науки криптографии, который может включать в себя алгоритмы шифрования, криптографические хеш-алгоритмы, алгоритмы цифровой подписи и алгоритмы распределения ключей.

3.2.35 **криптографический ключ** (cryptographic key): Входной параметр, который варьирует преобразование, выполненное криптографическим алгоритмом [10].

Примечание — Обычно употребляется сокращенный термин «ключ».

3.2.36 **кибербезопасность** (киберзащита) (cybersecurity): Действия, необходимые для предотвращения неавторизованного использования, отказа в обслуживании, преобразования, рассекречивания, потери прибыли, или повреждения критических систем или информационных объектов.

Примечание — Цель при этом — уменьшить персональный риск травмирования или риск угрозы здоровью населения, риск потери доверия общественности или потребителей, разглашения информации о важных объектах, незащищенности бизнес-объектов или несоответствия нормативам. Эти понятия применимы к

любой системе в производственном процессе, которая может включать в себя как независимые, так и связанные компоненты. Коммуникация между системами может осуществляться либо с помощью внутренних сообщений, либо через любые пользовательские или машинные интерфейсы, которые обеспечивают аутентификацию, работу, управление или обмен данными с любой из таких систем управления. Кибербезопасность включает в себя понятия идентификации, аутентификации, отслеживаемости, авторизации, доступности и приватности.

3.2.37 **конфиденциальность данных** (data confidentiality): Свойство, гарантирующее, что информация не стала доступна или раскрыта любым неавторизованным субъектам системы, включая неавторизованных лиц, структуры или процессы.

3.2.38 **целостность данных** (data integrity): Свойство, гарантирующее, что данные не были изменены, уничтожены или потеряны из-за несанкционированных действий или случайно.

Примечание — Термин затрагивает неизменность и конфиденциальность значений данных, но не информацию, которую отражают эти значения, и ненадежность источника значений.

3.2.39 **расшифровка** (decryption): Процесс преобразования зашифрованного текста в открытый текст с помощью криптографического алгоритма и ключа (см. 3.2.47) [10].

3.2.40 **эшелонированная защита** (defence in depth): Наличие множественной защиты, в частности — в виде уровней, с целью предотвращения или хотя бы сдерживания атаки.

Примечание — Эшелонированная защита предполагает наличие уровней защиты и обнаружения угроз даже на обособленных системах и обладает следующими признаками:

- злоумышленники сталкиваются с проблемой незаметного прохождения или обхождения каждого уровня;
- дефект на одном уровне может быть ослаблен возможностями других уровней;
- безопасность системы сводится к набору уровней, которые определяют также общую безопасность сети.

3.2.41 **демилитаризованная зона** (demilitarized zone): Периферический сегмент сети, который логически вставлен между внутренней и внешней сетями.

Примечание 1 — Функция демилитаризованной зоны — навязать политику безопасности внутренней сети в отношении внешнего обмена информацией и предоставлять внешним ненадежным источникам ограниченный доступ к информации, предполагающей ее раскрытие, одновременно защищая внутреннюю сеть от внешних атак.

Примечание 2 — В контексте систем промышленной автоматики и контроля термин «внутренняя сеть» обычно относится к сети или ее сегменту, которые составляют главный объект защиты. Например, управляющая сеть может считаться внутренней, если она соединена с внешней деловой сетью.

3.2.42 **отказ в обслуживании** (denial of service): Предотвращение или прерывание авторизованного доступа к ресурсу системы или задержка в действиях или функциях системы.

Примечание — В контексте систем промышленной автоматики и контроля отказ в обслуживании может относиться к прекращению функционирования процесса, а не только к прекращению передачи данных.

3.2.43 **цифровая подпись** (digital signature): Результат криптографического преобразования данных, который, при условии правильной реализации этого преобразования, предоставляет сервисы аутентификации источника, целостности данных и гарантию сохранения авторства подписавшегося.

3.2.44 **распределенная система управления** (distributed control system): Тип системы управления, в которой элементы системы рассредоточены, но работают взаимосвязанно.

Примечание 1 — Распределенные системы управления обычно характеризуются меньшими значениями констант времени связывания, чем системы SCADA.

Примечание 2 — Распределенные системы управления обычно привязаны и к непрерывным процессам, таким как выработка электроэнергии, очистка нефти и газа, химическое, фармацевтическое и бумажное производство, так и дискретным процессам, таким как производство автомобилей и прочих изделий, упаковка и складирование.

3.2.45 **домен** (domain): Среда или контекст, которые определены политикой безопасности, моделью безопасности или архитектурой безопасности и могут включать в себя группу ресурсов системы и группу субъектов, имеющих право на доступ к ресурсам.

3.2.46 **несанкционированное извлечение информации** (eavesdropping): Просмотр или фиксация переданной информации неавторизованными участниками.

3.2.47 **шифрование** (encryption): Криптографическое преобразование открытого текста в зашифрованный текст, который скрывает исходный смысл данных во избежание разглашения факта их существования или использования (см. 3.2.39).

Примечание — Если такое преобразование обратимо, то соответствующий обратный процесс называется «расшифровкой», при этом зашифрованные данные восстанавливаются до исходного состояния.

3.2.48 **предприятие** (enterprise): Субъект хозяйствования, который производит или транспортирует продукцию или эксплуатирует и обслуживает инфраструктурные сервисы.

3.2.49 **система масштаба предприятия** (enterprise system): Совокупность элементов информационных технологий (аппаратного и программного обеспечений, а также сервисов), внедренных с целью упрощения бизнес-процесса или процессов (административных или проектных).

3.2.50 **управляемое оборудование** (equipment under control): Оборудование, станки, аппаратура или установки, используемые в производственных, технологических, транспортных, медицинских или других целях.

3.2.51 **промышленная сеть ввода/вывода** (field I/O network): Соединительное звено (проводное или беспроводное), которое связывает датчики и исполнительные механизмы с управляющим оборудованием.

3.2.52 **межсетевой экран** (firewall): Устройство межсетевого взаимодействия, осуществляющее фильтрацию трафика между двумя связанными друг с другом сетями.

Примечание — Межсетевой экран может представлять собой либо приложение, установленное на компьютере общего назначения, либо выделенное устройство, которое направляет пакеты данных адресату или отказывает в передаче/возвращает пакеты обратно. Обычно межсетевые экраны используются для задания границ зон. Как правило, межсетевые экраны функционируют по алгоритмам, обеспечивающим избирательное открытие коммуникационных портов.

3.2.53 **шлюз** (gateway): Коммуникационное устройство, которое подсоединено к двум (или более) компьютерным сетям, имеющим схожее назначение, но реализованным различным образом, и обеспечивает связь хост-компьютеров одной сети с хост-компьютерами другой сети.

Примечание — Также может подразумеваться в виде промежуточной системы, выполняющей роль передаточного интерфейса между двумя компьютерными сетями.

3.2.54 **географический объект** (geographic site): Подмножество физической, географической или логической группы имущественных объектов предприятия.

Примечание — Географический объект может содержать участки, производственные линии, технологические ячейки и установки, центры управления и транспортные средства и быть связан с другими географическими объектами глобальной вычислительной сетью.

3.2.55 **страж** (guard): Шлюз, который расположен между двумя сетями (или компьютерами, а также прочими информационными системами), функционирующими на разных уровнях безопасности (обычно одна из сетей защищеннее другой), и служит промежуточным звеном на пути любого обмена информацией между данными сетями: либо для предотвращения передачи конфиденциальной информации из более защищенной сети в менее защищенную, либо для сохранения целостности данных в более защищенной сети.

3.2.56 **хост** (host): Компьютер, который соединен с коммуникационной подсетью или объединенной сетью и может использовать сервисы, предоставляемые сетью, для обмена данными с другими подсоединенными системами.

3.2.57 **системы промышленной автоматики и контроля** (industrial automation and control systems), IACS: Группа персонала, а также совокупность аппаратного и программного обеспечений, которые могут регулировать или воздействовать иным образом на безопасное, защищенное и надежное функционирование производственного процесса.

Примечание — Такие системы могут включать в себя, но не ограничиваются этим:

- промышленные системы управления, включающие в себя распределенные системы управления (DCS), программируемые логические контроллеры (PLC), пульты дистанционного управления (RTU), интеллектуальные электронные устройства, системы диспетчерского контроля и сбора данных (SCADA), объединенные системы электронного детектирования и контроля, а также системы мониторинга и диагностики. (В данном контексте системы управления процессами наделены базовыми функциями системы управления процессами и автоматизированной системы безопасности (SIS), которые могут быть или физически разделены друг от друга, или объединены друг с другом);

- ассоциированные информационные системы, например, системы упреждающего или многосвязного регулирования, а также сетевые оптимизаторы, специальные мониторы к оборудованию, графические интерфейсы, архиваторы, автоматизированные системы управления производственными процессами и информационно-управляющие системы предприятия;

- ассоциированные внутренние, пользовательские, сетевые или машинные интерфейсы, используемые для обеспечения управления, защиты и функциональности производственных операций в ходе непрерывных, периодических, дискретных и прочих процессов.

3.2.58 **исходный риск** (initial risk): Риск до реализации мер защиты или контрмер (см. 3.2.87).

3.2.59 **инсайдер** (insider): Доверенное лицо — сотрудник, подрядчик или поставщик, владеющие информацией, которая, как правило, не известна общественности (см. 3.2.74).

3.2.60 **целостность** (integrity): Свойство системы, отражающее логическую корректность и надежность операционной системы, логическую полноту аппаратного и программного обеспечений, которые реализуют защитные механизмы, а также постоянство структуры и содержания хранимых данных.

Примечание — В формальном укладе безопасности целостность часто понимают в более узком смысле — в значении защищенности от несанкционированного преобразования или уничтожения информации.

3.2.61 **перехват** (interception): Несанкционированный анализ трафика (снифинг) (sniffing). Перехват и раскрытие содержания сообщений или применение анализа трафика, основанного на выявлении адресата, источника сообщения, частоты или длительности передачи данных и других параметров связи, как средство нарушения конфиденциальности коммуникационной системы

3.2.62 **интерфейс** (interface): Логический вход или выход, которые обеспечивают передачу потоков логической информации к модулю или из модуля.

3.2.63 **несанкционированное проникновение** (intrusion): Акт нарушения безопасности системы (см. 3.2.9).

3.2.64 **детектирование несанкционированных проникновений** (intrusion detection): Сервис безопасности, который позволяет отслеживать и анализиро вать системные события с целью выявления и уведомления в режиме реального или почти реального времени о попытках получения несанкционированного доступа к ресурсам системы.

3.2.65 **IP-адрес** (IP address): Адрес компьютера или устройства, предназначенный для их идентификации и связи с ними с использованием межсетевого протокола Internet и других протоколов.

3.2.66 **ИСО** (ISO): Международная организация по стандартизации.

Примечание — ИСО — это не аббревиатура. Название происходит от греческого слова «iso», что означает «равный».

3.2.67 **управление ключами** (key management): Процесс манипулирования и управления криптографическими ключами и связанным с ними материалом (например, инициализирующими значениями) на протяжении их жизненного цикла в криптографической системе, включая заказ, генерацию, распределение, хранение, загрузку, депонирование, архивацию, аудит и уничтожение ключей и связанного с ними материала.

3.2.68 **линии, блоки, ячейки** (lines, units, cells): Низкоуровневые элементы, которые осуществляют функции изготовления, управления периферийными устройствами или транспортировки.

Примечание — Субъекты на этом уровне могут быть связаны между собой зональной сетью управления и содержать информационные системы, привязанные к процессам, которые происходят в конкретном субъекте.

3.2.69 **локальная вычислительная сеть** (local area network): Коммуникационная сеть, предназначенная для связывания между собой компьютеров и других интеллектуальных устройств в ограниченной географической области (обычно в пределах 10 км).

3.2.70 **вредоносный код** (malicious code): Программы или код, написанные с целью получения информации о системах или пользователях, уничтожения системных данных, создания благоприятных условий для дальнейшего несанкционированного проникновения в систему, фальсификации системных данных и отчетов, а также внесения путаницы в системные процессы и доставления длительных хлопот обслуживающему персоналу.

Примечание 1 — Вредоносные коды, используемые в ходе атак, могут принимать форму вирусов, червей, троянских коней или других автоматических программ, использующих уязвимости в системе.

Примечание 2 — Вредоносный код часто называют вредоносными программами (malware).

3.2.71 **производственные операции** (manufacturing operations): Совокупность операций изготовления, обслуживания и обеспечения качества и их связь с другими процессами на производственном объекте.

Примечание — Производственные операции включают в себя:

- организацию работы с производственным или технологическим оборудованием, на-правленную на распределение ресурсов персонала, оборудования и материалов, которые задействованы в преобразовании сырьевых материалов или деталей в продукцию;
- операции, которые могут выполняться физическим оборудованием, самим человеком и информационными системами;
- управление информацией о балансе, использовании, возможностях, характеристиках, изменении во времени и состоянии всех ресурсов (персонала, оборудования и материалов) на производственном объекте.

3.2.72 **защита от непризнания участия** (гарантия сохранения авторства) (nonrepudiation): Сервис безопасности, который обеспечивает защиту от ложного непризнания участия в коммуникации.

3.2.73 **OPC** (OPC): Набор стандартов для обмена информацией в среде управления процессами.

Примечание — Аббревиатура OPC происходит от «OLE для управления процессами», где OLE — «Связывание и встраивание объектов».

3.2.74 **аутсайдер** (outsider): Лицо или группа, не наделенные правом внутреннего доступа, которые могут быть как известны, так и не известны целевой организации (см. 3.2.59).

Примечание — Аутсайдеры могли когда-то быть инсайдерами.

3.2.75 **преодоление защиты** (penetration): Успешное несанкционированное получение доступа к защищенному ресурсу системы.

3.2.76 **фишинг** (phishing): Разновидность попыток несанкционированного доступа, когда жертву провоцируют на разглашение информации, посылая ей фальсифицированное электронное письмо с приглашением посетить веб-сайт, который на первый взгляд связан с законным источником.

3.2.77 **открытый текст** (plaintext): Незашифрованные данные, которые подлежат преобразованию методом шифрования или получены методом расшифровки.

3.2.78 **привилегия** (privilege): Авторизация или набор авторизаций на вы-полнение определенных функций, особенно в контексте операционной системы компьютера.

Пример — Операции, контролируемые использованием привилегий, включают в себя: квитирование сигнализации, изменение уставок и изменение алгоритмов управления.

3.2.79 **процесс** (process): Серия операций, выполняемых в ходе изготовления, обработки или транспортировки изделия или материала.

Примечание — В настоящем стандарте понятие «процесс» широко используется для описания оборудования, которое управляется системой промышленной автоматики и контроля.

3.2.80 **протокол** (protocol): Набор правил (т. е. форматов и процедур) для реализации и управления некоторыми видами ассоциаций (например, связи) между системами.

3.2.81 **базовая модель** (reference model): Структура, позволяющая описывать модули и интерфейсы системы единым образом.

3.2.82 **функциональная надежность** (надежность) (reliability): Способность системы выполнять требуемую функцию при заданных условиях в течение определенного периода времени.

3.2.83 **удаленный доступ** (remote access): Использование систем, которые находятся в пределах периметра зоны безопасности, предусмотренное из другой географической точки, причем указанное использование осуществляется на тех же правах, как если бы системы физически находились в этой точке.

Примечание — Точное определение «удаленного» может варьироваться в зависимости от ситуации. Например, доступ может исходить из точки, которая удалена от данной конкретной зоны, но все еще находится в границах компании или организации. Такой доступ может представлять меньший риск по сравнению с доступом, исходящим из точки, которая значительно удалена от рассматриваемой зоны и находится за границами компании.

3.2.84 **удаленный клиент** (remote client): Объект за пределами управляющей сети, который временно или постоянно соединен с хостом в пределах данной управляющей сети через связующее звено, чтобы иметь прямой или опосредованный доступ к элементам управляющего оборудования, закрепленного за данной управляющей сетью.

3.2.85 **непризнание участия** (repudiation): Полное или частичное непризнание одним из субъектов, участвовавших в передаче данных, своего участия в данной передаче.

3.2.86 **остаточный риск** (residual risk): Риск, сохраняющийся после реалиизации мер защиты или контрмер.

3.2.87 **риск** (risk): Ожидание ущерба, выраженное как вероятность того, что определенный источник угрозы воспользуется определенной уязвимостью системы, и это приведет к определенным последствиям[1)].

3.2.88 **оценка риска** (risk assessment): Процесс систематического выявления потенциальных уязвимостей значимых ресурсов системы и угроз для этих ресурсов, количественной оценки потенциального ущерба и последствий на основе вероятностей их возникновения, и (в случае необходимости) разработки рекомендаций по выделению ресурсов для организации контрмер с целью минимизации общей уязвимости.

Примечание 1 — Ресурсы могут быть физическими, логическими, кадровыми и др.

Примечание 2 — Оценки рисков часто бывают комбинированы с оценками уязвимостей, выполняемыми для выявления уязвимостей, и количественной оценкой связанных с ними рисков. Их проводят в самом начале и затем периодически для отражения изменений в границах допустимости рисков для организации, ее уязвимостях, процедурах, а также кадровых перестановок и технологических преобразований.

3.2.89 **управление риском** (risk management): Процесс определения и применения контрмер в соответствии со значимостью защищаемых объектов, на основе оценки риска.

3.2.90 **меры смягчения риска** (risk mitigation controls): Комбинация контрмер и планов ведения бизнеса.

3.2.91 **уровень допустимости риска** (risk tolerance level): Уровень остаточного риска, приемлемый для организации.

3.2.92 **ролевая модель управления доступом** (role-based access control): Форма управления доступом на основе идентификационной информации, когда субъекты системы, которые подвергаются идентификации и контролю, являются должностными позициями в организации или процессе.

3.2.93 **маршрутизатор** (router): Шлюз между двумя сетями, функционирующими на уровне 3 взаимодействия открытых систем (OSI), который перенаправляет и посылает пакеты данных во внутреннюю сеть. Наиболее известные типы маршрутизаторов пересылают пакеты интернет-протокола (IP).

3.2.94 **безопасность** (safety): Отсутствие недопустимого риска.

3.2.95 **автоматизированная система безопасности** (safety-instrumented system): Система, используемая для реализации одной или нескольких функций технологической безопасности.

Примечание — Автоматизированная система безопасности может представлять собой любую комбинацию из датчика(ов), логического решающего устройства(ств) и исполнительного механизма(ов).

3.2.96 **уровень целостности безопасности** (safety integrity level): Дискретный уровень (один из четырех) для определения требований к целостности безопасности, предъявляемых к функциям технологической безопасности, которыми наделяются автоматизированные системы безопасности.

Примечание — Уровень 4 целостности безопасности соответствует высшей степени целостности безопасности; уровень 1 целостности безопасности — низшей.

3.2.97 **сеть безопасности** (safety network): Сеть, которая связывает между собой автоматизированные системы безопасности для передачи информации о мерах обеспечения безопасности.

3.2.98 **секретность** (secret): Статус информации, защищаемой от передачи любым субъектам системы, кроме тех, на кого она ориентирована.

3.2.99 **защита** (security):

a) меры, предпринимаемые для защиты системы;

b) состояние системы, которое является результатом разработки и проведения мер защиты системы;

[1)] Другое определение риска, например, Специальная публикация Национального института стандартов и технологий (NIST) 800-30. Руководство по управлению рисками для систем информационных технологий.

c) состояние ресурсов системы, которые защищены от несанкционированного доступа к ним и несанкционированного или случайного их изменения, уничтожения, а также от утери;

d) возможность компьютерной системы гарантировать в достаточной степени, что неавторизованные лица и системы не смогут ни видоизменять программное обеспечение и данные о нем, ни получать доступ к функциям системы, но в то же время гарантировать, что это возможно для авторизованных лиц и систем;

e) предотвращение несанкционированного или нежелательного проникновения, а также вмешательства в исправную и запланированную работу системы промышленной автоматики и контроля.

Примечание — Указанные меры могут представлять собой меры защиты, относящиеся к физической безопасности (управление физическим доступом к вычислительным объектам), или логической безопасности (возможность входа в конкретную систему и приложение).

3.2.100 **архитектура безопасности** (security architecture): План и набор правил, описывающие сервисы безопасности, которые должна обеспечивать система для удовлетворения запросов ее пользователей, элементы системы, необходимые для реализации этих сервисов, и необходимые показатели эффективности функционирования элементов, воздействующих на угрожающую среду.

Примечание — В данном контексте архитектура безопасности представляет собой архитектуру, которая защищает управляющую сеть от намеренных или случайных событий безопасности.

3.2.101 **аудит безопасности** (security audit): Независимое исследование и проверка записей и действий системы для определения адекватности мер защиты системы, обеспечения их соответствия заданной политике безопасности и заданному набору процедур, выявления уязвимых мест в сервисах безопасности и подготовки рекомендаций по любым необходимым изменениям контрмер.

3.2.102 **компоненты безопасности** (security components): Объекты, такие как межсетевые экраны, модули аутентификации или программное обеспечение для шифрования, используемые для улучшения показателей защиты системы промышленной автоматики и контроля (см. 3.2.33).

3.2.103 **управление безопасностью** (security control): См. 3.2.33.

Примечание — Применительно к настоящему стандарту выбран термин «контрмера» во избежание путаницы с термином «управление» в контексте управления процессом.

3.2.104 **событие безопасности** (security event): Событие в системе, относящееся к безопасности системы.

3.2.105 **функция безопасности** (security function): Функция зоны или тракта, направленная на предотвращение несанкционированного электронного вмешательства, которое способно нарушить или повлиять на нормальное функционирование устройств и систем в пределах данной зоны или тракта.

3.2.106 **инцидент безопасности** (security incident): Неблагоприятное событие в системе или сети, а также угроза такого события.

Примечание — Иногда используется термин «несостоявшийся инцидент» для описания события, которое могло обернуться инцидентом при несколько других обстоятельствах.

3.2.107 **взлом системы безопасности** (security intrusion): Событие безопасности или комбинация нескольких событий безопасностей, представляющее собой инцидент безопасности, при котором злоумышленник получает или пытается получить доступ к системе (или ресурсу системы) без соответствующей авторизации.

3.2.108 **уровень безопасности** (security level): Степень необходимой эффективности контрмер и внутренне присущих свойств безопасности устройств и систем для зоны или тракта, основанная на оценке риска для данных зоны или тракта.

3.2.109 **цель безопасности** (security objective): Аспект безопасности, назначением которого является применение определенных смягчающих мер, таких как конфиденциальность, целостность, доступность, аутентичность пользователя, санкционирование доступа, отслеживаемость и т. д.

3.2.110 **периметр безопасности** (security perimeter): Граница (логическая или физическая) домена, в пределах которой применимы политика безопасности или архитектура безопасности, т. е. граница области, в которой сервисы безопасности защищают ресурсы системы.

3.2.111 **эффективность безопасности** (security performance): Соответствие программы установленным требованиям, полнота мер специальной защиты от рисков, методов постсобытийного анализа, мер перепроверки меняющихся бизнестребований, обзора информации о новых угрозах и

уязвимостях и периодического аудита систем управления с целью поддержания мер безопасности на эффективном и адекватном уровне.

Примечание — Для оценки практической эффективности безопасности необходимы испытания, аудиты, инструментарии, критерии и другие средства и методы.

3.2.112 **политика безопасности** (security policy): Набор правил, которые регламентируют или регулируют способ предоставления сервисов безопасности системой или организацией для защиты ее объектов.

3.2.113 **процедуры безопасности** (security procedures): Описания точных способов воплощения и реализации на практике методик обеспечения безопасности.

Примечание — Процедуры безопасности реализуются посредством обучения персонала и других действий по доступной на текущий момент технологии.

3.2.114 **программа безопасности** (security program): Комбинация всех аспектов управления безопасностью — от формулировки и доведения до сведения политики до реализации передовых промышленных методик, рутинных операций и аудита.

3.2.115 **сервисы безопасности** (security services): Механизмы, используемые для обеспечения конфиденциальности, целостности данных, аутентификации, или предотвращения непризнания участия в обмене информацией.

3.2.116 **нарушение безопасности** (security violation): Акт или событие, которые приводят к нарушению или преодолению барьеров политики безопасности и являются следствием несанкционированного проникновения в систему или действий благонамеренного инсайдера.

3.2.117 **зона безопасности** (security zone): Совокупность логических или физических объектов, к которым предъявляются общие требования безопасности.

Примечание 1 — Термин «зона», употребляемый в настоящем стандарте, следует всегда относить к зоне безопасности.

Примечание 2 — Зона имеет четкую границу с другими зонами. Политика безопасности зоны обычно определяется комбинацией механизмов как на периферии зоны, так и внутри нее. Зоны могут иметь иерархическую структуру в том смысле, что могут быть образованы совокупностью подзон.

3.2.118 **датчики и исполнительные механизмы** (sensors and actuators): Измерительные или исполнительные элементы, соединенные с технологическим оборудованием и системой управления.

3.2.119 **сервер** (server): Устройство или приложение, которые предоставляют информацию или сервисы клиентским приложениям и устройствам.

3.2.120 **несанкционированный анализ трафика (сниффинг)** (sniffing): См. 3.2.61.

3.2.121 **фиктивная авторизация** (spoof): Выдача себя за авторизованного пользователя с целью выполнения несанкционированного действия.

3.2.122 **система диспетчерского контроля и сбора данных** (supervisory control and data acquisition system), **система SCADA** (SCADA system): Разновидность слабо связанной рассредоточенной системы мониторинга и контроля, которая обычно ассоциируется с системами передачи и распределения электрической энергии, трубопроводами нефти и газа, а также системами водопотребления и канализации.

Примечание — Системы диспетчерского контроля используются также на объектах для осуществления серийного, непрерывного и дискретного производства, с целью централизации процессов мониторинга и контроля на этих объектах.

3.2.123 **система (system):** Взаимодействующие между собой, взаимосвязанные или взаимозависимые элементы, образующие сложное целое.

3.2.124 **системное программное обеспечение** (system software): Специальное программное обеспечение, которое разработано для конкретной компьютерной системы или семейства компьютерных систем с целью упрощения использования и обслуживания компьютерной системы и относящихся к ней программ и данных.

3.2.125 **угроза** (threat): Потенциальная возможность нарушения безопасности при наличии обстоятельства, средства, процесса или события, способных нарушить безопасность и нанести ущерб.

3.2.126 **угрожающее действие** (threat action): Посягательство на безопасность системы.

3.2.127 **фактор угрозы** (threat agent): Причинный фактор угрожающего действия.

3.2.128 **анализ трафика** (traffic analysis): Извлечение информации из видимых характеристик потока(ов) данных, даже если данные зашифрованы или непосредственно недоступны, причем указанные характеристики включают в себя степени идентичности и месторасположения источника(ов) и адресата(ов), наличие и объем потоков, а также частоту и длительность их передачи.

3.2.129 **Троянский конь** (Trojan horse): Компьютерная программа, которая на первый взгляд имеет полезную функцию, но имеет также скрытую и потенциально вредоносную функцию, которая позволяет обойти механизмы безопасности зачастую путем использования подлинных авторизационных данных субъекта системы, вызывающего программу.

3.2.130 **надежный канал** (trusted channel): Связующее звено, способное обеспечивать защищенную связь между зонами безопасности.

3.2.131 **ненадежный канал** (untrusted channel): Связующее звено, которое не может гарантировать защищенной связи между зонами безопасности.

3.2.132 **вариант использования** (use case): Способ ввода потенциальных функциональных требований, предусматривающий использование одного или более сценариев, которые сообщают, каким образом система должна взаимодействовать с конечным пользователем или другой системой для достижения конкретной цели.

Примечание — Обычно при реализации вариантов использования система предстается как «черный ящик», и взаимодействия с системой, включая ответы системы, распознаются за пределами системы. Варианты использования популярны благодаря тому, что они упрощают описание требований, избавляя от предположений, каким образом реализовать ту или иную функцию.

3.2.133 **пользователь** (user): Лицо, организационная единица или автоматический процесс, получающие доступ в систему как на санкционированной, так и несанкционированной основе.

3.2.134 **вирус** (virus): Самотиражируемая или самовоспроизводимая программа, которая распространяется за счет внедрения своих копий в другой исполнимый код или документы.

3.2.135 **уязвимость** (vulnerability): Дефект или несовершенство структуры или способа реализации системы, а также ее функционирования и управления, как благоприятная возможность для нарушения целостности системы или политики ее безопасности.

3.2.136 **глобальная вычислительная сеть** (wide area network): Коммуникационная сеть, предназначенная для связывания между собой компьютеров, сетей и других устройств, находящихся на значительном расстоянии друг от друга, например, в разных уголках страны или всего мира.

3.2.137 **перехват информации** (wiretapping): Атака, направленная на перехват и доступ к данным и другой информации в потоке данных, передаваемых в коммуникационной системе.

Примечание 1 — Хотя термин изначально относился к выполнению механического подсоединения к электрическому проводнику, связывающему между собой два узла, сегодня он используется в значении считывания информации с носителя любого рода, используемого для связи, а также самого узла, такого как шлюз или переключатель подсетей.

Примечание 2 — Активный перехват имеет целью изменить данные или воздействовать на поток данных иным образом, в то время как пассивный перехват имеет целью лишь обнаружить поток данных и извлечь сведения из содержащейся в них информации.

3.2.138 **червь** (worm): Компьютерная программа, которая может действовать независимо, распространять свою полную рабочую версию на другие хосты сети и потреблять ресурсы компьютера с их разрушением.

3.2.139 **зона** (zone): См. 3.2.117.

Примечание — Термин «зона», употребляемый в настоящем документе, следует всегда относить к зоне безопасности.

3.3 Сокращения

В настоящем подразделе приведены сокращения, использованные в настоящем стандарте:

ANSI — Американский национальный институт стандартов (American National Standards Institute);

CIA — конфиденциальность, целостность и доступность (Confidentiality, Integrity and Availability);

CN — управляющая сеть (Control Network);

COTS — коммерчески доступные продукты (Commercial Off The Shelf);

CSMS — система управления кибербезопасностью (Cyber Security Management System);

DCS — распределенная система управления (Distributed Control System);

DdoS — распределенная атака типа «отказ в обслуживании» (Distributed Denial of Service);

DoS — отказ в обслуживании (Denial of Service);

DMZ — демилитаризованная зона (Demilitarized Zone);

FIPS — Федеральные стандарты обработки информации (U. S. Federal Information Processing Standards);

IACS — системы промышленной автоматики и контроля (Industrial Automation and Control Systems);

IEC — Международная электротехническая комиссия (International Electrotechnical Commission);

IEEE — Институт инженеров по электротехнике и электронике (Institute of Electrical and Electronics Engineers);

I/O — ввод/вывод (Input/Output);

IP — интернет-протокол (Internet Protocol);

IT — информационная технология (Information Technology);

LAN — локальная вычислительная сеть (Local Area Network);

NASA — Национальное управление по воздухоплаванию и исследованию космического пространства (U.S. National Aeronautics and Space Administration);

NOST — Бюро стандартов и технологий НАСА (NASA Office of Standards and Technology);

OSI — взаимодействие открытых систем (Open Systems Interconnect);

PLC — программируемый логический контроллер (Programmable Logic Controller);

RTU — пульт дистанционного управления (Remote Terminal Unit);

SCADA — диспетчерский контроль и сбор данных (Supervisory Control and Data Acquisition);

SIL — уровень целостности безопасности (Safety Integrity Level);

SIS — автоматизированная система безопасности (Safety-Instrumented System);

WAN — глобальная вычислительная сеть (Wide Area Network).

4 Ситуация

4.1 Общие положения

Системы промышленной автоматики и контроля функционируют в сложной среде. Организации осуществляют все более интенсивный обмен информацией между бизнес-системами и системами промышленной автоматики, и партнеры в одном деловом начинании могут быть конкурентами в другом. Однако оборудование систем промышленной автоматики и контроля привязано непосредственно к процессу, поэтому разглашение производственных тайн и сбои в передаче информации — не единственные последствия нарушения безопасности. Куда более серьезными последствиями являются вероятность человеческих жертв или производственных потерь, вред окружающей среде, нарушения регламентных норм и безопасности в эксплуатации. Масштабы таких последствий могут выходить за пределы одной организации; может быть нанесен значительный ущерб инфраструктуре целого региона или государства.

Озабоченность вызывают не только внешние угрозы; серьезный риск для безопасности могут представлять хорошо информированные инсайдеры, имеющие злые намерения, или даже невинное неумышленное действие. Кроме того, системы промышленной автоматики и контроля часто бывают объединены с другими бизнес-системами. Модификация или тестирование операционных систем могут привести к непредусмотренным электронным воздействиям на процессы внутри систем. Персонал, находящийся за пределами участка систем управления, все чаще проводит тестирование безопасности систем, преумножая количество и последствия таких эффектов. С учетом комбинации всех этих факторов легко увидеть, насколько реален риск получения несанкционированного или вредоносного доступа к промышленному процессу.

Несмотря на то, что технологии меняются, и партнерские отношения могут приносить пользу бизнесу, увеличивается потенциальный риск нарушения безопасности. С ростом угроз для субъектов хозяйствования повышаются и требования к безопасности.

4.2 Существующие системы

Системы промышленной автоматики и контроля эволюционировали из отдельных обособленных компьютеров с проприетарными операционными системами и сетей во взаимосвязанные системы и приложения, использующие готовые коммерческие (COTS) технологии (т. е. операционные системы и протоколы). В настоящее время ведется интеграция таких систем с системами масштаба

предприятия и другими бизнес-приложениями через разнообразные коммуникационные сети. Повышенная степень интеграции дает значительные бизнес-преимущества, в числе которых:

a) повышенная прозрачность функций систем промышленного контроля (рабочего процесса, состояния оборудования, графиков производства) и интегрированных технологических систем уровня бизнеса, что позволяет проводить более эффективные исследования, направленные на снижение производственных издержек и повышение производительности;

b) интегрированные системы производства и предоставления услуг, имеющие более прямой доступ к информации бизнес-уровня, что обеспечивает более адаптивную деятельность;

c) общие интерфейсы, которые позволяют снизить полные расходы на обслуживание и допускают дистанционное обслуживание производственных процессов;

d) дистанционный мониторинг систем управления процессами, позволяющий снизить расходы на обслуживание и обеспечивающий более быстрое решение проблем.

Можно определить стандарты на модели, термины и информационные обмены, позволяющие унифицировать обмен информацией в пределах совокупности систем

промышленной автоматики и контроля. Однако такая возможность обмена информацией повышает уязвимость перед неумелым использованием и атаками со стороны злоумышленников и связана с потенциальными рисками для предприятия, использующего системы промышленной автоматики и контроля.

Конфигурации систем промышленной автоматики и контроля могут быть весьма сложными в отношении аппаратного обеспечения, программирования и коммуникаций, что может препятствовать решению следующих вопросов:

- кто авторизован на доступ к электронной информации;
- когда пользователь может иметь доступ к информации;
- к каким данным или функциям пользователь сможет иметь доступ;
- откуда исходит запрос доступа;
- как происходит запрос доступа.

4.3 Текущие тенденции

Ряд нижеперечисленных предпосылок заставляет делать повышенный акцент на безопасности систем промышленной автоматики и контроля:

a) за последние годы отмечено значительное увеличение количества атак на бизнес-системы и персональные компьютерные системы с использованием вредоносных кодов. По данным хозяйствующих субъектов, с каждым годом растет количество несанкционированных попыток (как намеренных, так и случайных) получения доступа к электронной информации;

b) системы промышленной автоматики и контроля постепенно переходят на готовые коммерческие (COTS) операционные системы и протоколы и объединяются с бизнес-сетями. В результате такие системы уязвимы перед теми же программными атаками, что и деловые и настольные устройства;

c) средства для автоматизированных атак обычно доступны через Интернет. Внешняя угроза применения таких средств теперь исходит, среди прочего, от кибер-преступников и кибертеррористов, которые, вероятно, располагают большими ресурсами и сведениями для атак на систему промышленной автоматики и контроля;

d) совместные предприятия, партнерства и услуги сторонних организаций в промышленном секторе усугубили ситуацию с численностью организаций и групп, что отразилось на безопасности систем промышленной автоматики и контроля. Такие формы деятельности необходимо учитывать при разработке норм безопасности для этих систем;

e) опасность получения несанкционированного доступа исходит теперь не только от взломщиков-дилетантов или недовольных наемных работников, но и от организованных преступников или террористов, которые имеют целью воздействовать на крупные организации и объекты;

f) внедрение протоколов отраслевых документов, таких как Интернет-протокол (IP), для обмена данными между системами промышленной автоматики и контроля и промышленными устройствами. Внедрение IP подвергает такие системы тем же уязвимостям, что и коммерческие системы, функционирующие на сетевом уровне.

Эти предпосылки, взятые в совокупности, существенно увеличили риски для организаций, связанные с разработкой и эксплуатацией систем промышленной автоматики и контроля. В то же время кибербезопасность систем промышленного контроля превратилась в более значимую и общепри-

знанную проблему. А это в свою очередь требует более структурированных директив и регламентов для определения кибербезопасности, применимой к системам промышленной автоматики и контроля, а также возможности их соответствующего взаимодействия с другими системами.

4.4 Потенциальные воздействия

Лица, которым известны особенности открытых операционных систем (OS) и сетей, потенциально способны получать несанкционированный доступ к консольным устройствам, дистанционным устройствам, базам данных и, в некоторых случаях, управляющим платформам. Последствия проникновений злоумышленников в системы промышленной автоматики и контроля могут включать в себя:

a) несанкционированный доступ, кража или ненадлежащее использование конфиденциальной информации;

b) разглашение информации неавторизованным адресатам;

c) потерю целостности или надежности технологических данных и информации о производстве;

d) потерю работоспособности систем;

e) технологические сбои, ведущие к нарушению функционирования процессов, ухудшению качества продукции, увеличению производственных потерь, нарушению безопасности процессов или выбросам в окружающую среду;

f) повреждение оборудования;

g) причинение вреда здоровью работников;

h) нарушение нормативно-правовых требований;

i) угрозу здоровью населения и потери доверия со стороны общественности;

j) угрозу национальной безопасности.

5 Базовые концепции

5.1 Общие положения

В настоящем разделе изложены несколько базовых концепций, которые образуют основу для понимания последующих разделов настоящего стандарта и других стандартов серии МЭК 62443. В частности, в настоящем разделе рассмотрены следующие вопросы:

a) в чем заключаются главные концепции, используемые для описания безопасности;

b) в чем заключаются важные концепции, образующие основу исчерпывающей программы безопасности.

5.2 Цели безопасности

Информационная безопасность изначально была направлена на достижение трех целей — конфиденциальности, целостности и доступности, которые часто обозначаются аббревиатурой CIA. Стратегия информационно-технической безопасности для типичного бэк-офиса или бизнес-системы может ставить на первое место конфиденциальность и меры по управлению доступом, необходимые для ее достижения. Второй по приоритетности может быть целостность, а последней — доступность.

В контексте систем промышленной автоматики и контроля общая приоритетность этих целей зачастую различна. Безопасность в таких системах затрагивает в основном поддержание работоспособности всех компонентов систем. Существуют риски, относящиеся к промышленному оборудованию, которое управляется, контролируется или подвергается иному воздействию со стороны систем промышленной автоматики и контроля. Таким образом, целостность часто стоит на втором месте по значимости. Обычно конфиденциальность еще менее важна, поскольку данные часто бывают «сырыми» и требуют анализа в рамках контекста, который позволит получить конкретные значения.

Существенную роль играет аспект времени отклика. Требуемое время отклика систем управления может составлять порядка одной миллисекунды, в то время как традиционные бизнес-системы способны успешно функционировать при времени отклика от одной до нескольких секунд.

В некоторых случаях приоритеты обратны, как показано на рисунке 1.

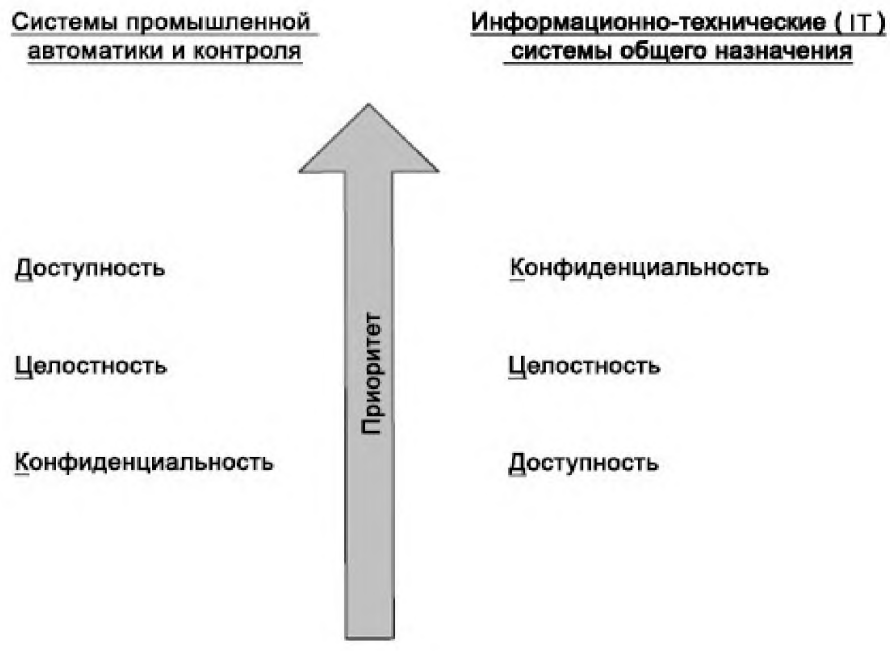

Рисунок 1 — Сравнение приоритетов целей IACS и IT-систем общего назначения

В определенных обстоятельствах целостность системы может также иметь высший приоритет. В рамках определенных требований к эксплуатации отдельные компоненты или системы в целом будут иметь иные приоритеты в качестве целей (т. е. значение целостности или доступности может перевесить значение конфиденциальности или наоборот). В результате для достижения целей безопасности организация может быть вынуждена применять другие контрмеры.

5.3 Основные требования

Простая модель CIA, показанная на рисунке 1, недостаточна для полного понимания требований к безопасности систем промышленной автоматики и контроля. Рассмотрение полного и подробного списка требований выходит за рамки настоящего стандарта, однако существует несколько базовых или фундаментальных требований к безопасности промышленной автоматики, перечисленных ниже:

a) управление доступом (AC): управлять доступом к определенным устройствам, информации или и тому, и другому, для предотвращения несанкционированного запроса устройства или информации;

b) контроль использования (UC): контролировать использование определенных устройств, информации или и того, и другого, для предотвращения несанкционированного использования устройства или информации;

c) целостность данных (DI): обеспечивать целостность данных на определенных коммуникационных каналах для предотвращения несанкционированного извлечения информации;

d) конфиденциальность данных (DC): обеспечивать конфиденциальность данных на определенных коммуникационных каналах для предотвращения несанкционированного извлечения информации;

e) ограничение потока данных (RDF): ограничивать перемещение данных по коммуникационным каналам для предотвращения попадания информации к неавторизованным источникам;

f) своевременное реагирование на событие (TRE): реагировать на нарушение безопасности путем уведомления соответствующей инстанции, предоставления данных для судебной экспертизы на-

рушения и автоматического принятия своевременного корректирующего действия в ситуациях, критически важных с точки зрения достижения поставленной цели или безопасности;

g) доступность ресурсов (RA): обеспечивать доступность всех ресурсов сети для предотвращения атак на отказ в обслуживании.

Настоящий стандарт содержит вышеперечисленные требования, но в некоторых случаях другие стандарты серии МЭК 62443 предоставляют более детальные нормативные данные. Например, технические требования, такие как целостность и конфиденциальность данных, будут детально рассмотрены в последующей части МЭК 62443.

5.4 Эшелонированная защита

Как правило, невозможно достичь целей безопасности применением единственной контрмеры или методики. Наиболее совершенной стратегией является использование концепции эшелонированной защиты, которая предполагает применение множественных контрмер в виде уровней или ступеней. Например, могут применяться системы детектирования несанкционированных проникновений, оповещающие о проникновении через сетевой экран.

5.5 Контекст безопасности

Контекст безопасности образует основу для понимания терминов и концепций и показывает, как различные элементы безопасности соотносятся между собой. Понятие «безопасность» подразумевает здесь предотвращение несанкционированного или нежелательного проникновения, а также вмешательства в исправную и запланированную работу системы промышленной автоматики и контроля. Кибербезопасность распространяется на компьютер, сеть или другие программируемые компоненты системы.

Контекст безопасности основан на концепциях угроз, рисков и контрмер, а также взаимосвязях между ними. Взаимосвязь между этими концепциями можно показать на простой модели. Одна из таких моделей, описанная в ИСО/МЭК 15408-1 («Общие критерии»), представлена на рисунке 2. Другой аспект взаимосвязи проиллюстрирован на рисунке 3.

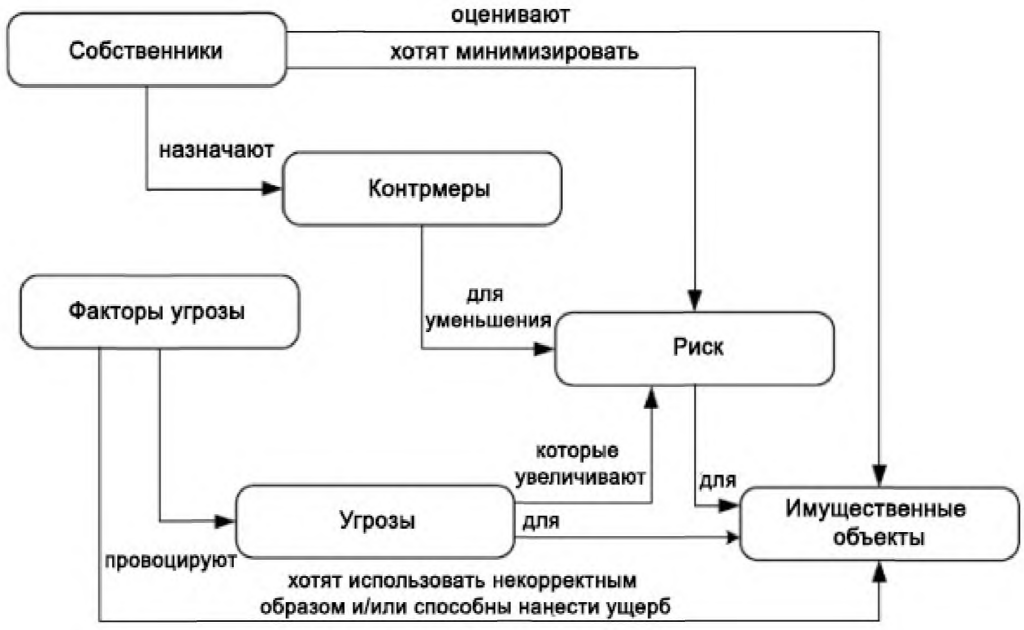

Рисунок 2 — Взаимосвязи между элементами контекста

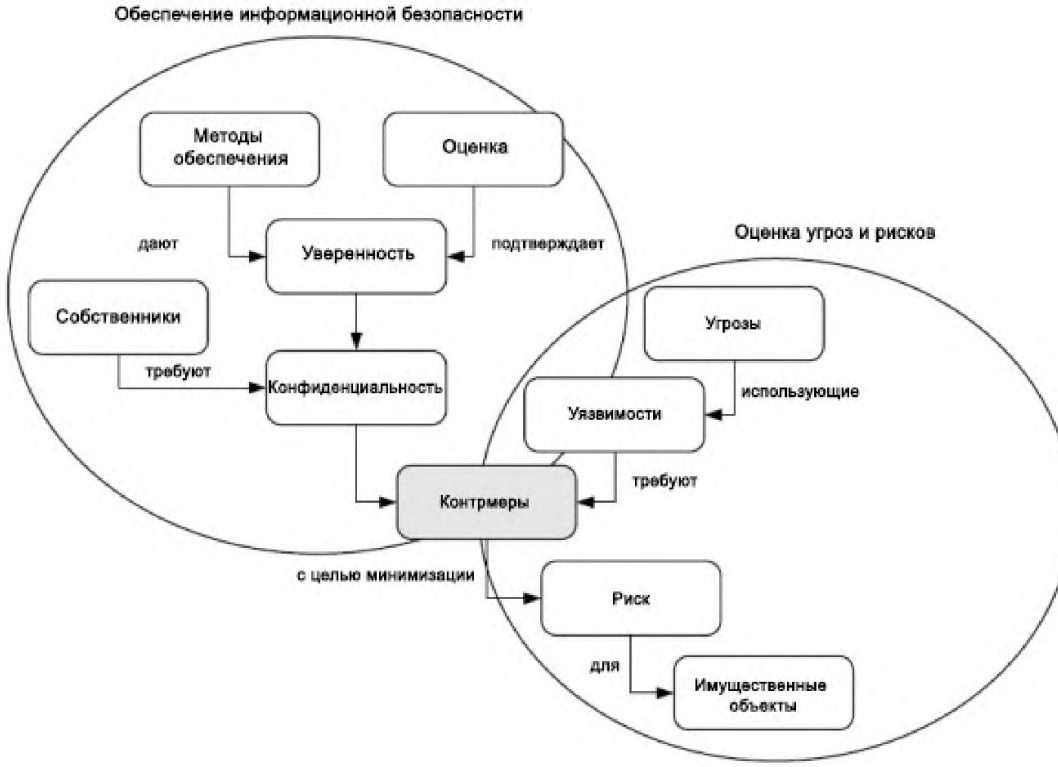

Рисунок 3 — Модель контекста безопасности

Модель контекста безопасности, представленная на рисунке 3, показывает, как соотносятся друг с другом расширенный набор концепций в рамках двух взаимосвязанных процессов — обеспечения информационной безопасности и оценки угроз и рисков.

5.6 Оценка угроз и рисков

5.6.1 Общие положения

В контексте оценки угроз и рисков имущественные объекты подвержены рискам. Эти риски в свою очередь минимизируются применением контрмер, устраняющих уязвимости, которые используются сами или позволяют использовать другие уязвимости различными угрозами. Каждый из этих элементов описан подробнее в 5.6.2–5.6.6.

5.6.2 Имущественные объекты

5.6.2.1 Общие положения

В центре внимания программы безопасности — имущественные объекты. Это то, что защищается. Чтобы в полной мере осознать риск для среды IACS, необходимо сначала составить опись имущественных объектов, нуждающихся в защите. Объекты имущества можно подразделить на физические и логические, а также кадровые ресурсы.

а) физические объекты: включают в себя любой физический компонент или группу компонентов, принадлежащих организации. В промышленной среде такие объекты могут включать в себя системы управления, физические компоненты сетей и среды прохождения сигналов, системы транспортировки, стены, помещения, здания, грунт или любые другие физические объекты, которые так или иначе участвуют в управлении, мониторинге или анализе производственных процессов или поддержании

основной коммерческой деятельности. Наиболее значимые физические объекты составляют оборудование, которое управляется системой автоматизации;

b) логические объекты: носят информативный характер. Они могут включать в себя интеллектуальную собственность, алгоритмы, внутрифирменные методики, специализированную информацию или другие информационные элементы, которые воплощают способность организации функционировать или осуществлять нововведения. Кроме того, объекты такого типа могут включать в себя репутацию в глазах общественности, доверие покупателей или другие показатели, снижение которых непосредственно отражается на бизнесе. Логические объекты могут быть в форме человеческой памяти, документов, информации, содержащейся на материальных носителях, или электронных записей, относящихся к информационному объекту. Логические объекты могут включать в себя также результаты испытаний, данные соответствия нормативным документам или любую другую информацию, которая считается важной или проприетарной, или может либо дать, либо обеспечить конкурентное преимущество. Утрата логических объектов часто чревата весьма длительными и вредоносными последствиями для организации.

Процессы управления являются особой формой логических объектов. Они содержат логику автоматизации, применяемую при осуществлении промышленного процесса. Такие процессы сильно зависят от цикличной или непрерывной реализации точно определенных событий. Нарушение безопасности технологических объектов может осуществляться как физическими (например, разрушение носителей), так и нефизическими (например, несанкционированное изменение) средствами и приводить к некоторой потере целостности или доступности самого процесса;

c) кадровые ресурсы: включают в себя работников, а также их знания и навыки, соответствующие их производственной деятельности. Последняя может включать в себя необходимые процедуры сертификации, опыт работы с оборудованием, или другую деятельность, которая не затрагивает процессы автоматизированного производства, или важные навыки, необходимые в чрезвычайных ситуациях. Технологическое оборудование редко бывает полностью автоматизированным, и сбои в операциях, производимых сотрудниками, могут существенно отразиться на производстве, несмотря на относительную сохранность физических и логических систем. Например, из-за ошибочного срабатывания заводской сигнализации персонал может предпринять останов и эвакуацию с завода, хотя в системах промышленной автоматики и контроля ничего не было нарушено ни на физическом, ни на логическом уровне. Любое происшествие или атака, приводящие к травмированию сотрудника, будут рассматриваться как затрагивающие кадровый ресурс.

5.6.2.2 Оценка имущественных объектов

Чтобы соответствовать категории физического или логического объекта имущества, этот объект должен принадлежать организации или относиться к ней иным способом. Он должен также представлять ценность для организации. Ценность объекта может быть выражена, либо в количественном, либо в качественном отношениях. Некоторые организации могут считать качественную оценку достаточным критерием для выражения имущественного ущерба в ходе анализа рисков.

a) количественная оценка объектов: объекту, которому дана количественная оценка, соответствует точный потенциальный финансовый ущерб. Он может выражаться в стоимости замены, стоимости потерянного сбыта или других финансовых показателях. Количественная оценка требует скрупулезного анализа стоимости для получения точной цифры, зато дает организации намного более ясную картину потенциальных последствий ущерба;

b) качественная оценка объектов: качественный ущерб обычно выражает более абстрактный уровень ущерба, например, его процентную или относительную величину,

которая соответствует, например, незначительным последствиям, значительным последствиям или отсутствию последствий. Многие объекты можно проанализировать лишь с точки зрения качественного ущерба. Процедуру оценки рисков можно начинать с качественной оценки объектов для документирования больших рисков и обоснования проекта по расходованию денег на ликвидацию последствий с целью снижения риска, а затем подкрепить количественным анализом для получения детальной картины подверженности риску.

Ценность можно классифицировать по типу причиняемого ущерба, который может быть прямым или косвенным;

c) прямой ущерб: отражает стоимость замены объекта. Применительно к физическому объекту эта стоимость может включать в себя стоимость замены самого устройства. Логическим объектам соответствует относительно малый прямой ущерб по сравнению с их полезностью, поскольку носитель, используемый для хранения такого объекта, обычно дешевый;

d) косвенный ущерб: отражает любой ущерб, вызванный выходом объекта из строя, за который несет ответственность сама организация. Такой ущерб может включать в себя убытки, связанные с технологическими простоями, доработкой, или другие производственные расходы, обусловленные выходом объекта из строя. Косвенный ущерб применительно к физическим объектам обычно включает в себя последствия спада производства из-за выхода из строя компонента. Косвенный ущерб применительно к логическим объектам часто значителен. Он включает в себя потерю доверия общественности, утрату лицензии на эксплуатацию из-за нарушения нормативных предписаний, и потерю конкурентного преимущества, достигнутого благодаря реализации интеллектуальной собственности (например, конфиденциальной технологии).

5.6.2.3 Классификация ущерба

Объединив информацию о типах объектов и оценке, можно показать типы ущерба для каждого типа объекта, как показано в таблице 1.

Таблица 1 — Типы ущерба в зависимости от типов объектов

Тип объекта	Прямой ущерб	Косвенный ущерб	Качественная или количественная оценка
Физический	Может быть значительным, отражая стоимость замены объекта. Прямой ущерб является следствием неисправности физических объектов по причине утраты их целостности или доступности, и на рушения точной последовательности операций или стабильного характера процесса	Последствия спада производства, вызванного выходом объекта из строя, включая потерю управления, выход из строя или повреждение других объектов, и убытки из-за простоев	Качественная или количественная, может быть сначала качественной для высоких уровней риска, а затем — количественной для большей точности
Логический	Низкий, т. к. носители информации часто дешевы и легко заменимы	Значителен, часто из-за утраты интеллектуальной собственности, раскрытия проприетарных методик или нарушения нормативно-правового соответствия. Косвенный ущерб от повреждения оборудования или разглашения данных может побудить к приостановке процессов, доработкам, модификациям или другим действиям по восстановлению контроля над производственным процессом	Чаще всего качественная, однако некоторые последствия спада производства могут иметь количественный характер

Окончание таблицы 1

Тип объекта	Прямой ущерб	Косвенный ущерб	Качественная или количественная оценка
Кадровый ресурс	От низкого до среднего в зависимости от тяжести травмы работника. Незначительные травмы при коротком периоде реабилитации могут обернуться низким прямым ущербом для организации, хотя сама травма может иметь длительные последствия для травмированного работника	От низкого до значительного в зависимости от тяжести травмы и роли работника в осуществлении процесса. Затраты на сверхурочную работу и расходы на временную замену работника могут значительно варьироваться в зависимости от длительности периода реабилитации работника. Травмы, приводящие к бессрочной потере работоспособности, или смерть могут повлечь значительные расходы из-за косвенного ущерба, если при его оценке принимаются в расчет социальная ответственность, потенциальные судебные издержки и компенсации	Непосредственный качественный ущерб производству, за которым следует количественный ущерб, обус-ловленный расходами на восстановление трудоспособности или замену работника

5.6.3 Уязвимости

Уязвимости представляют собой слабые места в системах, компонентах или организациях.

Уязвимости могут быть результатом намеренных проектных решений или быть случайными и являться следствием непонимания функциональной среды. Они могут

возникать и по мере старения оборудования, приводящего к его непригодности, если это случается быстрее, чем заканчивается типичный срок функционирования основного процесса или управляемого оборудования. Уязвимости не сводятся только к электронным или сетевым системам. Понимание взаимосвязи между физическими (в том числе человеческими) и электронными уязвимостями крайне важно для определения эффективной безопасности систем промышленной автоматики и контроля.

Система промышленной автоматики и контроля, изначально имеющая ограниченную уязвимость, может стать более уязвимой в таких условиях как изменение среды, изменение технологий, отказ компонентов системы, невозможность замены компонентов, текучесть кадров и раскрытие информации об существующих уязвимостях.

5.6.4 Риск

5.6.4.1 Общие положения

Риск определяют как ожидание ущерба, выраженное вероятностью того, что определенный источник угрозы воспользуется определенной уязвимостью объекта, что приведет к отрицательным последствиям. Риск зависит от угрозы, уязвимости и последствия, где последствие — это отрицательное воздействие на организацию, которое обусловлено конкретным вредом имущественному объекту или объектам внутри организации, причиняемым конкретной угрозой или уязвимостью. Угроза и уязвимость могут быть выражены через вероятность возникновения. Вероятность возникнове- ния — это вероятность того, что конкретное действие произойдет.

Собственникам имущественных объектов следует ранжировать стоимость смягчения последствий или стоимость ремонта и включать их в оценку риска. Собственникам следует также назначать соответствующие контрмеры для максимального смягчения рисков нарушения безопасности при минимальных финансовых затратах.

Любая полноценная методика оценки риска предполагает поэтапный анализ всех задействованных систем, начиная с систем непосредственно доступных для угрозы, и далее к системам менее доступным. Базовый метод оценки риска состоит из следующих трех этапов:

1) оценка исходного риска;

2) реализация контрмер по смягчению риска;

3) оценка остаточного риска.

При необходимости этапы 2 и 3 данного метода повторяют для снижения остаточного риска до допустимого уровня. В частности, второй этап включает в себя оценку существующих мер защиты и реализацию планов по добавлению корректирующих или дополнительных контрмер. В последующей части МЭК 62443 будет представлено более детальное описание метода определения риска.

Типичные риски, принимаемые во внимание, включают в себя:

a) риски для безопасности персонала, такие как смерть или травмы;

b) риски для технологической безопасности, такие как повреждения оборудования или сбои в коммерческой деятельности;

c) риски для информационной безопасности, такие как финансовые, правовые нарушения или потеря репутации торговой марки;

d) экологический риск, такой как уведомление о нарушении, правовые нарушения или значительный ущерб;

e) риски для бизнеса, такие как сбои коммерческой деятельности.

5.6.4.2 Уровень допустимости риска

Выходными данными качественного анализа риска является перечень объектов или сценариев со сводной вероятностью возникновения и градацией последствий. В обязанности руководства входит определение соответствующих мер воздействия по пунктам на основе таких градаций. Некоторые организации приемлют относительно высокие уровни риска (в частности, динамично развивающиеся компании), а некоторые консервативны и являются противниками риска. А значит, определенный уровень остаточного риска может быть приемлем для одной организации и неприемлем для другой. Даже в пределах одной организации отдельные предприятия могут иметь разные пожелания относительно рисков или их допустимости. Руководству следует четко определять и осознавать, каковы его пожелания относительно рисков или их допустимости, чтобы лучше продумывать уровень своих ответных действий по отношению к выявленным остаточным рискам.

Решение проблем, связанных с безопасностью систем промышленной автоматики и контроля, в целом не привносит новых рисков, но может способствовать новому восприятию уже существующих рисков. Например, в контексте промышленной автоматизации рискам, связанным с безопасностью, обычно уделяют больше внимания.

Безопасность систем промышленной автоматики и контроля не требует переосмысления способа определения уровня допустимости рисков; этот способ заимствуют из других методик управления рисками в организации.

5.6.4.3 Меры воздействия на риск

Существует несколько возможных мер воздействия на риск. В зависимости от обстоятельств организации могут прибегать к той или иной комбинации мер в каждой ситуации:

a) исключение риска из проекта: одна из форм смягчения риска — изменить проект системы таким образом, чтобы исключить этот риск. Некоторые риски сущест- вуют просто потому, что возможен доступ к чему-то, несмотря на то, что доступ никогда не потребуется. Смягчить риск можно путем полной отмены ненужной функции или блокирования к ней доступа. Организации могут принимать соответствующие бизнес-решения, чтобы исключить риск. Такая мера воздействия может включать в себя сознательный отказ от чего-либо, будь то новый продукт поставщика, система или заключение договоренности;

b) снижение риска: риск можно снизить до допустимого уровня путем реализа-ции контрмер, которые уменьшают вероятность атаки или ограничивают ее последствия. Принципиальный момент в данном случае — достичь достаточного уровня безопасности, но не исключить риск полностью;

c) принятие риска: всегда есть вариант принять риск, рассматривая его как часть издержек эксплуатации предприятия. Организации должны брать на себя некоторые риски, и их не всегда удается смягчить или передать при оптимальных затратах;

d) передача или распределение риска: возможно заключить какой-либо договор страхования или соглашение по передаче всего риска или его части стороннему субъекту. Типичный пример — субподряд на определенные операции или услуги. Такое решение может быть не всегда эффективно,

поскольку может распространяться не на все имущественные объекты. Страховой договор кибербезопасности может компенсировать некоторые типы ущерба, но не ущерб, относящийся к логическим объектам, например, потерю доверия со стороны потребителей;

e) исключение или пересмотр избыточных или неэффективных мер защиты: в рамках эффективной оценки рисков выявляют и приводят в соответствие подобные меры защиты, чтобы можно было уделять больше внимания мерам защиты, которые эффективны и результативны.

5.6.5 Угрозы

5.6.5.1 Общие положения

Угрозы характеризуют возможные действия, которые могут быть предприняты в отношении системы. Они проявляются в самых различных формах, но наиболее распространенные формы следующие:

a) случайные: лицо, не знакомое с соответствующим регламентом и политикой, или по недосмотру, создает случайный риск. Возможно также, что организация не знает обо всех рисках и обнаруживает их случайно в ходе эксплуатации сложных систем промышленной автоматики и контроля;

b) несанкционированные изменения: обновления, исправления и другие изменения в операционных системах, программных приложениях, конфигурациях, возможностях взаимодействия и оборудовании могут создать неожиданную угрозу безопасности систем промышленной автоматики и контроля или соответствующего производственного процесса.

Фактор угрозы — понятие, используемое для описания субъекта, представляющего собой угрозу. Факторы угрозы известны и как злоумышленники или нарушители. Они представлены во множестве различных форм. Примеры таких факторов включают в себя:

c) инсайдер: доверенное лицо, сотрудник, подрядчик или поставщик, владеющие информацией, которая, как правило, не известна общественности. Инсайдер может представлять собой угрозу даже при отсутствии неблаговидных намерений. Например, угроза может возникнуть в результате обхождения инсайдером элементов управления безопасностью для выполнения своей работы;

d) аутсайдер: лицо или группа, не наделенные правом внутреннего доступа, известное или не известное целевой организации. Аутсайдеры могли когда-то быть инсайдерами;

e) природные события: включают в себя ураганы, землетрясения, наводнения и торнадо, которые обычно считаются физической угрозой.

Угрозы, перешедшие в действие, известны как атаки (иногда обозначаются как несанкционированные проникновения). Как при разработке компонентов и систем, так и при реализации программы безопасности в пределах производственного объекта или организации, можно моделировать атаки, чтобы удостоверяться, что контрмеры действуют и способны выявлять и сдерживать их. Моделирование сценариев и схемы атак — это примеры методов, которые можно использовать.

Угрозы могут быть пассивными или активными. Каждый тип угроз описан в нижеследующих подпунктах.

5.6.5.2 Пассивные угрозы

Сбор пассивной информации может дать потенциальному злоумышленнику много ценных сведений. Факторы угрозы обычно включают в себя пассивную информацию при случайных вербальных коммуникациях с сотрудниками и подрядчиками. Однако лица, находящиеся на территории или за территорией производственных объектов, могут также получать пассивную информацию посредством визуальных наблюдений. Сбор пассивной информации может включать в себя сбор данных о пересменах, функционировании оборудования, материально-техническом снабжении, графиках патрулирования и прочих уязвимостях. Сбор пассивной информации иногда трудно обнаружить, особенно если информацию собирают малыми частями и из нескольких источников. Постоянное наблюдение над необычайно любопытными посетителями, фотографами и персоналом (зачастую за пределами мест исполнения их служебных обя-занностей) может помочь организациям выявить сбор пассивной информации, особенно если при этом тщательно проверяются их биографические данные.

Примером пассивной угрозы является сниффинг. Сниффинг — это отслеживание данных в потоке информации. Самыми известным способом сниффинга является перехват данных в потоке информации. Сниффинг может быть весьма изощренным. Инструменты сниффинга общедоступны и позволяют перехватывать данные в различных коммуникационных сетях. Такие устройства обычно используются для управления конфигурациями, поиска и устранения неисправностей в сетях и анализа трафика данных, однако их можно также использовать для сбора специальных данных о любом взаимодействии в пределах сети. Например, при сниффинге пакетов данных и паролей злоумышленник тайно подключается к сети через удаленную станцию или компьютер. Инструмент сниффинга за-

тем пассивно отслеживает информацию, пересылаемую внутри сети, и фиксирует информацию на дисковом запоминающем устройстве, причем эту информацию можно в дальнейшем загрузить и анализировать для получения идентификационной информации и паролей пользователя.

5.6.5.3 Активные угрозы

5.6.5.3.1 Общие положения

Активные угрозы бывают нескольких видов:

- коммуникационная атака;
- вторжение в базу данных;
- воспроизведение;
- фиктивная авторизация и маскировка под законного пользователя;
- социальная инженерия;
- фишинг;
- вредоносный код;
- отказ в обслуживании;
- расширение привилегий;
- физическое повреждение.

5.6.5.3.2 Коммуникационная атака

Коммуникационная атака имеет целью нарушить коммуникацию с системой промышленной автоматики и контроля. Коммуникационные атаки бывают нескольких видов. Данные атаки могут осуществляться на нескольких уровнях внутри системы, начиная с уровня процессора компьютера и далее — по восходящей, и инициироваться за пределами предприятия, как в случае атаки вида «отказ в обслуживании» (DoS) для коммуникационных систем.

5.6.5.3.3 Вторжение в базу данных

Вторжение в базу данных — форма атаки на вебсайт, управляемый базой данных, в ходе которой злоумышленник реализует неавторизованные команды, пользуясь ненадежным кодом в системе, соединенной с Интернетом, и действуя в обход межсетевого экрана. Атаки с вторжением в базу данных применяют для похищения информации из базы данных, которые, в нормальном режиме недоступны, и/или получения доступа к хост-компьютерам организации через компьютер, содержащий базу данных.

5.6.5.3.4 Воспроизведение

Из коммуникационных путей систем управления могут быть скопированы сигналы, которые впоследствии могут быть воспроизведены для обеспечения доступа к защищенным системам или фальсификации данных в системе промышленной автоматики и контроля. Потенциальные злоумышленники могут воспроизводить сигналы управления доступом, биометрические сигналы и другие сигналы системы для получения несанкционированного доступа к защищенным участкам или системам, сокрытия незаконной деятельности или выполнения ложных отвлекающих маневров. Система может реализовывать в себе серию путей для сбора данных, оповещения и контроля, что позволит предотвратить сбор всей информации (с целью ее дальнейшего воспроизведения) через единичное подключение, для всей подсистемы, узла оборудования, приложения или базы данных.

5.6.5.3.5 Фиктивная авторизация и маскировка под законного пользователя

В контексте вычислительных сетей понятия «фиктивная авторизация и маскировка под законного пользователя» используются для описания разнообразных способов, которыми можно обмануть аппаратное или программное обеспечение. Злоумышленники могут подделать заголовок электронного письма, чтобы сообщение выглядело как поступившее от какого-либо источника или адресата, отличных от подлинного. IP-спуфинг, например, задействует обманный трюк, благодаря которому сообщение выглядит как поступившее с авторизованного IP-адреса.

5.6.5.3.6 Социальная инженерия

К факторам угрозы относятся также получение или попытки получения конфиденциальных данных, обманом заставляя человека раскрыть конфиденциальную информацию. Социальная инженерия эффективна потому, что ее жертвы по своей сущности хотят доверять другим людям и готовы прийти на помощь. Жертвы социальной инженерии раскрывают информацию, не ведая о том, что она будет использована для атак на компьютерную сеть.

5.6.5.3.7 Фишинг

Разновидность посягательств на безопасность, когда жертву провоцируют на разглашение информации, посылая ей фальсифицированное электронное письмо с приглашением посетить веб-

сайт, который на первый взгляд связан с законным источником. Фишинг основан на социальной инженерии, т. к. человек склонен верить в надежность брендов, связывая их с авторитетностью.

5.6.5.3.8 Вредоносный код

Назначением вредоносного кода может быть сбор информации о системах или пользователях, уничтожение системных данных, создание закладки для дальнейшего несанкционированного проникновения в систему, фальсификация системных данных и отчетов, или внесение путаницы в системные процессы и создание сложностей обслуживающему персоналу. Вредоносные коды, используемые в ходе атак, могут принимать форму вирусов, червей, автоматических эксплойтов или троянских коней.

Вирус — это программа или часть кода внутри другой программы, которая загружается в компьютер без ведома пользователя и функционирует против его воли. Вирусы могут также самотиражироваться. Все компьютерные вирусы создаются человеком. Простой вирус, способный производить копию самого себя снова и снова, может быть создан относительно легко. Такой простой вирус уже опасен, поскольку он быстро завладеет всей доступной памятью и будет препятствовать работе системы. Еще более опасная разновидность вируса — это вирус, способный передаваться по сетям в обход систем безопасности.

Автоматический код-эксплойт вносится в систему для сбора информации или оповещения кого-либо или других систем о конкретных событиях или взаимодействиях. Относительно простой код-эксплойт способен собирать информацию для предстоящих несанкционированных проникновений, получения финансовой выгоды или статистических данных (маркетинг). Автоматический код-эксплойт может использовать другие ресурсы или приложения, которые находятся уже в самой системе, для умножения своих возможностей по сбору информации или уничтожению данных. Полностью автоматический код-эксплойт обычно называют червем. Червь представляет собой автономную программу или алгоритм, который самотиражируется в пределах компьютерной сети и обычно выполняет вредоносные действия, такие как расходование компьютерных ресурсов и, возможно, остановка работы системы.

Троянский конь — это вредоносная программа, которая маскируется под полезное приложение. В отличие от вирусов, троянские кони (также известны как «трояны») не самотиражируются, но могут быть такими же вредоносными. Одна из наиболее коварных разновидностей троянских коней — это программа, которая предлагает очистить компьютер от вирусов, но вместо этого вносит в него новые вирусы.

Вредоносный код может быть внесен с созданием ботнета, т. е. совокупности машин с нарушенной безопасностью, которые реализуют программы в рамках общей инфраструктуры контроля и управления. Создатель ботнета может управлять группой компьютеров дистанционно, как правило в неблаговидных целях.

5.6.5.3.9 Отказ в обслуживании

Атаки типа «отказ в обслуживании» (DoS) или ухудшение его качества воздействуют на работоспособность сети, операционной системы или прикладных ресурсов. Распространенной формой атаки с целью сетевого отказа в обслуживании является распределенная атака типа «DDoS», которая использует множественные устройства с нарушенной безопасностью для причинения значительного ущерба сети, устройству или приложению.

5.6.5.3.10 Расширение привилегий

Чтобы спланировать и осуществить эффективную атаку на систему, факторы угрозы должны во многих случаях сначала получить привилегированный доступ. Благодаря расширенным привилегиям злоумышленник может совершать действия, которые в противном случае будут запрещены.

5.6.5.3.11 Физическое повреждение

Атаки с физическим повреждением имеют целью разрушение или выведение из строя физических компонентов (т. е. аппаратного обеспечения, устройств хранения программного обеспечения, соединительных элементов, датчиков и контроллеров), которые являются частью системы промышленной автоматики и контроля. Такие атаки могут принимать форму физических атак непосредственно на компоненты или физических атак посредством кибератак, которые инициируют действия системы, ведущие к физическому ущербу, повреждению или выходу из строя компонента.

5.6.6 Контрмеры

Контрмеры — это предпринимаемые действия или принимаемые меры предосторожности для снижения риска до допустимого уровня или соответствия политике безопасности. Как правило, они не устраняют риск. Характер применяемых контрмер зависит от характера рассматриваемой угрозы.

Возможны различные контрмеры для отражения внешних угроз. Примеры таких мер включают в себя:

a) аутентификацию пользователей и/или компьютеров;

b) меры управления доступом;

c) выявление несанкционированных проникновений;

d) шифрование;

e) использование цифровых подписей;

f) изоляцию или разделение ресурсов;

g) сканирование на предмет обнаружения вредоносного программного обеспечения;

h) мониторинг активности системы;

i) обеспечение физической безопасности.

В случае внутренних угроз может потребоваться другой подход, поскольку злоумышленник имеет возможность обойти некоторые из стандартных контрмер управления доступом. Это заставляет уделять больше внимания таким контрмерам как служебные инструкции, разделение обязанностей, мониторинг активности, аудит систем и шифрование.

Пассивные угрозы типа сниффинга очень трудно обнаружить, поскольку инструмент сниффинга только считывает информацию, передаваемую от одного средства коммуникации к другому, и не распространяет собственных сигналов в канал передачи сигнала. Сниффинг с использованием механического подсоединения можно обнаружить с помощью современных устройств управления связью, таких как коммутатор передачи, но беспроводной сниффинг практически невозможно обнаружить даже с помощью очень сложного и дорогого оборудования радиосвязи. Доступность сниффинга можно ограничить управлением и перекрыванием неиспользуемых голосовых портов и портов передачи данных на предприятии и повышением осведомленности об оборудовании управления связью.

5.7 Степень завершенности программ безопасности

5.7.1 Обзор

Учитывая рост рисков кибербезопасности, многие организации руководству- ются упреждающим подходом при устранении рисков безопасности своих информационно-технических систем и сетей. Организации начинают осознавать, что решение вопросов, связанных с кибербезопасностью, — это непрерывная деятельность или процесс, а не проект с четко обозначенным стартом и финишем.

Изначально организации, создававшие и обслуживавшие информационные системы для бизнеса и системы промышленной автоматики и контроля, функционировали в двух взаимоисключающих областях. Профессиональный опыт, знания, и требования каждой отдельной организации не учитывались или не признавались другими организациями. Проблемы начали возникать по мере того, как организации пытались применить общие технологии IT-безопасности для систем промышленной автоматики и контроля.

В некоторых случаях технологии безопасности противоречили стандартным технологиям производства, запроектированным на обеспечение максимальной безопасности и бесперебойности производства. Сегодняшние информационные технологии общедоступны и широко применяются в системах промышленной автоматики и контроля, поэтому для безопасной реализации таких технологий требуются дополнительные знания. Информационно-техническим и производственно-технологическим организациям следует взаимодействовать между собой и объединять свои знания и опыт для разрешения вопросов, связанных с безопасностью. На промышленных объектах, которые связаны с высоким риском инцидентов, относящихся к охране труда, технике безопасности и охране окружающей среды, необходимо также предусмотреть систему обеспечения техники безопасности (PSM) и задействовать персонал службы физической безопасности.

Цель — полноценная программа безопасности, которая связывает все аспекты кибербезопасности, объединяя настольные и коммерческие вычислительные системы с системами промышленной автоматики и контроля. На рисунке 4 показан процесс слияния кибербезопасности коммерческих систем и IACS, с которым сталкиваются многие хозяйствующие субъекты. Многие организации имеют достаточно детальные и полные программы кибербезопасности, рассчитанные на их компьютерные бизнес-системы, но технологии управления кибербезопасностью IACS разработаны еще не в полной мере.

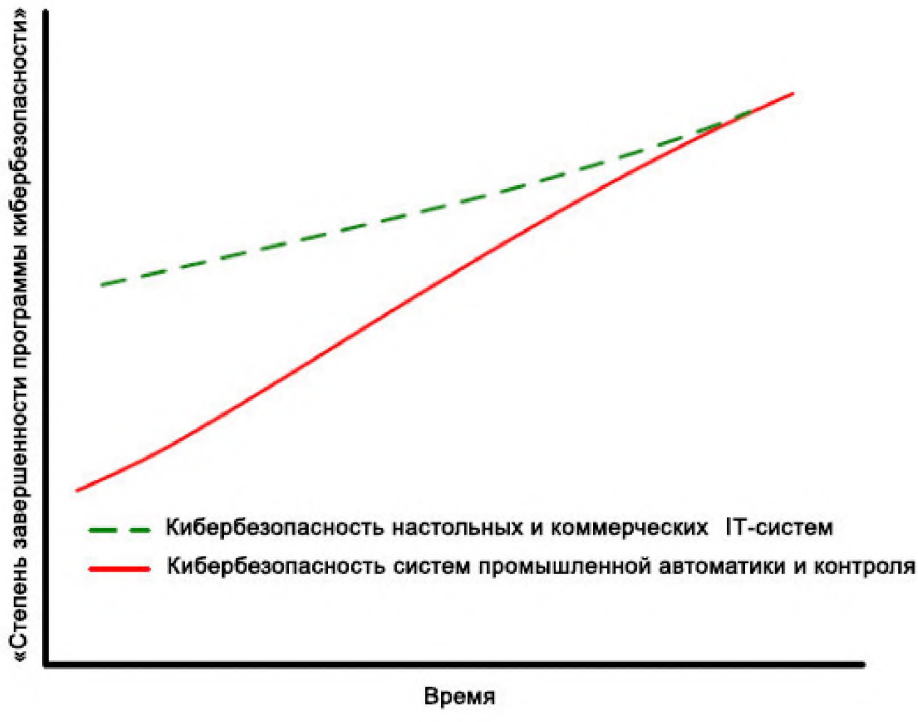

Рисунок 4 — Слияние кибербезопасности коммерческих систем и IACS

Типичная ошибка — рассматривать кибербезопасность как проект с начальной датой и датой окончания. В этом случае уровень безопасности зачастую снижается со временем, как показано на рисунке 5. Риски кибербезопасности постоянно меняются, по мере того как проявляются новые угрозы и уязвимости, а также меняются способы реализации технологий. Для сохранения достигнутого уровня безопасности и удержания рисков на приемлемом уровне необходим другой подход.

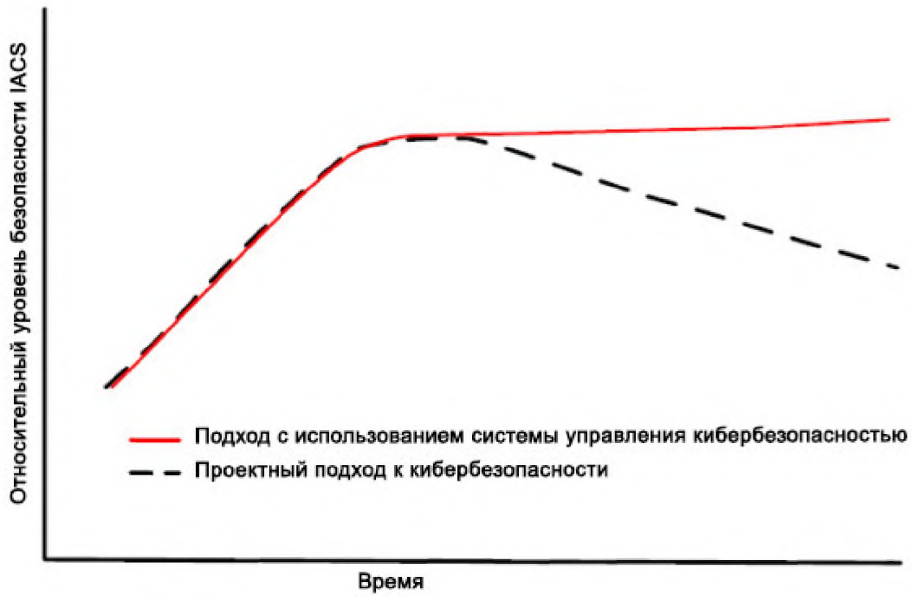

Рисунок 5 — Изменение уровня кибербезопасности со временем

Желательно разработать и внедрить систему управления кибербезопасностью (CSMS) в масштабе организации, включающую в себя программные элементы для пересмотра риска и совершения корректирующих действий, чтобы устранить тенденцию снижения уровня безопасности со временем. Во втором стандарте серии МЭК 62443 приведено исчерпывающее описание ключевых элементов системы управления кибербезопасностью [8].

Ход реализации системы управления кибербезопасностью для каждой организации будет различен в зависимости от целей организации и уровней допустимости рисков. Включение кибербезопасности в документированную методику обеспечения безопасности организации — это изменение корпоративной культуры организации, которое требует времени и ресурсов. Как показано на рисунках 4 и 5, такого изменения невозможно достичь в один этап. Это эволюционирующий процесс, который соответствует подходу к кибербезопасности. Технологии безопасности, которые предстоит внедрить, должны быть по возможности адекватны уровню риска. Технологии безопасности будут различны для разных организаций и даже могут быть различны для разных процессов внутри одной и той же организации в зависимости от общих необходимостей и требований. Отдельно взятые политика и регламенты могут быть также различны для каждого класса системы в пределах организации, поскольку уровень риска и требования безопасности могут быть различны. Система управления кибербезопасностью устанавливает единую программу, которая устраняет эти несоответствия.

Обучение и повышение осведомленности персонала крайне важны для успешного устранения рисков кибербезопасности IACS, как отмечено выше. Следует рассматривать несколько возможных вариантов:

a) инструктаж персонала, имеющего отношение к IACS, с целью разъяснения актуальных проблем, которые относятся к информационной технике и кибербезопасности;

b) инструктаж IT-персонала с целью разъяснения технологий IACS, а также действий и методов по управлению технологической безопасностью;

c) разработка методик, позволяющих объединять компетенции всех организаций, с целью совместного решения проблем, которые связаны с кибербезопасностью.

Для успешного исхода программы кибербезопасности необходимо собрать команду специалистов для подготовки как проектов по смягчению рисков, так и всеобщей программы CSMS. На рисунке 6 показан типичный спектр знаний и навыков, которые должны быть объединены и получены от раз-

личных групп специалистов для доведения программы кибербезопасности до целостного, завершенного вида.

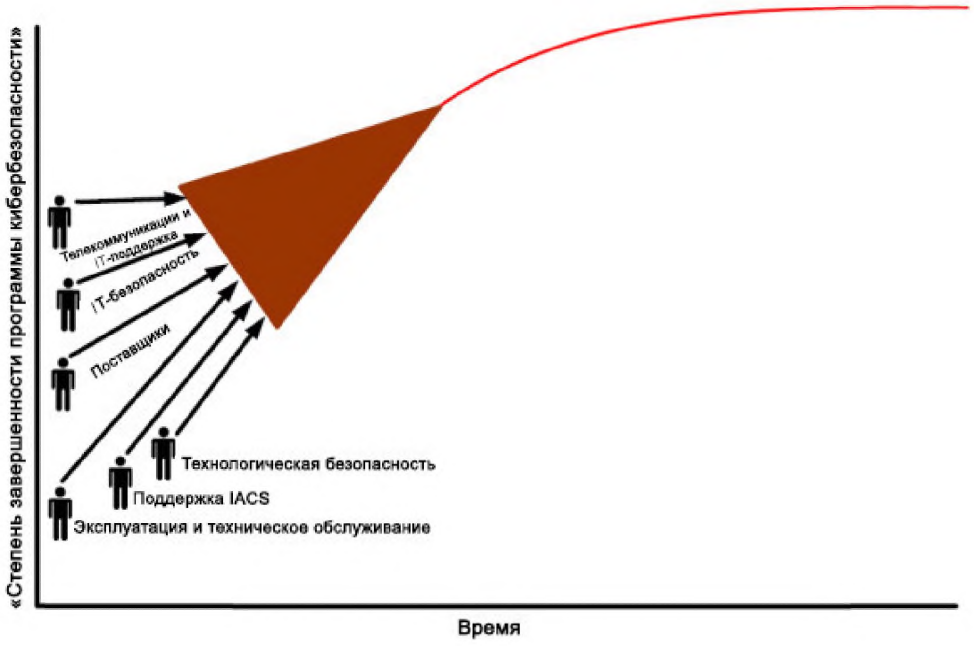

Рисунок 6 — Объединение ресурсов для создания CSMS

5.7.2 Этапы завершенности

Степень относительной завершенности программы кибербезопасности можно описать с помощью жизненного цикла, который состоит из нескольких этапов. Каждый из этих этапов состоит из одной или более стадий.

Отдельные части системы промышленной автоматики и контроля, или зоны управления внутри системы управления, могут находиться на разных этапах завершенности. Такая ситуация может быть вызвана несколькими причинами, такими как бюджетные ограничения, процессом оценки уязвимостей и угроз, результатами анализа рисков, модернизация автоматики, планы относительно утилизации или замены, наличие планов относительно продажи сегмента производственного объекта или хозяйствующего субъекта, или доступность других ресурсов для модернизации систем безопасности до более высокого уровня.

Организации могут получить более подробную информацию о степени завершенности программы безопасности, оценивая результаты в пределах отдельных частей системы промышленной автоматики и контроля по этапам и стадиям, представленным в таблице 2.

Таблица 2 — Этапы завершенности программы безопасности

Этап	Стадия
Концепция	Идентификация Составление концепции
Функциональный анализ	Техническая проработка

Окончание таблицы 2

Этап	Стадия
Реализация	Функциональный проект Рабочий проект Конструирование
Применение	Технологические операции Контроль за соблюдением установленных требований
Прекращение действия и утилизация	Снятие с эксплуатации Прекращение действия

В таблицах 3 — 7 представлены общие описания каждого из этапов и стадий завершенности жизненного цикла.

Таблица 3 — Стадия составления концепции

Стадия	Описание
Идентификация	Обоснование необходимости защиты имущественных объектов, сервисов или персонала Начало разработки программы безопасности
Составление концепции	Продолжение разработки программы безопасности Документирование имущественных объектов, сервисов и данных о персонале, для которых требуется та или иная степень защиты Документирование потенциальных внутренних и внешних угроз для предприятия Утверждение целей, концепций и шкалы ценностей безопасности Разработка политики безопасности для систем промышленной автоматики и контроля, а также оборудования, информационных систем и персонала

Таблица 4 — Этап функционального анализа

Стадия	Описание
Техническая проработка	Продолжение разработки программы безопасности Установление функциональных требований к безопасности систем промышленной автоматики и контроля, а также оборудования, производственных систем, информационных систем и персонала Выполнение оценки уязвимостей технических средств и соответствующих сервисов согласно списку потенциальных угроз Выявление и установление законодательных требований к системам промышленной автоматики и контроля Выполнение анализа рисков в отношении потенциальных уязвимостей и угроз

Окончание таблицы 4

Стадия	Описание
Техническая проработка	Ранжирование рисков, потенциальных последствий для предприятия и потенциальных мер их смягчения Разбиение задач по обеспечению безопасности на управляемые задания и модули для создания функциональных проектов Создание определений сетевой функциональности для участков. безопасности систем промышленной автоматики и контроля

Таблица 5 — Этап реализации

Стадия	Описание
Функциональный проект	На данном этапе завершается разработка программы безопасности Определение функциональных требований к зонам безопасности предприятия, завода и управления. Определение и документирование потенциальных процессов и событий для оформления функциональных требований и воплощения планов относительно создания защищенного предприя-тия Определение функциональной организации и структуры безопасности Определение функций как требуемых в плане реализации Определение и обнародование зон и границ безопасности, а также порталы управления доступом Завершение работы над политикой и регламентами безопасности и ввод их в действие
Рабочий проект	Проектирование физических и логических систем, реализующих функциональные требования, определенные ранее применительно к безопасности Осуществление программ инструктажа
Рабочий проект	Полная разработка плана реализации Инициирование программ по управлению имущественными объектами и изменениями Проектирование границ и портала управления доступом для защищенных зон
Конструирование	Претворение плана реализации. Ввод в действие оборудования физической безопасности, логических приложений, конфигураций, регламентов для персонала для оформления зон и границ безопасности в пределах предприятия Ввод в действие и обслуживание атрибутов портала управления доступом Завершение программ инструктажа Программы управления имущественными объектами и изменениями находятся в рабочем состоянии и действуют Комплекты документации по сдаче-приемке системы безопасности оформлены и готовы для принятия эксплуатационным и обслуживающим персоналом

Таблица 6 — Этап применения

Стадия	Описание
Действия	Оборудование безопасности, сервисы, приложения и конфигурации реализованы и приняты на эксплуатацию и обслуживание Персонал обучен, и ведется непрерывный инструктаж по вопросам безопасности Проводимое техническое обслуживание позволяет контролировать узлы безопасности предприятия, завода или зон управления, обеспечивая их исправное функционирование Действует и поддерживается управление имущественными объектами и изменениями
Контроль за соблюдением установленных требований	Внутренние аудиты Пересмотры рисков Внешние аудиты

Таблица 7 — Этап прекращения действия и утилизации

Стадия	Операция
Снятие с эксплуатации	Устаревшие системы безопасности надлежащим образом демонтируются и утилизируются Границы безопасности корректируются или воссоздаются для защиты зон Портал управления доступом создаются, переопределяются, перекомпоновываются или закрываются Персонал информируется об изменениях в системах и компонентах безопасности, и о влиянии этих изменений на соответствующие системы безопасности
Прекращение действия	Интеллектуальная собственность надлежащим образом собирается, документируется и надежно архивируется или уничтожается Портал управления доступом и соответствующие связующие звенья перекрываются Персонал информируется о прекращении действия систем и компонентов безопасности и о влиянии этого на оставшиеся системы безопасности

5.8 Политики безопасности

5.8.1 Общие положения

Политики безопасности дают возможность организации придерживаться последовательной программы по обеспечению допустимого уровня безопасности. Политики безопасности определяют в организации на различных уровнях, при этом они могут принимать самую разную форму, начиная от политики управления или администрирования, устанавливаемых на уровне предприятия, заканчивая политикой эксплуатации, определяющей подробные данные управления безопасностью. Политики безопасности, относящиеся к особому уровню — это документы организации, относительно которых можно определять соответствие установленным требованиям в рамках аудитов безопасности.

Политики безопасности — это правила, которые определяют или регулируют способ защиты организацией уязвимых и особо важных системных ресурсов. Политики безопасности однозначно формулируют, что обязательно для исполнения. Поскольку политики безопасности обязательны для со-

блюдения и однозначны, они допускают их использование для аудитов. Политики безопасности организации учитывают также нормативно-правовые и контрактные обязательства, относительно которых осуществляется проверка фактической деятельности организации в рамках аудитов.

Дополняют политики безопасности регламенты. Регламенты безопасности определяют детальную последовательность действий, необходимых для осуществления той или иной меры безопасности. По уровню применения регламенты используют для решения конкретной проблемы. Регламенты могут относиться к конкретной технологии. Политики безопасности ссылаются на регламенты и уполномочивает их применение.

Противоположностью политикам безопасности и регламентам являются директивы. Директивы не обязательны для выполнения. Они предназначены для описания способа выполнения чего-либо, что желательно, но не обязательно. Поскольку директивы не обязательны для выполнения и могут быть неоднозначны, практические действия не могут подвергаться аудитам с опорой на директивы. Директивы иногда разрабатывает группа специалистов, которая неправомочна требовать их выполнения. Директивы не содержат описания практических действий, которые подлежат обязательному выполнению.

Политики и регламенты безопасности в основном различны для разных частей организации, поэтому важно их правильное координирование. В частности, политику безопасности систем промышленной автоматики и контроля следует координировать с аналогичной политикой безопасности информационной техники общего назначения. Программа безопасности будет реализована успешнее, если в команде установлены хорошие деловые взаимоотношения, и правильно скоординированные методики действий могут им поспособствовать.

Некоторое единообразие структуры для разных политик безопасности и регламентов повышает согласованность между универсальными наборами политик безопасности и регламентов. Каждый документ, описывающий политику или регламент, содержит краткую, но точную формулировку своего назначения. Документ содержит также формулировку границ применимости документа. Кроме того, он содержит описание рисков, которые предполагается снизить, и ключевых принципов, на которых строится документ.

Разным этапам жизненного цикла системы соответствуют разные профили проблем безопасности. Политики и регламенты безопасности могут затрагивать лишь конкретные этапы жизненного цикла. В некоторых политике и регламенте может быть указано, что они относятся только к определенным этапам жизненного цикла. В наборе политик и регламентов безопасности все вопросы безопасности, относящиеся к разным этапам жизненного цикла, рассматриваются в соответствующих пунктах.

Политики и регламенты безопасности содержат инструкции относительно того, каким образом организация должна определять степень соответствия политики нормативам и как обновлять их. При проведении или оценке аудитов организации часто обнаруживают, что политика требует пересмотра. Аудиты могут выявить неясности в политике и регламенте в целом или в их частях, ведущие к неоднозначной трактовке требуемой операции или результата. Аудиты могут выявить проблемы, которые следует учесть при разработке политики и регламента. Аудиты могут выявить и требования, которые следует пересмотреть и скорректировать или даже исключить в случае необходимости.

Политики и регламенты безопасности должны по возможности учитывать непредвиденные обстоятельства, которые делают невозможным их применение. Политика должна по возможности устанавливать порядок документирования и утверждения исключений к политике и регламентам. Если утвержденные исключения документировать, это обеспечит более совершенную безопасность, чем если оставлять в политике и регламентах неточности и неясности.

Кроме того, организации должны обеспечивать четкость понимания того, что в политике является требованием, а что — пожеланием. Такая четкость обеспечивается использованием глаголов вроде «должен», «следует», «может» и «является». Эти слова могут быть уточнены во вступительных разделах текста политики. «Должен» используется в контексте требований; «следует» используется в контексте рекомендаций. «Может» используется в контексте пожелания, которое является необязательным. Может быть целесообразно предусмотреть варианты изложения требования. Фразы типа «там, где возможно» или «при необходимости» вносят неясность, если только при этом не описано, как отличить контекст возможности от контекста необходимости.

Политики и регламенты безопасности устанавливают, кто и за что отвечает: отвечает ли технологический персонал за управляющую сеть, отвечает ли он за DMZ, расположенную между управляющей сетью и корпоративной сетью. В случае, если отдел корпоративных информационных систем

отвечает за условия, требующие от технологического персонала выполнения тех или иных действий, то эти действия должны быть по возможности прописаны.

Для организации, которая только начинает создавать свою программу безопасности, политики и регламенты — это хорошая отправная точка. Будучи составлены, они могут сначала охватывать набор норм безопасности, которые организация способна соблюсти в ближайшей перспективе благодаря наличию необходимого оборудования. Со временем они могут быть пересмотрены и ужесточены по мере роста возможностей организации. Они могут быть введены в действие без задержки на приобретение и установку систем и устройств.

5.8.2 Политика уровня предприятия

Политика уровня предприятия санкционирует программу безопасности и обозначает курс. Она устанавливает общие цели безопасности организации.

Формулировка основных положений политики, определяемая высшим руковод-ством, должна быть достаточно продуманна и оставаться и адекватной и точной при изменениях в структуре организации, в системе и технологиях безопасности, а также изменений характера угроз безопасности. Будучи продуманной, политика может оставаться неизменной и будет нуждаться в переработке только в случае кардинального изменения позиции организации в отношении безопасности. Однако формулировка политики должна быть однозначной, четко устанавливать, что требуется.

Политика уровня предприятия определяет участки ответственности и устанавливает подотчетность для таких участков. Политика может определять взаимосвязи между работой IT-отдела и работой завода и устанавливать сферы их компетенций. Политика может дифференцировать цели безопасности системы управления от целей безопасности корпоративной сети. Например, важнейшим аспектом безопасности корпоративной сети может быть обеспечение конфиденциальности в ней, а важнейшим аспектом безопасности системы управления может быть обеспечение ее бесперебойной работы.

Кроме того, политика устанавливает конкретные стандарты и нормы, применимые для организации. Она может определять инструктаж как важную составляющую программы безопасности. Политика может также устанавливать санкции за ее нарушения.

Руководству следует доводить политику до сведения сотрудников всей организации так, чтобы все сотрудники понимали ее.

5.8.3 Операционные политики и регламенты

Операционные политики и регламенты безопасности разрабатывают на более низких уровнях организации и определяют способ реализации политики уровня предприятия в конкретной совокупности обстоятельств. Регламенты безопасности претворяют политику в действие. Регламенты устанавливают, что должна предпринять организация для достижения целей политики и выполнения ее требований. Регламенты определяют процессы, которые позволят устранить все проблемы, обозначенные политикой.

Регламенты отражают все обязательные составляющие программы безопасности, которые включают в себя:

a) конструирование системы;

b) материально-техническое обеспечение;

c) монтаж;

d) технологический процесс;

e) техническое обслуживание систем;

f) персонал;

g) аудит;

h) инструктаж.

Регламенты определяют конкретные действия, лиц, ответственных за их выполнение, и условия для их выполнения.

Письменные регламенты прописывают порядок их изменения в случае изменения ситуации. За каждой политикой или регламентом закреплено лицо, отвечающее за сроки внесения обновлений и обеспечение их внесения.

Политики и регламенты следует оценивать на предмет их эффективности, которая покажет, служат ли они своему предполагаемому назначению. Следует также измерять финансовые затраты для организации, чтобы она могла определять, согласуется ли итог снижения риска с финансовыми затратами на реализацию политики. Если итог неприемлем, то политику и регламенты может потре-

боваться скорректировать. Регламенты необходимо пересматривать, если произошли изменения в технологиях.

Регламенты могут использоваться аудитами. Аудит безопасности устанавливает соответствие выявленных действий организации письменным регламентам.

5.8.4 Задачи, решаемые с помощью политик и регламентов

5.8.4.1 Общие положения

Существует ряд задач, которые могут решать политики и регламенты безопасности. Каждая организация уникальна и должна по возможности устанавливать соответствующие политики и регламенты безопасности, которые применимы для ее систем промышленной автоматики и контроля. Такие задачи могут включать в себя:

- управление риском;
- управление доступом;
- доступность и планирование бесперебойности;
- физическую безопасность;
- архитектуру;
- портативные устройства;
- беспроводные устройства и датчики;
- удаленный доступ;
- персонал;
- политику субподряда;
- аудит;
- обновление политики безопасности.

5.8.4.2 Управление риском

Управление риском играет крайне важную роль при разработке экономичной программы безопасности, которая обеспечивает одинаковый уровень приемлемой безопасности, но не требует оборудования или регламентов, которые обходятся слишком дорого и находятся за рамками требуемой безопасности. Тем не менее, управление риском сложно и поэтому должно быть приспособлено к конкретной организации. Политика управления риском устанавливает, как определять приемлемый уровень риска и как управлять риском. Этот уровень варьируется в зависимости от целей и обстоятельств отдельно взятой организации. Процесс определения уровня риска следует периодически повторять для приведения его в соответствие с изменениями окружающей обстановки.

5.8.4.3 Управление доступом

Безопасность системы повышают путем ограничения доступа в пользу лишь тех пользователей, которые нуждаются в доступе и наделены правом на него. Политика управления доступом устанавливает различные функции пользователей и какой род доступа необходим для каждой функции применительно к каждому классу имущественных объектов (физических или логических). Такая политика прописывает обязанности наемных работников в деле защиты имущественных объектов и обязанности руководителей в деле обслуживания регламентов управления доступом. Санкционирование привилегий доступа должно быть по возможности одобрено руководством и убедительно отражено в документах, а также периодически пересматриваться. Управление доступом может быть так же важно и даже важнее для обеспечения целостности и доступности системы, чем необходимость сохранения конфиденциальности данных.

5.8.4.4 Доступность и планирование бесперебойности

Политика в этой области предусматривает необходимую концепцию и ожидаемые требования к резервированию и восстановлению, а также планированию ведения бизнеса и восстановления после чрезвычайных происшествий. Она определяет также параметры архивирования (например, как долго следует сохранять данные).

5.8.4.5 Физическая безопасность

Безопасность системы управления зависит от физической защищенности пространства, которое включает в себя систему управления. Для заводской территории может быть прописана политика безопасности еще до того, как политика безопасности будет прописана для системы управления. Однако политика физического доступа к определенным системам может отличаться от политики, относящейся к объектам из других систем. Например, весь персонал нефтеперерабатывающего завода может иметь общий доступ практически ко всем техническим средствам в пределах стен завода, однако доступ к помещениям IT-инфраструктуры может быть ограничен лишь в пользу персонала, имеющему отношение к информационной технике — хотя бы в целях предотвращения случайных

повреждений. Политика безопасности системы управления должна по возможности включать в себя ссылку на политику физической безопасности и устанавливать ее зависимость. Политика безопасности системы управления должна по возможности содержать достаточно подробные данные о физической безопасности для того, чтобы можно было в каждом конкретном случае распространить политику безопасности заводского объекта на систему управления. Например, в такой политике может значиться: «такое-то оборудование должно находиться в закрытых кабинетах, а ключи к ним — храниться в месте ограниченного доступа».

5.8.4.6 Архитектура

Политика и регламенты описывают безопасные конфигурации систем управления, охватывая такие вопросы, как:

a) рекомендуемые компоновки сетей;

b) рекомендуемая конфигурация межсетевого экрана;

c) авторизация и аутентификация пользователей;

d) соединение между различными сетями управления процессами;

e) использование беспроводных коммуникаций;

f) домены и доверительные отношения;

g) управление патчами (включая аутентификацию);

h) управление антивирусами;

i) усиление защиты систем за счет закрытия программных портов, блокировки или отказа от неиспользуемых или опасных сервисов и отказа от использования съемных накопителей данных;

j) доступ к внешним сетям (т. е. к Интернету);

k) надлежащее использование электронной почты.

5.8.4.7 Портативные устройства

Портативным устройствам соответствуют все риски безопасности, которые соответствуют стационарному оборудованию, но из-за их мобильности менее вероятно, что на них удастся распространить обычные регламенты безопасности на протяжении всего периода от монтажа до аудита. Портативность таких устройств создает дополнительный риск для их повреждений, когда они находятся за пределами зон физической безопасности, или для перехвата информации в ходе их соединения с защищенными зонами. Таким образом, часто необходима специальная политика, которая распространяется на портативные устройства. Такая политика должна по возможности устанавливать требования к защите безопасности, которые аналогичны требованиям к тому или иному стационарному устройству, однако технические и административные механизмы, обеспечивающие эту защиту, могут отличаться.

5.8.4.8 Беспроводные устройства и датчики

Уже много лет в некоторых сферах в качестве управляющих систем широко применяется управляющее оборудование, которое использует радиочастотную передачу сигнала взамен проводной. По мере снижения финансовых расходов и появления новых стандартов расширяется сфера применения систем промышленной автоматики и контроля, что отчасти обусловлено меньшими финансовыми расходами на монтаж. Ключевым отличием проводных устройств от беспроводных является то, что в случае последних сигналы не ограничены пределами области физической безопасности, а это увеличивает риск их перехвата и искажения. Таким образом, политика безопасности, относящаяся именно к беспроводным устройствам, подходит для организаций, которые в данный момент используют или могут использовать в будущем в своей работе беспроводные устройства или датчики. Такая политика может регламентировать, для каких задач могут использоваться беспроводные устройства, какие методы защиты и управления требуются и как взаимосвязаны проводные и беспроводные сети.

5.8.4.9 Удаленный доступ

Удаленный доступ позволяет обойти средства обеспечения локальной физической безопасности, установленные на границах системы. Он позволяет перенести доступ к доверенной зоне в совершенно другую географическую точку и предполагает, среди прочего, использование компьютера, который мог не быть подвергнут проверкам безопасности, проводимым для компьютеров, находящихся физически в пределах доверенной зоны. Необходимы другие механизмы, которые обеспечивают за пределами доверенной зоны уровень безопасности, аналогичный уровню безопасности доверенной зоны.

5.8.4.10 Персонал

Вопросы, относящиеся к персоналу, могут быть обозначены в политиках безопасности предприятия для персонала и информационной технологии. Политика безопасности системы управления ох-

ватывает специфические подробности, в то время как более общая политика не охватывает аспекты систем управления. Например, политика безопасности систем управления согласует роли доступа к системам управления с методиками отбора и контроля местонахождения персонала.

5.8.4.11 Политика субподряда

Вопросы безопасности затрагивают деятельность, которая может требовать привлечения субподрядчиков в лице поставщика, сборщика, поставщика услуг технического обслуживания, консультанта и др. Политика безопасности, предусматривающая субподряд, рассматривает взаимодействия с субподрядчиком, который может открывать уязвимости. Политика определяет обязанности различных сторон. Политика учитывает изменение обязанностей по мере перехода проектов из этапа в этап и по мере поставки материалов и систем. Политика может требовать прописания в контрактах с субподрядчиками определенных сроков.

Без надлежащей организации работ контрактных (сторонних) программистов целостность прикладных программ и процессов может быть поставлена под угрозу, а программный код потерять поддержку. Важно найти квалифицированных контрактных программистов, которые будут придерживаться организационных стандартов программирования и документирования и выполнять надлежащие тестирования, а также будут надежными и соблюдать сроки разработки.

5.8.4.12 Аудит

Безопасность системы регулярно подвергают аудиту для определения степени соответствия безопасности политике и нормам безопасности. Политика безопасности учитывает необходимость аудитов и устанавливает ответственность, периодичность и требования к корректирующим воздействиям. Всесторонняя процедура аудита может затрагивать аспекты, отличные от безопасности, например, эффективность и результативность процессов, а также их нормативно-правовое соответствие.

5.8.4.13 Обновление политики безопасности

Политику безопасности подвергают мониторингу для определения изменений, необходимых в политике как таковой. Мониторинг политики безопасности — это обязательный раздел каждого документа, содержащего политику и регламент. Политика безопасности предприятия устанавливает общий подход. В каждом документе, содержащем операционную политику и регламент, приведены инструкции на предмет того, когда и кем должна быть пересмотрена и обновлена политика или регламент как таковые.

Должны по возможности действовать программы инструктажа ввиду найма новых работников, новых операций эксплуатации и технического обслуживания, модернизаций и планирования преемственности. Программы инструктажа следует надлежащим образом документировать, структурировать и дорабатывать с регулярной периодичностью для учета изменений в операционной среде.

5.9 Зоны безопасности

5.9.1 Общие положения

Каждой ситуации соответствует свой допустимый уровень безопасности. В случае крупных или сложных систем может быть нецелесообразно или не следует применять один и тот же уровень безопасности для всех компонентов. Различия можно учитывать, используя понятие зоны безопасности или защищаемого участка. Зона безопасности представляет собой логическое объединение физических, информационных и прикладных объектов имущества, к которым предъявляются общие требования безопасности. Это понятие применимо к электронной среде, в которой некоторые системы входят в состав зоны безопасности, а все остальные находятся за ее пределами. Могут существовать также зоны внутри зон или подзоны, которые обеспечивают многоуровневую (эшелонированную) защиту, соответствуя серии уровней требований безопасности. Эшелонированная защита может быть обеспечена за счет присвоения различных свойств ее зонам безопасности.

Зона безопасности имеет границу, которая представляет собой рубеж между элементами, принадлежащими ей и элементами ей не принадлежащими. Концепция зоны предполагает также обязательную возможность доступа к объектам, находящимся как внутри зоны, так и вне ее. Это определяет коммуникацию и доступ, необходимые для перемещения информации и людей внутри зон безопасности и между ними. Зоны можно рассматривать как надежные и ненадежные.

Зоны безопасности могут быть определены в физическом смысле (физическая зона) или логическом смысле (виртуальная зона). Физические зоны определены посредством группировки объектов по их физическому местоположению. В случае зон такого типа легко установить, какие объекты находятся внутри каждой зоны. Виртуальные зоны определены посредством группировки физических

объектов или их частей в зоны безопасности на основе функциональности или других характеристик объектов, чем их фактического местоположения.

5.9.2 Определение требований

5.9.2.1 Общие положения

При определении зоны безопасности организации следует сначала определиться с требованиями безопасности (целями безопасности) и лишь затем решать, следует ли рассматривать конкретный объект в качестве находящегося внутри зоны или за ее пределами. Требования безопасности можно подразделить на следующие типы:

- коммуникационный доступ;
- физический доступ и удаленность.

5.9.2.2 Коммуникационный доступ

Чтобы группа объектов, находящихся в пределах границы безопасности, нормально функционировала, они должны быть связаны с объектами, находящимися за пределами зоны безопасности. Такой доступ может иметь множество форм, в числе которых физическое перемещение объектов (изделий) и людей (служащих и поставщиков) или электронная коммуникация с субъектами, находящимися за пределами зоны безопасности.

Удаленная коммуникация — это передача информации от одного субъекта к другому, которые находятся на значительном удалении друг от друга. В контексте настоящего стандарта удаленный доступ определен как коммуникация с объектами, находящимися за пределами периметра рассматриваемой зоны безопасности.

Локальный доступ обычно рассматривают как коммуникацию между объектами в пределах одной зоны безопасности.

5.9.2.3 Физический доступ и удаленность

Физические зоны безопасности служат для ограничения доступа к конкретному участку, ввиду того, что все системы на этом участке требуют одинаковой степени надежности операторов, обслуживающего персонала и разработчиков. При этом не исключено, что зона с более низким уровнем физической безопасности может содержать зону с более высоким уровнем физической безопасности, или зона с более низким уровнем физической безопасности может содержать зону высокоуровневого коммуникационного доступа. В случае физических зон замки на дверях или другие физические средства защищают от несанкционированного доступа. Преградой является стена или кабинет, которые сдерживают доступ. Физические зоны должны по возможности иметь физические барьеры, которые соответствуют требуемому уровню безопасности и согласуются с планами относительно безопасности других объектов.

Примером физической зоны безопасности является обычный завод. Авторизованные лица пропускаются на завод авторизующим субъектом (сотрудником охраны или идентификационным терминалом), а доступ на завод неавторизованных лиц сдерживается тем же авторизующим субъектом и оградой.

Объекты в пределах границы безопасности — это объекты, которые нуждают- ся в защите на установленном уровне безопасности или в соответствии с установленной политикой. Все устройства, находящиеся в пределах этой границы, должны соответствовать одному и тому же минимальному уровню требований безопасности. То есть они должны быть по возможности защищены в соответствии с одной и той же политикой безопасности. Механизмы защиты могут различаться в зависимости от защищаемого объекта.

Объекты, находящиеся за пределами зоны безопасности, удовлетворяют по определению меньшему или иному уровню безопасности. Эти объекты защищены на разных уровнях безопасности и по определению уже не могут быть доверены одному и тому же уровню безопасности или политике.

5.10 Тракты

5.10.1 Общие положения

Информация должна поступать в зону безопасности, выходить из этой зоны безопасности и перемещаться в ее пределах. Даже в несвязанной системе присутствует некоторая коммуникация (например, периодическое соединение между собой программирующих устройств для создания и обслуживания систем). Чтобы охватить аспекты безопасности коммуникации и создать концепцию, затрагивающую уникальные требования к коммуникациям, в настоящем стандарте определен особый тип зоны безопасности — коммуникационный тракт.

Тракт — это особый тип зоны безопасности, группирующей информационные взаимодействия, способные быть логически организованы в группу информационных потоков, распространяющихся внутри зоны и вне ее. Тракт может представлять собой единый сервис (т. е. единую сеть Интернет) или быть образован серией переносчиков информации (серией сетевых кабелей и прямых физических доступов). Как и зона, тракт может быть образован как физическими, так и логическими компонентами. Тракты могут связывать между собой субъекты в пределах одной зоны или связывать между собой различные зоны.

Как и зоны, тракты могут быть доверенными или недоверенными. Тракты, не пересекающие границ зоны, обычно являются доверенными до уровня коммуникационных процессов в пределах этой зоны. В доверенных трактах, пересекающих границы зоны, необходимо реализовывать сквозной доверенный процесс.

Недоверенные тракты — это тракты, уровень безопасности которых отличен от уровня безопасности крайней точки зоны. В этом случае фактическая безопасность коммуникации сводится к безопасности отдельного канала, как показано на рисунке 7.

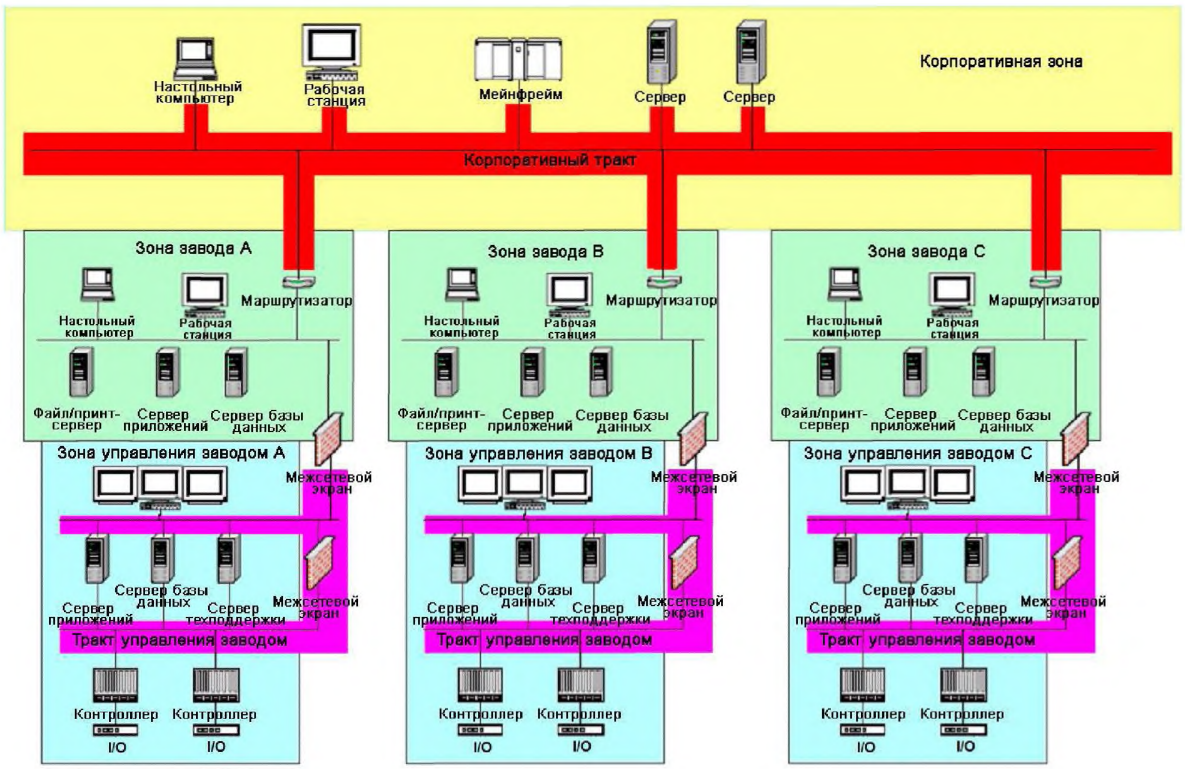

Рисунок 7 — Пример тракта

На рисунке 7 изображена организация, включающая в себя три завода и отдельный центральный офис. Каждый из трех заводов связан с корпоративной сетью для обеспечения обмена данными между отдельно взятым заводом и центральным офисом, а также другими заводами. На рисунке обозначено четыре возможных тракта (возможны и другие тракты, но для наглядности они опущены). Первый из них — корпоративный тракт, показанный в верхней части рисунка. Данный тракт связывает несколько заводов, расположенных на разных территориях, с корпоративным дата-центром. Если WAN сформирована с использованием выделенных или частных линий связи, то такую сеть можно считать надежным трактом. Если в такой сети использованы как общедоступные, так и частные сети, то ее можно отнести к ненадежному тракту. В состав тракта входит любое коммуникационное оборудование и межсетевые экраны, которые образуют связные линии заводов.

Варианты ненадежных трактов показаны на каждом заводе. В данном случае каждый завод содержит свой собственный доверенный тракт для передачи управляющих воздействий.

5.10.2 Каналы

Каналы — это особые линии связи, созданные внутри коммуникационного тракта. Каналы повторяют свойства безопасности тракта, используемого в качестве коммуникационной среды (т. е. канал, находящийся внутри защищенного тракта, будет поддерживать уровень безопасности защищенного тракта). Каналы могут быть надежными или ненадежными.

Доверенные каналы — это связные линии, обеспечивающие защищенный обмен данными с другими зонами безопасности. Надежный канал может использоваться для расширения виртуальной зоны безопасности с целью включения в нее субъектов, находящихся за пределами физической зоны безопасности.

Недоверенные каналы — это связные линии, уровень безопасности которых отличен от уровня безопасности рассматриваемой зоны безопасности. Правильность передачи данных в рассматриваемую зону и из нее (зону, которая определяет незащищенный обмен данных) должна быть проверена перед принятием информации.

5.11 Уровни безопасности

5.11.1 Общие положения

Концепция уровней безопасности была создана для того, чтобы привязать понятие безопасности к зонам, а не к отдельным устройствам или системам. Как правило, IACS состоит из устройств и систем, полученных от нескольких поставщиков, причем все эти устройства и системы функционируют совместно, обеспечивая целостные функции автоматического управления промышленным процессом. Аналогично тому, как функциональные возможности отдельных устройств влияют на возможности IACS, параметры безопасности отдельных устройств и реализуемых контрмер должны быть согласованы между собой для достижения требуемого уровня безопасности зоны. Уровни безопасности обеспечивают систему критериев для принятия решений о применении контрмер и устройств с различающимися параметрами собственной безопасности.

Уровни безопасности обеспечивают качественный подход к решению вопросов, относящихся к безопасности зоны. Установление уровня безопасности целесообразно применять для качественного сравнения уровней безопасности. По мере увеличения количества доступных данных и разработки математических моделей риска, угроз и инцидентов безопасности данная концепция будет сводиться к количественному методу выбора и верификации уровней безопасности (SL). Эта концепция будет применима как к организациям-потребителям, так и к поставщикам IACS и продуктов безопасности. Она будет использоваться при выборе устройств IACS и контрмер с целью их применения в отдельно взятой зоне, а также при определении и сравнении безопасности зон в организациях различных сегментов промышленности.

Каждой организации, применяющей метод SL, следует дать определение того, что отражает каждый уровень и как измерять SL зоны. Это определение или характеристику следует применять на систематической основе в масштабе всей организации. SL может применяться для определения стратегии полноценной многоуровневой эшелонированной защиты зоны, причем эта стратегия включает в себя технические контрмеры на основе аппаратных и программных средств, а также административные контрмеры.

SL соответствует требуемой эффективности контрмер и внутренне присущих свойств безопасности устройств и систем для зоны или тракта с учетом оценки риска для этой зоны или тракта. Метод SL позволяет категоризировать риск для зоны или тракта. Метод SL помогает также определять требуемую эффективность контрмер, применяемых для предотвращения несанкционированного электронного вмешательства, которое способно привести к утечке данных или воздействию на нормальное функционирование устройств и систем в пределах зоны или тракта. SL — это свойство скорее зоны и тракта, чем устройства, системы или любой ее части.

Рекомендован минимум из трех SL. Эти три уровня можно охарактеризовать качественно, как показано в таблице 8. Организации могут предпочесть расширить количество имеющиеся SL и определить дополнительные уровни для описания своих уникальных требований безопасности.

Таблица 8 — Уровни безопасности (SL)

Уровень безопасности	Качественная характеристика
1	Низкий
2	Средний
3	Высокий

5.11.2 Типы уровней безопасности (SL)

5.11.2.1 Общие положения

Могут быть определены три типа SL:

a) SL (целевой) — целевой уровень безопасности зоны или тракта;

b) SL (достигнутый) — достигнутый уровень безопасности зоны или тракта;

c) SL (потенциальный) — потенциальный уровень безопасности контрмер, привязанных к зоне или тракту, или потенциальный уровень внутренне присущей безопасности устройств или систем внутри зоны или тракта.

5.11.2.2 SL (целевой) — целевой уровень безопасности

SL (целевой) следует назначать зоне. SL (целевой) может быть назначен и тракту. SL (целевой) зоны или тракта определяют в ходе оценки рисков. Не следует назначать SL (целевой) трактам, если параметры безопасности тракта учитываются в ходе оценки рисков зон, которые используют рассматриваемый тракт. Оценка риска зоны или тракта должна по возможности учитывать вероятность нарушения безопасности и ее проявление

Оценка рисков может быть качественной, полуколичественной или количественной. SL (целевой) определяет необходимую эффективность контрмер, устройств и систем, которые должны быть задействованы для предотвращения нарушения безопасности зоны или тракта.

Контрмеры могут быть:

a) техническиими (межсетевые экраны, антивирусное программное обеспечение и т. д.);

b) административными (политика и регламенты);

c) физическиими (запертые двери и т. д.).

На определение SL (целевой) зоны и тракта влияют следующие факторы:

d) сетевая архитектура с определенными границами зон и трактами;

e) SL (целевой) зон, с которыми будет взаимодействовать рассматриваемая зона;

f) SL (целевой) тракта (если этот уровень назначен), используемого зоной для коммуникации;

g) физический доступ к устройствам и системам в пределах зоны.

Вычисление целевого уровня безопасности в пределах зоны следует основывать на уровнях безопасности и их влиянии на общую безопасность.

5.11.2.3 SL (достигнутый) — достигнутый уровень безопасности

SL (достигнутый) зоны или тракта зависит от внутренне присущих свойств безопасности устройств и систем внутри зоны или тракта и/или свойств контрмер, которые задействованы для предотвращения нарушения безопасности зоны или тракта. SL (достигнутый) является функцией от времени и снижается с течением времени из-за снижения эффективности контрмер, новых уязвимостей, эволюционировавших угроз или скорректированных методов атак, уязвимостей в уровнях безопасности и внутренне присущих свойств безопасности устройств и систем до их проверки, замены или модернизации.

Задача — обеспечить, что в тот или иной момент времени SL (достигнутый) зоны или тракта был больше или равен SL (целевой) этой зоны или тракта.

5.11.2.4 SL (потенциальный) — потенциальный уровень безопасности контрмер, устройств или систем

SL (потенциальный) определен для контрмер и внутренне присущих свойств безопасности устройств и систем внутри зоны или тракта, вносящих вклад в безопасность зоны или тракта, что является степенью эффективности контрмеры, устройства или системы в отношении свойства безопасности, которое они затрагивают.

Ниже приведены примеры свойств безопасности, которые могут затрагиваться контрмерой, устройством или системой:

a) подтверждение аутентичности равноуровневого субъекта;

b) сохранение аутентичности и целостности сообщений;

c) сохранение конфиденциальности сообщений/информации/коммуникации;

d) обеспечение отслеживаемости (защиты от непризнания участия);

e) обеспечение выполнения политики управления доступом;

f) предотвращение атак типа «отказ в обслуживании»;

g) обеспечение доверительности платформ;

h) выявление взломов;

i) отслеживание статуса безопасности.

SL (потенциальный) контрмеры, устройства или системы внутри зоны или тракта вносит вклад в SL (достигнутый) с учетом соответствующих свойств безопасности, которые затрагиваются контрмерами, устройствами или системами для этой зоны или тракта.

5.11.3 Факторы, влияющие на SL (достигнутый) зоны или тракта

5.11.3.1 Общие положения

Существует ряд факторов, влияющих на SL (достигнутый) зоны или тракта. SL (достигнутый) зоны или тракта может быть выражен в виде функции этих факторов:

SL (достигнутый) = f (x1, ... , xn, t),

где: факторы xi (1 < = i < = n) включают в себя, но не ограничиваются этим:

x1 — SL (потенциальный) контрмер, привязанных к зоне или тракту, и внутренне присущие свойства безопасности устройств и систем в пределах зоны или тракта;

x2 — SL (достигнутый) зон, с которыми предстоит установить коммуникации;

x3 — тип трактов и свойства безопасности, относящиеся к трактам, которые служат для коммуникации с другими зонами (относится только к зонам);

x4 — эффективность контрмер;

x5 — периодичность аудитов, и тестирования контрмер и внутренне присущих свойств безопасности устройств и систем в пределах зоны или тракта;

x6 — познания злоумышленников и ресурсы, доступные для злоумышленников;

x7 — снижение эффективности контрмер и внутренне присущих свойств устройств и систем;

x8 — выявление несанкционированных проникновений;

t — время.

Данные факторы подробнее описаны в нижеследующих подпунктах.

5.11.3.2 SL (потенциальный) контрмер и внутренне присущих свойств

Соответствующие свойства безопасности, затрагиваемые контрмерами, устройствами и системами в пределах зоны или тракта, и их эффективность, вносят вклад в SL (достигнутый) зоны или тракта.

Контрмеры способны затрагивать несколько свойств безопасности, но если ни одно из них не относится к безопасности зоны или тракта, то такие контрмеры не вносят вклада в SL (достигнутый) этой зоны или тракта. Аналогичным образом, если внутренне присущие свойства безопасности устройств и систем в пределах зоны или тракта не имеют отношения к безопасности этой зоны или тракта, то эти свойства не вносят вклада в SL (достигнутый) этой зоны или тракта.

5.11.3.3 SL (достигнутый) зон, с которыми предстоит установить коммуникацию

Безопасность зоны или тракта не может рассматриваться изолированно. На нее влияет SL (достигнутый) зон, с которыми они осуществляют коммуникацию.

Рассмотрим, например, SIS на химическом заводе, которая осуществляет коммуникацию с DCS через последовательный канал. Если предположить, что DCS и SIS находятся в двух разных зонах, то на SL (достигнутый) зоны SIS будет влиять SL (достигнутый) зоны DCS.

5.11.3.4 Тип трактов и относящиеся к ним свойства безопасности

Тракт может представлять собой линию связи «точка — точка», LAN или WAN с внутренне присущими свойствами безопасности. Тракт может включать в себя контрмеры, которые улучшают свойства безопасности тракта. Свойства безопасности тракта, вносящие вклад в безопасность тракта, будут вносить вклад и в SL (достигнутый) тракта. Свойства безопасности тракта, используемого зоной для осуществления коммуникации с другими зонами, будут вносить вклад в SL (достигнутый) зоны.

5.11.3.5 Эффективность контрмер

Могут быть реализованы технические и административные контрмеры, которые позволяют достичь требуемого SL (целевой) зоны или тракта.

В контексте IACS доступны разнообразные технические контрмеры, затрагивающие различные свойства безопасности. Технические контрмеры должны по возможности затрагивать свойства безопасности, относящиеся к данной конкретной зоне, но если такие свойства безопасности неэффективны для этой зоны, то их вклад в SL (достигнутый) зоны будет крайне незначителен или вообще нулевым. Примеры технических контрмер включают в себя системы обнаружения несанкционированных проникновений (IDS), межсетевые экраны и антивирусное программное обеспечение.

Оценка эффективности технических контрмер должна по возможности учитывать следующее:

a) процесс разработки: доступность письменных регламентов, плана управления качеством и т. д. Это поможет сократить систематические ошибки, например, ошибки в программном обеспечении или утечки памяти, которые могут отражаться на безопасности;

b) тестирование: уровень тестирования каждого свойства безопасности, которое затрагивают контрмеры, устройство или система. Данные тестирований могут быть выведены и на основе оценок предшествующих систем;

c) сбор данных: количество случаев нарушения безопасности зоны или тракта из-за несовершенства аналогичной контрмеры, устройства или системы; степень и серьезность уязвимостей, выявленных для контрмеры, устройства или системы.

Если технические контрмеры неосуществимы или нецелесообразны, то следует применять административные контрмеры. Примером административной меры является ограничение физического доступа к компонентам IACS.

5.11.3.6 Периодичность аудитов и тестирований контрмер

Эффективность контрмер и внутренне присущих свойств безопасности устройств и систем должна по возможности подвергаться аудитам и/или оценкам с регулярной периодичностью и на базе регламентов, которые позволяют аудировать и/или тестировать по меньшей мере те свойства безопасности, которые относятся к зоне. В некоторых случаях поводом к аудиту или тестированию может послужить и обнаружение новых уязвимостей.

5.11.3.7 Познания злоумышленника и ресурсы, доступные злоумышленнику

На SL (достигнутый) зоны или тракта влияют познания злоумышленника и доступные ему ресурсы, в числе которых различные инструменты и время. Следует брать в расчет средства и инструменты злоумышленников, характерные для отрасли. Время, имеющееся в распоряжении злоумышленника для нарушения безопасности зоны, будет зависеть от конкретной задачи и контрмер, реализованных для данной зоны или тракта.

5.11.3.8 Снижение эффективности контрмер

Эффективность контрмер и внутренне присущих свойств устройств и систем будет существенно снижаться со временем, что приведет к снижению SL (достигнутый) зоны или тракта. Эффективность контрмер и внутренне присущих свойств устройств и систем снижается по следующим причинам:

a) обнаружение новых уязвимостей;

b) повышение мастерства злоумышленников;

c) повышение осведомленности злоумышленников о существующих контрмерах;

d) получение злоумышленниками доступа к более эффективным ресурсам.

5.11.3.9 Выявление несанкционированных проникновений

Контрмеры и внутренне присущие свойства безопасности устройств и систем могут включать в себя выявление несанкционированных проникновений. На SL (достигнутый) зоны и тракта влияет время, доступное для реагирования на выявленное несанкционированное проникновение.

5.11.4 Влияние контрмер и внутренне присущих свойств безопасности устройств и систем

Использование контрмер и внутренне присущих свойств безопасности устройств и систем для достижения SL (целевой) может приводить к снижению эффективности коммуникации. Необходимо оценивать снижение эффективности коммуникации из-за контрмер и внутренне присущих свойств безопасности устройств и систем, чтобы гарантировать выполнение минимальных функциональных требований, предъявляемых к зоне.

Например, важным требованием к IACS является быстрота отклика. Контрмеры могут привносить в коммуникацию задержки во времени, что при выполнении определенных задач может быть недопустимо.

5.12 Жизненный цикл уровня безопасности

5.12.1 Общие положения

Уровни безопасности становятся важной составляющей жизненного цикла безопасности зоны IACS, как только определены границы зоны и тракты. Важно осознавать, что жизненный цикл уровня безопасности ориентирован на изменение уровня безопасности зоны или тракта во времени. Жизненный цикл уровня безопасности не следует путать с этапами жизненного цикла самих физических объектов, составляющих IACS в пределах зоны. Существует множество пересекающихся и дополняющих друг друга процессов, которые относятся как к жизненному циклу имущественных объектов, так и к жизненному циклу уровня безопасности зоны, однако всем этим процессам соответствуют разные пороговые точки для перехода от одного этапа к другому. Кроме того, изменение в физическом объекте может повлечь ряд действий, относящихся к уровню безопасности, или изменение в уязвимостях безопасности или объекте может повлечь изменение в физическом объекте.

На рисунке 8 показан жизненный цикл безопасности. На этапе «Оценка» жизненного цикла безопасности зоне назначают SL (целевой). На этапе «Реализация» реализуют контрмеры для достижения SL (целевой) зоны. SL (достигнутый) зоны зависит от разных факторов. Чтобы гарантировать, что SL (достигнутый) зоны выше или равен SL (целевой) этой зоны во всех случаях, контрмеры подвергают аудитам и/или тестированию и в случае необходимости дорабатывают на этапе «Поддержание» жизненного цикла безопасности.

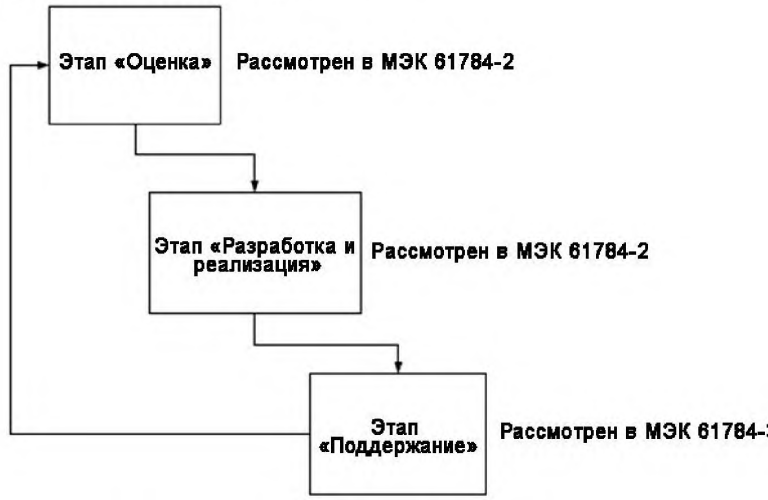

Рисунок 8 — Жизненный цикл безопасности

5.12.2 Этап «Оценка»

Этап «Оценка» жизненного цикла безопасности включает в себя действия, указанные на рисунке 9. Перед назначением зоне SL (целевой) необходимо установить:

a) границы зоны;

b) критерии допустимости риска для организации.

Следует выполнить оценку риска для зоны и назначить ей SL (целевой). Оценка риска и другие действия, относящиеся к этапу оценки, будут рассмотрены подробнее в последующей части МЭК 62443.

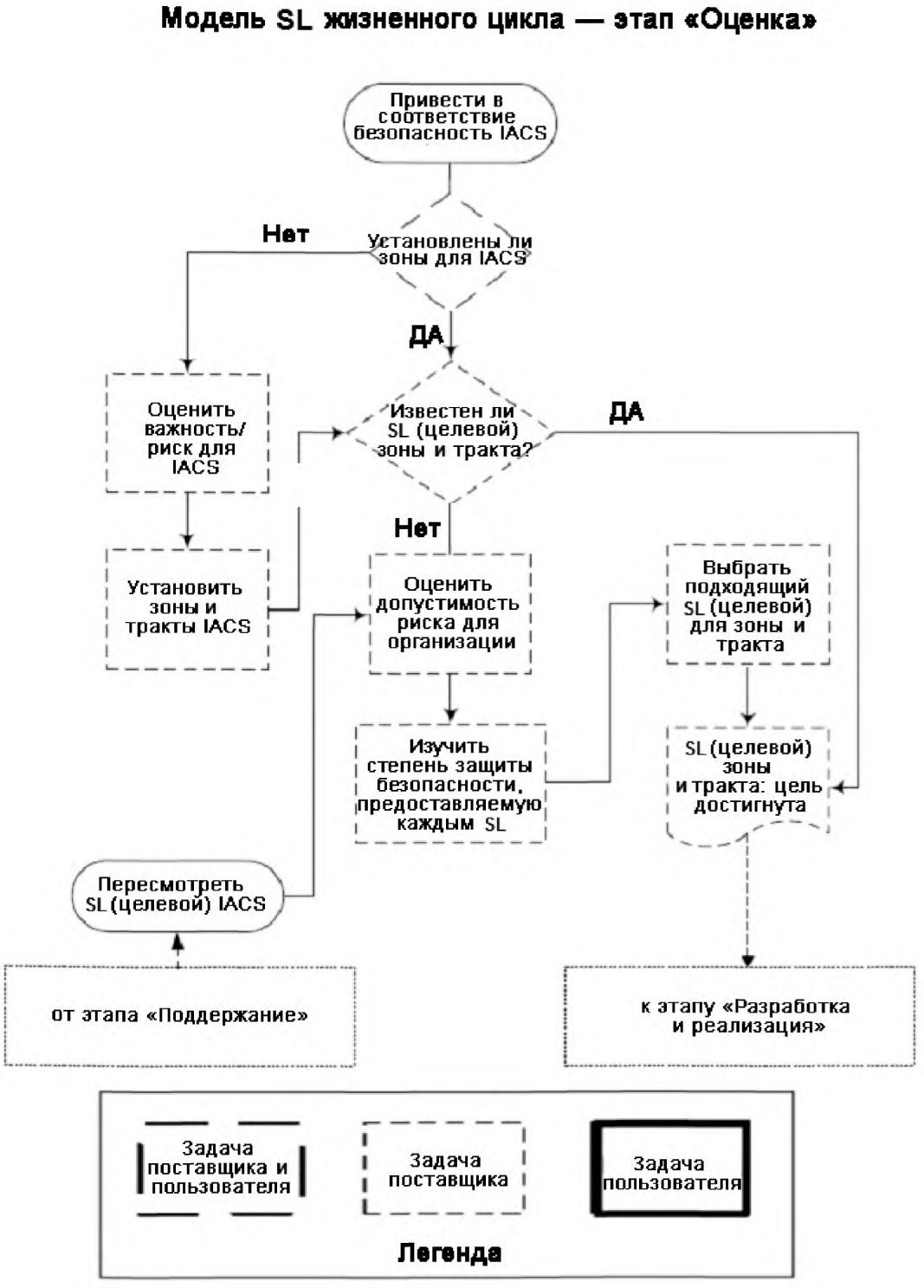

Рисунок 9 — Жизненный цикл SL — этап «Оценка»

5.12.3 Этап «Разработка и реализация»

Как только на этапе «Оценка» зоне назначен SL (целевой), следует реализовывать контрмеры, чтобы SL (достигнутый) зоны был выше или равен SL (целевой) этой зоны. На рисунке 10 указаны действия, выполняемые на этапе «Реализация» жизненного цикла SL, для новых и существующих зон IACS. SL (достигнутый) определяют после того, как система признана соответствующей требованиям безопасности для зоны.

Действия, относящиеся к этапу реализации, будут рассмотрены подробнее в последующей части МЭК 62443.

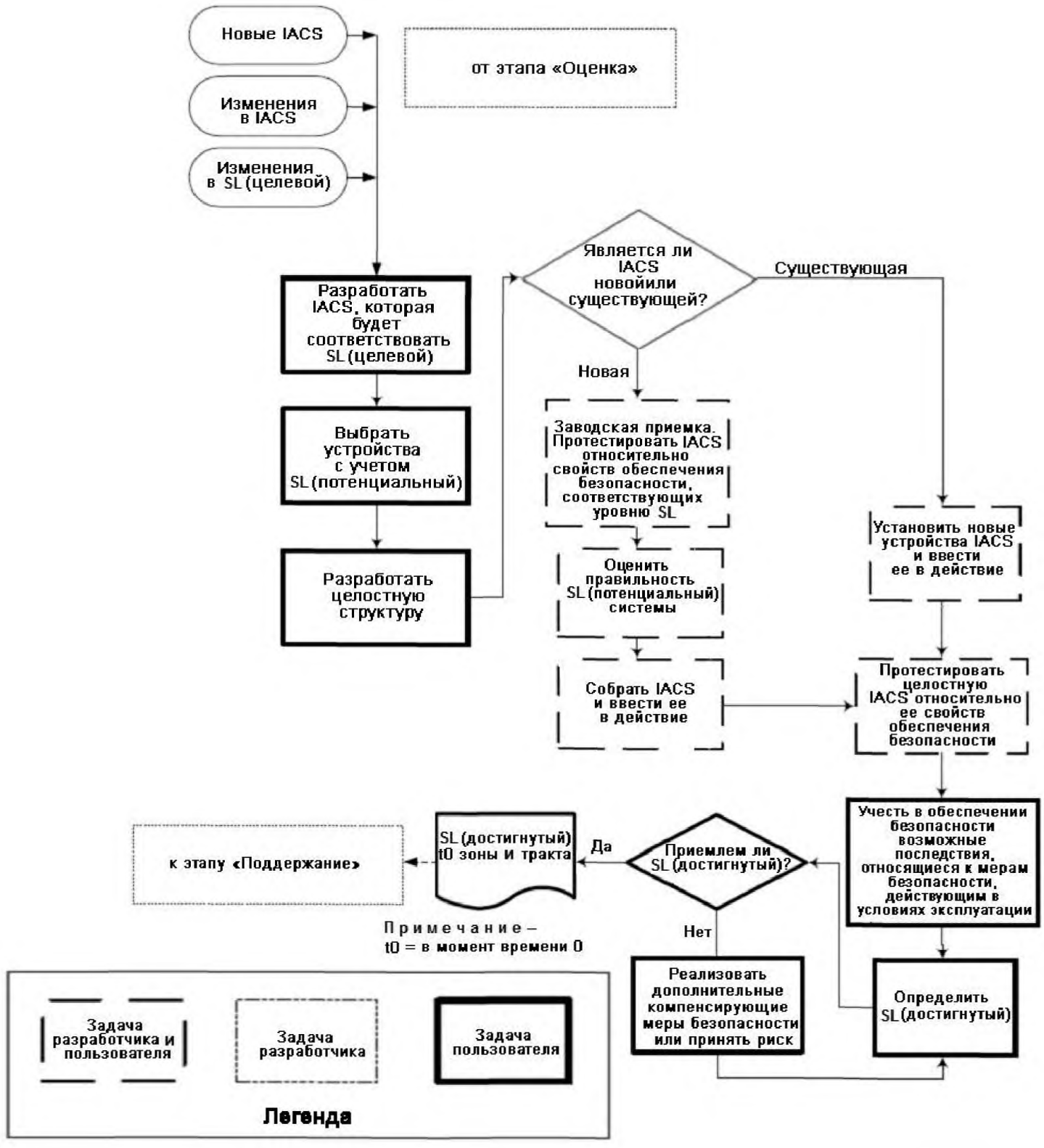

Рисунок 10 — Жизненный цикл SL — этап «Реализация»

5.12.4 Этап «Поддержание»

Контрмеры и внутренне присущие свойства безопасности устройств и систем со временем теряют свою эффективность. Свойства безопасности, относящиеся к зоне, в том числе к ассоциированным с ней трактам, следует подвергать аудитам и/или тестированиям с регулярной периодичностью или всякий раз при обнаружении новой уязвимости, чтобы SL (достигнутый) зоны был гарантированно больше или равен уровню SL (целевой) этой зоны во всех случаях. Действия, относящиеся к поддержанию SL (достигнутый), отмечены на рисунке 11.

Действия, относящиеся к этапу поддержания, будут рассмотрены подробнее в последующей части МЭК 62443.

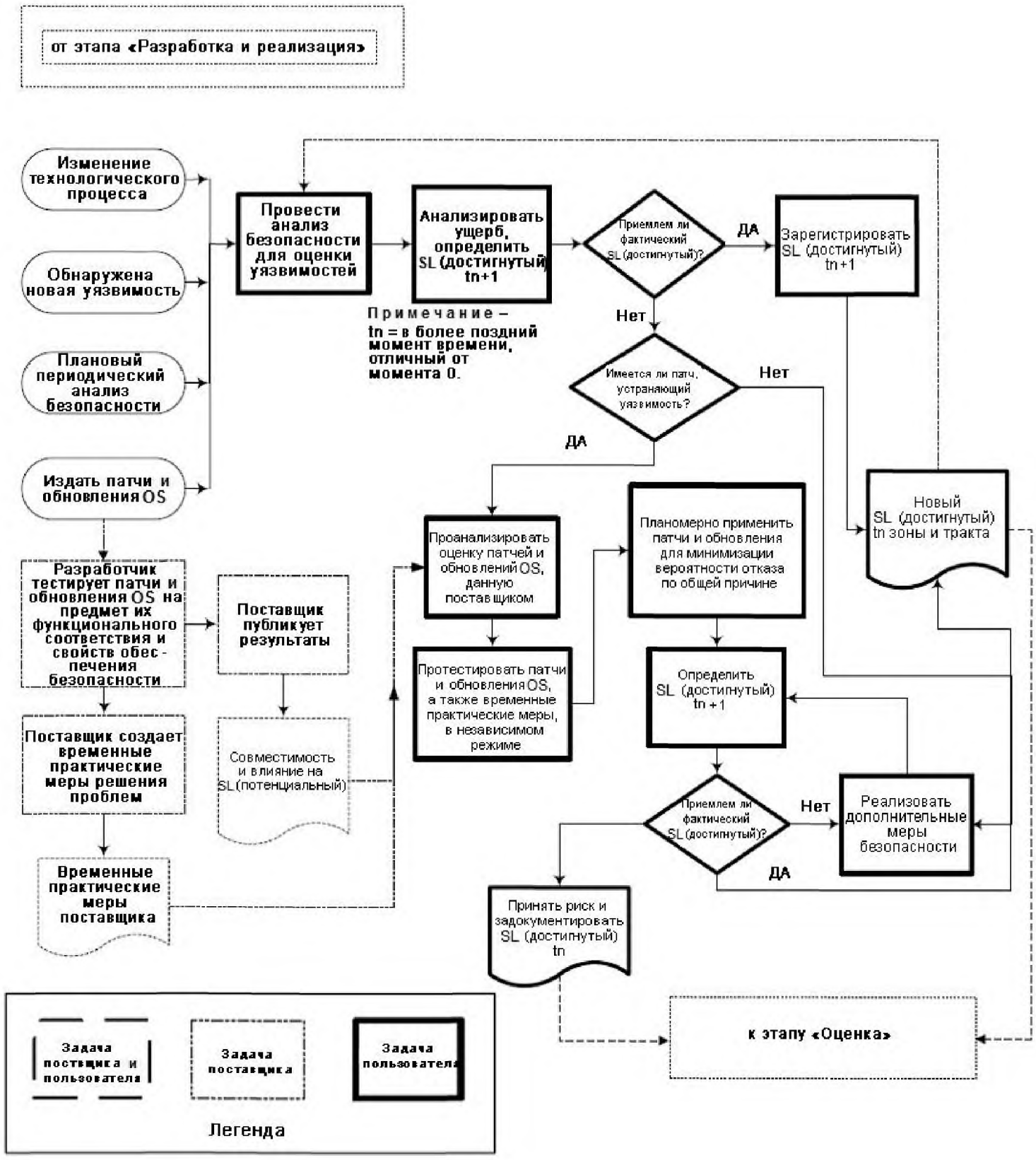

Рисунок 11 — Жизненный цикл SL — этап «Поддержание»

6 Модели

6.1 Общие положения

В настоящем разделе описана серия моделей, которая может использоваться при разработке соответствующей программы безопасности. Цель разработки — выявить требования к безопасности и важные характеристики среды на уровне детализации, необходимом для рассмотрения вопросов безопасности с общим пониманием кон-цепции и номенклатуры. Существует множество видов таких моделей, которые включают в себя:

a) базовые модели, которые обеспечивают общую концептуальную базу для более детальных моделей, указанных далее;

b) объектные модели, которые описывают отношения между имущественными объектами в структуре системы промышленной автоматики и контроля;

c) базовую архитектуру, которая описывает конфигурацию объектов. Базовая архитектура может быть уникальна для каждого предприятия или подмножества предприятий. Она уникальна для каждой ситуации и зависит от задач, которые решает рассматриваемая система промышленной автоматики и контроля;

d) зональную модель, которая группирует элементы базовой архитектуры по заданным характеристикам. Это обеспечивает контекст для определения политики, регламентов и директив, которые, в свою очередь, применяются к объектам.

Вся эта информация используется для разработки подробной программы управления безопасностью системы промышленной автоматики и контроля.

Каждый из основных типов моделей описан подробнее в настоящем разделе.

6.2 Базовые модели

6.2.1 Общие положения

Базовая модель устанавливает систему критериев для последующей более детальной информации. Термин «базовая модель» стал расхожим вместе с успехом семиуровневой модели ИСО для взаимодействия открытых систем (OSI). Бюро НАСА по стандартам и технологиям (NOST) (США) определяет этот термин следующим образом:

«Базовая модель — это концепция, которая проясняет существенные отношения между субъектами некой среды, позволяя разработать единые стандарты или спецификации, поддерживающие эту среду. Базовая модель основана на небольшом количестве обобщающих понятий и может использоваться как база для обучения и разъяснения стандартов неспециалисту».

Базовая модель характеризует исходный вид единой технологической или производственной системы, выраженный как серия логических уровней. Базовая модель, используемая в стандартах серии МЭК 62443, показана на рисунке 12. Эта модель получена из общей модели, использованной в МЭК 62264-1.

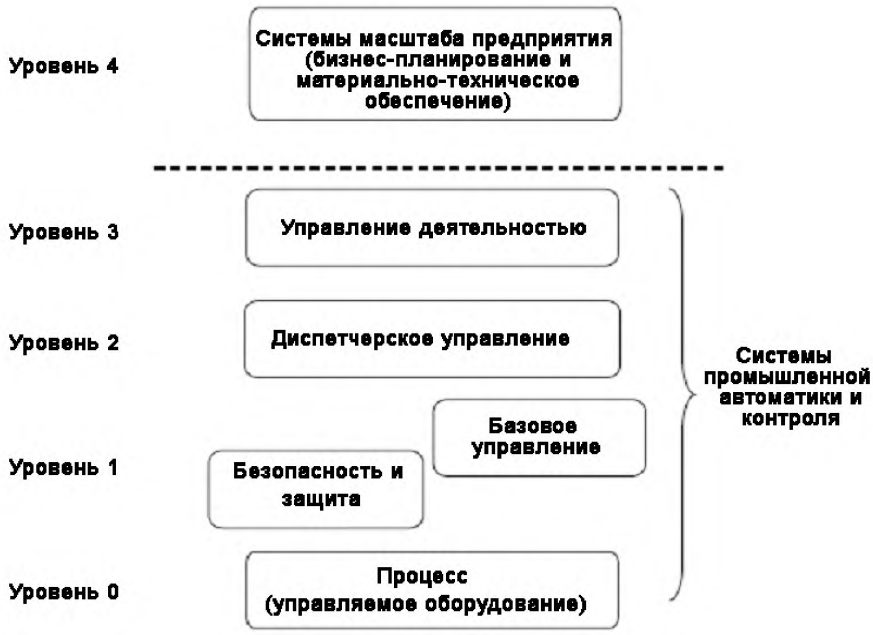

Рисунок 12 — Базовая модель по МЭК 62443

Для задач, решаемых с помощью SCADA, может использоваться базовая модель несколько иного вида. Такая модель показана на рисунке 13.

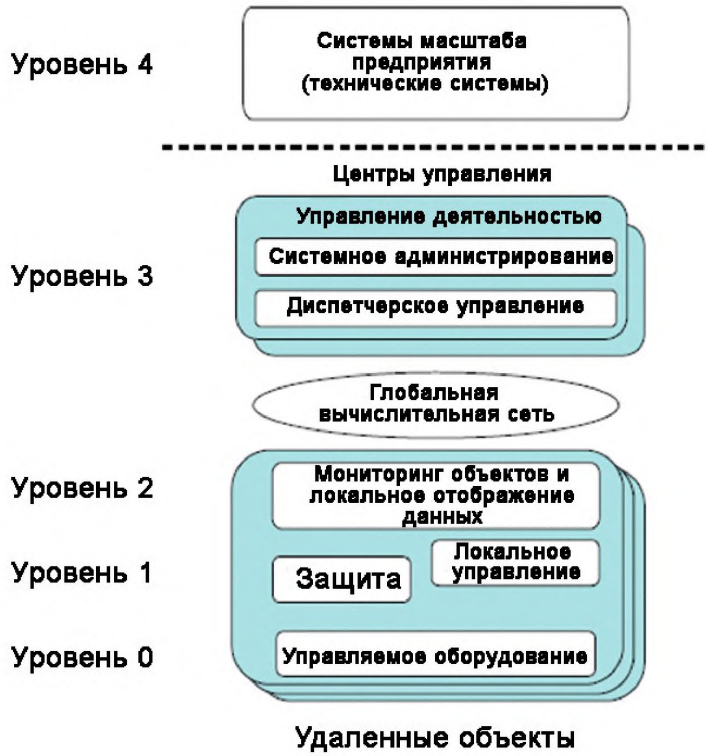

Рисунок 13 — Базовая модель SCADA

6.2.2 Уровни базовой модели

6.2.2.1 Общие положения

Обе вышеприведенные модели состоят из одинаковых базовых уровней, каждый из которых соответствует определенному классу функциональности. Определения уровней основаны на модели функциональной иерархии, приведенной в МЭК 62264-1 и описывают функции и действия начиная от уровня процесса (уровень 0) и заканчивая уровнем предприятия (уровень 4).

В 6.2.2.2–6.2.2.6 описан подробнее каждый из уровней данной модели.

6.2.2.2 Уровень 4 — Системы масштаба предприятия

Данный уровень, обозначенный в МЭК 62264-1 как бизнес-планирование и материально-техническое обеспечение, определен как включающий в себя функции, задействованные в бизнес-процессах, необходимые для управления производственной ор-

ганизацией. Функции распространяются на корпоративные или региональные финансовые системы и другие элементы корпоративной инфраструктуры, такие как планирование производства, операционное управление и управление жизнедеятельностью для отдельного завода или объекта предприятия. В контексте настоящего стандарта к этому уровню принадлежат и технические системы.

Действия уровня 4 включают в себя:

a) сбор данных и обеспечение расхода сырья и запчастей, а также накопление и обслуживание доступного запаса, и предоставление данных для закупки сырья и запчастей;

b) сбор данных и обеспечение общего расхода энергии, а также накопление и обслуживание доступного запаса, и предоставление данных для закупки энергоресурсов;

c) накопление и инвентаризация продукции в процессе производства;

d) накопление и обслуживание картотеки данных по контролю качества по мере их отношения к требованиям потребителей;

e) сбор данных и обеспечение функционирования оборудования и станков, а также накопление и обслуживание картотеки их жизненного цикла, необходимой для их планово-предупредительного обслуживания;

f) сбор и сохранение данных об использовании людских ресурсов для передачи таких данных персоналу и ведения отчетности;

g) установление базового графика производства для завода;

h) корректировку базового заводского графика производства в пользу получаемых заказов, с учетом изменений в доступных ресурсах, наличия доступных энергоресурсов, уровней потребления энергии и потребностей в техническом обслуживании;

i) разработку оптимальных графиков профилактического обслуживания и обновления оборудования в увязке с базовым заводским графиком производства;

j) определение оптимальных уровней запасов сырья, энергоресурсов, запчастей и незавершенного производства в каждом месте хранения. Такие функции включают в себя также планирование потребности в материалах (MRP) и комплектацию запчастей;

k) необходимую корректировку базового заводского графика производства при любых значительных сбоях в производстве;

l) планирование производительности с учетом всех вышеуказанных действий.

6.2.2.3 Уровень 3 — Управление деятельностью

Уровень 3 включает в себя функции, задействованные в управлении рабочими процессами для изготовления конечных продуктов, например, выдачу заказов на изготовление продукции, детальное планирование производства, обеспечение надежности и оптимизацию управления в масштабе производственного объекта.

Действия на уровне 3 включают в себя:

a) предоставление отчетов о ходе производства на участках, в т. ч. о текущих производственных издержках;

b) сбор и хранение данных о ходе производства, имеющемся оборудовании, рабочей силе, сырье, запчастях и энергопотреблении для разных участков;

c) сбор данных и их автономный анализ в соответствии с требованиями инженерных функций. Это может включать в себя статистический анализ качества и соответствующие функции управления;

d) осуществление необходимых функций, относящихся к персоналу, таких как: статистика рабочего времени (например, время, задание), график отпусков, баланс рабочей силы, сводная диаграмма продвижений по службе, а также внутренние инструктажи и повышение квалификации персонала;

e) установление оперативного детального графика производства для отдельно взятых участков, который охватывает техническое обслуживание, транспортировку и другие производственные нужды;

f) оптимизацию издержек на отдельно взятых производственных участках при одновременном соблюдении графика производства, установленного функциями уров-ня 4;

g) корректировку графиков производства для компенсации сбоев заводского производства, которые могут произойти на соответствующих участках ответственности.

6.2.2.4 Уровень 2 — Диспетчерское управление

Уровень 2 включает в себя функции, задействованные в отслеживании и управлении физическим процессом. На заводе обычно имеется некоторое множество производственных участков, например, участок дистилляции, риформинга, смешивания на нефтезаводе или турбинной площадке, и средства подготовки и обогащения угля — на электростанции.

Уровень 2 включает в себя следующие функции:

a) человеко-машинные интерфейсы для операторов;

b) средства аварийно-предупредительной сигнализации для операторов;

c) функции диспетчерского контроля;

d) сбор данных о динамике процесса.

6.2.2.5 Уровень 1 — Локальное или базовое управление

Уровень 1 включает в себя функции, задействованные в контролировании и управлении физическим процессом.

Оборудование мониторинга процессов считывает данные с датчиков, приводит в случае необходимости в исполнение алгоритмы и сохраняет данные о динамике процессов. Примеры систем мониторинга процессов включают в себя системы измерения параметров в резервуаре, системы непрерывного мониторинга выбросов, системы мониторинга вращающегося оборудования и системы индикации температуры. Оборудование управления процессами имеет схожее назначение. Оно считывает

данные с датчиков, приводит в исполнение управляющий алгоритм и подает выходной сигнал на исполнительный элемент (например, контрольные клапаны или приводы задвижек). Контроллеры уровня 1 непосредственно связаны с датчиками и исполнительными механизмами, участвующими в процессе.

Уровень 1 распространяется на непрерывное управление, последовательное управление, периодическое управление и дискретное управление. Многие современные контроллеры представляют собой устройство, которое может реализовывать все типы управления.

Уровень 1 распространяется также на системы безопасности и защиты[1)], которые отслеживают процесс и автоматически возвращают его в безопасное состояние, если он вышел за рамки безопасности. Такая категория включает в себя также системы, которые отслеживают процесс и оповещают оператора об угрозе возникновения небезопасных условий.

Системы безопасности и защиты традиционно реализовывались с использованием физически разделенных контроллеров, но в последнее время стало возможно реализовывать их с помощью так называемого метода логического разделения в пределах общей инфраструктуры. Для данной базовой модели выбрано изображение, ко-

торое подчеркивает необходимость такого разделения (логического или физического) в обеспечении целостности функций безопасности. Оборудование уровня 1 включает в себя, но не ограничивается этим:

a) контроллеры DCS;

b) PLC;

c) RTU.

Системы безопасности и защиты часто налагают дополнительные требования к безопасности, которые могут не согласовываться или не относиться к требованиям кибербезопасности. Такие системы включают в себя системы безопасности, применяемые на химических и нефтехимических заводах, как указано в стандартах серии МЭК 61511, системы безопасности АЭС или системы, связанные с безопасностью АЭС, как указано в стандартах серии МЭК 61513, и защитные функции, как указано в стандартах энергетического сообщества IEEE.

6.2.2.6 Уровень 0 — Процесс

Уровень 0 соответствует фактическому физическому процессу. Такие процессы относятся к разного рода производственному оборудованию во всех секторах, которые включают в себя, но не ограничиваются этим, штучное производство, нефтехимическую промышленность, товародвижение, фармацевтику, целлюлозно-бумажную промышленность и электроэнергетику.

Уровень 0 распространяется на датчики и исполнительные механизмы, непосредственно относящиеся к процессу и технологическому оборудованию.

6.3 Объектные модели

6.3.1 Общие положения

Современные системы управления — это сложные компьютерные сети со множеством взаимосвязанных компонентов, которые выполняют разнообразные функции, обеспечивая безопасное и эффективное функционирование химических заводов, заводов по изготовлению автомобильных деталей, трубопроводов, средств выработки электроэнергии, сетей передачи и распределения и многих других промышленных объектов, систем транспортировки и инженерных коммуникаций.

Одно время такие системы были изолированы от других компьютеров предприятия и в них использовалось проприетарное аппаратное и программное обеспечение и

сетевые протоколы. Сейчас дело обстоит иначе, поскольку разработчики систем управления приняли на вооружение коммерчески доступную информационную технику из-за ее ценовых преимуществ, а бизнес-потребности послужили стимулом к объединению систем управления с коммерческими информационными системами.

С точки зрения безопасности следует уделять особое внимание самому управляющему оборудованию, пользователям этого оборудования, соединениям между компонентами системы управления и ее взаимосвязям с бизнес-системами и другими сетями.

[1)] Такие системы упоминаются как автоматизированные системы безопасности в таких стандартах как стандарты серии МЭК 61511.

Настоящий стандарт применим к широкому спектру систем промышленной автоматики и контроля, которые используются в ряде отраслей промышленности. Таким образом, объектная модель должна по возможности стартовать на верхнем уровне, а также быть достаточно универсальна и применима ко всем ситуациям, в которых применяются системы управления. См. рисунок 14.

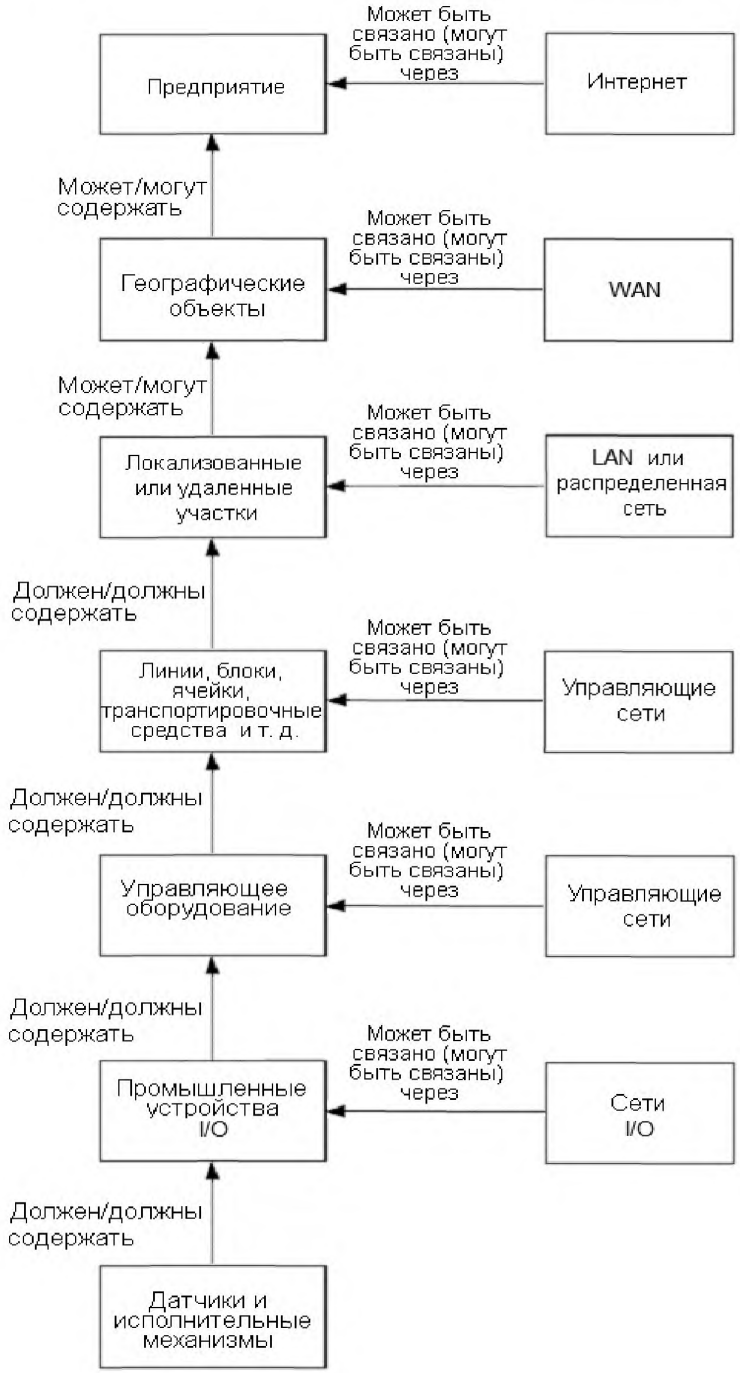

Рисунок 14 — Пример модели объектов непрерывного производства

Поскольку сети играют в безопасности важную роль, объектная модель включает в себя в явной форме сетевые элементы, которые обычно присутствуют на каждом уровне иерархии. На каждом уровне оборудование (или помещения) связано между собой сетью соответствующего типа. Несмотря на то, что сами сети могут быть связаны между собой, данная модель не иллюстрирует этой связи.

Как и в случае с базовой моделью, прикладным системам SCADA соответствует несколько иное изображение. Типичная объектная модель SCADA показана на рисунке 15.

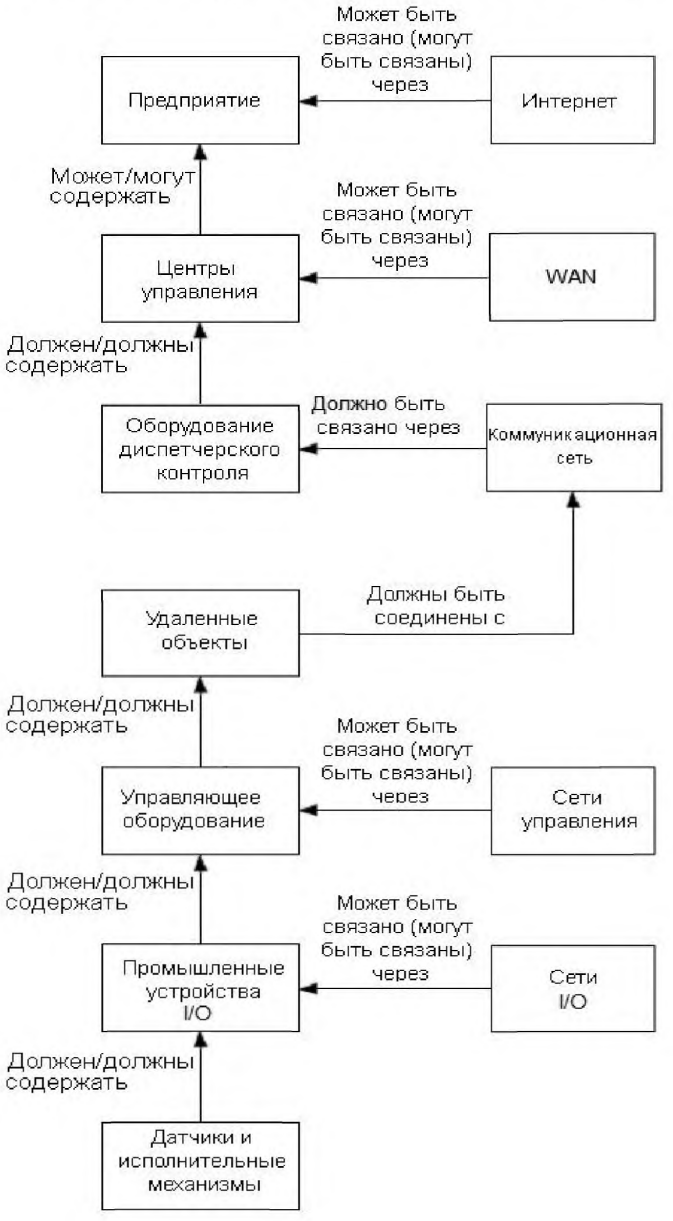

Рисунок 15 — Пример модели объектов системы SCADA

Данная объектная модель отражает вспомогательные информационные системы, которые могут присутствовать на различных уровнях иерархии. Такие системы не управляют процессом напрямую, но взаимодействуют с управляющим оборудованием, получая от него данные и направляя ему команды и технологические инструкции. Информационные системы линий, участков и объектов служат

также хранилищами производственной информации, которая предоставляется пользователям в пределах всего предприятия, и могут взаимодействовать с приложениями для планирования ресурсов предприятия, действующими в корпоративном дата-центре.

При необходимости модель может быть сжата или расширена для отражения рассматриваемого субъекта, при условии, что она согласуется с другими моделями и изображениями. Например, применительно к заводу, имеющему только один участок, можно обойтись без классификации таких участков, при условии, что базовая архитектура и полученная в итоге зона отражают сжатую объектную модель.

6.3.2 Предприятие

Предприятие — это субъект хозяйствования, который производит и транспортирует продукцию или эксплуатирует и обслуживает инфраструктурные сервисы. Предприятия часто бывают соединены с Интернетом для обмена данными с другими предприятиями или предоставления информации и сервисов (таких как электронная почта) наемным сотрудникам. Предприятия обычно используют один или более дата-центров для обработки информации в соответствии с требованиями предприятия. Безопасность бизнес-процессов, поддерживаемых такими IT-объектами, выходит за рамки настоящего стандарта.

6.3.3 Географические объекты

6.3.3.1 Общие положения

Объект — это подмножество физической, географической или логической группы имущественных объектов предприятия. Объект может содержать участки, производственные линии, технологические ячейки и установки, центры управления и транспортировочные средства. Объекты могут быть связаны с другими объектами посредством WAN. Объект может содержать информационные системы, такие как система управления производством, которая координирует производственные процессы на объекте.

6.3.3.2 Центр управления

Центр управления — это особый тип объекта. На предприятиях промышленной инфраструктуры обычно используются один или более центров управления для контроля или координации процессов, происходящих на предприятии. Если центров управления на предприятии несколько (например, имеется резервный центр на отдельной территории объекта), то они, как правило, связаны между собой посредством WAN. Центр управления содержит хост-компьютеры SCADA и соответствующие устройства отображения информации для операторов, а также вспомогательные информационные системы, такие как сервер архивных данных.

6.3.3.3 Удаленный объект

Удаленные объекты содержат оборудование в форме PLC, RTU или интеллектуальных электронных устройств (IED), которые отвечают за отслеживание и управление процессами, происходящими внутри или снаружи объекта. Удаленные объекты соединены с центром управления через коммуникационную сеть (иногда называемую также телеметрической сетью). Удаленные объекты могут быть соединены и между собой (например, для упрощения таких функций как релейная защита между подстанциями в сети электропередач).

6.3.4 Участок

Участок — это подмножество физической, географической или логической группы имущественных объектов, расположенных на территории производственного объекта. Участок может содержать производственные линии, технологические ячейки и единицы оборудования. Участки могут быть связаны между собой через LAN объекта и содержать информационные системы, которые соответствуют операциям, осуществляемым на участках.

6.3.5 Линии, блоки, ячейки, транспортировочные средства

Участки образованы низкоуровневыми элементами, осуществляющими функции изготовления, управления инфраструктурными объектами или транспортировки. Субъекты на этом уровне могут быть связаны между собой зональной сетью управления и содержать информационные системы, которые соответствуют операциям, осуществляемым в субъектах.

6.3.6 Оборудование диспетчерского контроля

Оборудование диспетчерского контроля включает в себя компьютерные серверы, человеко-машинные интерфейсы, LAN и коммуникационные устройства, позволяющие операторам дистанционно контролировать работу и управлять техническими средствами, которые рассредоточены на большой географической области.

6.3.7 Управляющее оборудование

Управляющее оборудование включает в себя DMS, PLC, контроллеры движения, интеллектуальные накопители и соответствующие пульты операторов, используемые для управления и контроля процесса. Термин распространяется также на промышленные сети, где логика и алгоритмы управления реализованы на интеллектуальных периферийных устройствах, координирующих процессы в таких сетях.

6.3.8 Промышленная сеть ввода/вывода

Промышленная сеть ввода/вывода представляет собой соединительное звено (проводное или беспроводное), которое связывает эти элементы с управляющим оборудованием

6.3.9 Датчики и исполнительные механизмы

Датчики и исполнительные механизмы представляют собой оконечные элементы, соединенные с технологическим оборудованием.

6.3.10 Управляемое оборудование

Ниже уровня объектов системы управления стоят объекты, которые составляют управляемое оборудование. Этот уровень соотносят также с физическим или эксплуатационным процессом.

6.4 Базовая архитектура

Базовая архитектура составляется из субъектов, определенных в объектной модели. Базовая архитектура индивидуальна для каждой рассматриваемой ситуации и будет индивидуальна для каждой модели. Каждая организация создает одну или более базовых архитектур в зависимости от выполняемых бизнес-функций, а также рассматриваемых функций. Как правило, организация имеет единую базовую архитектуру для корпорации, которая сведена к общим законам и охватывает все эксплуатационные средства. Каждый технический объект или тип объектов может также иметь более детальную схему базовой сетевой архитектуры, дополняющую корпоративную модель. Рисунок 16 иллюстрирует пример упрощенной базовой архитектуры для производственного процесса.

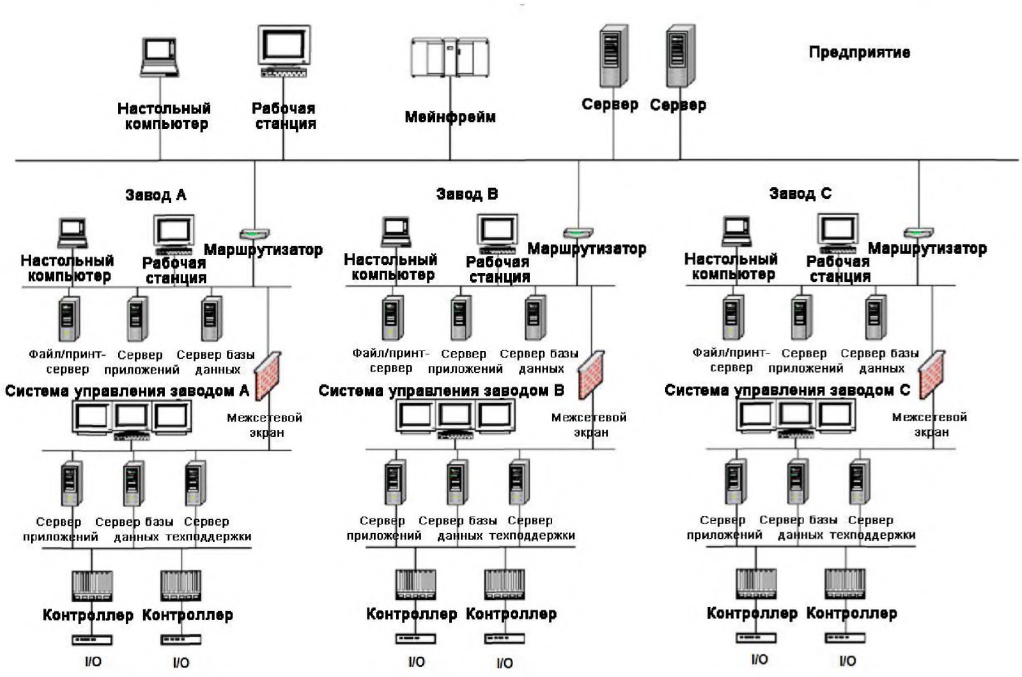

Рисунок 16 — Пример базовой архитектуры

6.5 Зональная и трактовая модель

6.5.1 Общие положения

Зональная и трактовая модель разрабатывается на основе базовой архитектуры. Такая модель служит для описания логических групп объектов в пределах предприятия или его подпространства. Объекты группируются в субъекты (например, относящиеся к бизнесу, техническим средствам, производственным объектам или IACS), которые затем могут быть проанализированы на предмет соответствия политике безопасности, а следовательно и ее требованиям. Модель позволяет оценивать общие угрозы, уязвимости и соответствующие контрмеры, необходимые для достижения уровня безопасности (целевого уровня безопасности), достаточного для защиты сгруппированных объектов. Группируя объекты таким образом, можно определить политику безопасности для всех объектов, входящих в состав зоны. Результаты таких исследований могут быть затем использованы для определения защиты, необходимой с учетом процессов, происходящих в зоне.

Примечание — Термин «зона», употребляемый в настоящем стандарте в явной форме, следует всегда относить к зоне безопасности.

6.5.2 Определение зон безопасности

Зоны — один из наиболее важных инструментов, определяющих успех программы безопасности, и правильное определение зон — это наиболее важный аспект процесса построения такой программы. При определении зон организациям следует использовать как базовую архитектуру, так и объектную модель, чтобы получаемые в итоге зоны безопасности и уровни безопасности соответствовали целям безопасности, установленным в политике безопасности систем промышленной автоматики и контроля.

Если в одном и том же устройстве осуществляются процессы разного уровня, то организация может либо увязать физическое устройство с более жесткими требованиями безопасности, либо создать отдельную зону с отдельной политикой безопасности, которая представляет собой смешанную политику для двух зон. Типичный пример относится к серверам-архиваторам. В целях эффективности такой сервер должен иметь доступ к критическим устройствам управления, которые являются источником получаемых данных. Однако по мере производственной необходимости может требоваться представление этих данных диспетчерам и персоналу по оптимизации производственного процесса, поэтому необходим более свободный доступ к устройству по сравнению с доступом, который предусматривают типичные требования к безопасности систем управления.

Если в одном и том же физическом устройстве функционирует несколько прикладных систем, задействующих процессы разного уровня, то может быть создана и граница логической зоны. Доступ к конкретной системе ограничен в пользу лиц, имеющих привилегии для системы этого уровня. Примером является машина, обеспечивающая функционирование как OPC-сервера, так и OPC-инструментов анализа, выполняемого клиентами. Доступ к OPC-серверу ограничен в пользу лиц, имеющих привилегии более высокого уровня, в то время как доступ к динамическим таблицам с использованием клиентского OPC-подключения возможен для всех сотрудников.

6.5.3 Идентификация зон

Зоны могут быть совокупностью независимых имущественных объектов, совокупностью подзон или совокупностью как независимых объектов, так и объектов, сгруппированных в свою очередь в подзоны, содержащиеся в главной зоне. Для зон характерно наследование свойств, т. е. дочерняя зона (или подзона) должна соответствовать всем требованиям, предъявляемым к родительской зоне. На рисунке 17 показана упрощенная зональная модель для нескольких заводов. В данном случае корпоративная зона — это родительская зона, а каждый завод представляет собой дочернюю зону или подзону, которая вмещает собственную подзону управления.

Примечание — Можно достичь значительного преимущества, если совместить зоны безопасности с физическими участками или зонами на производственном объекте, например, совместить центр управления с зоной управления безопасностью.

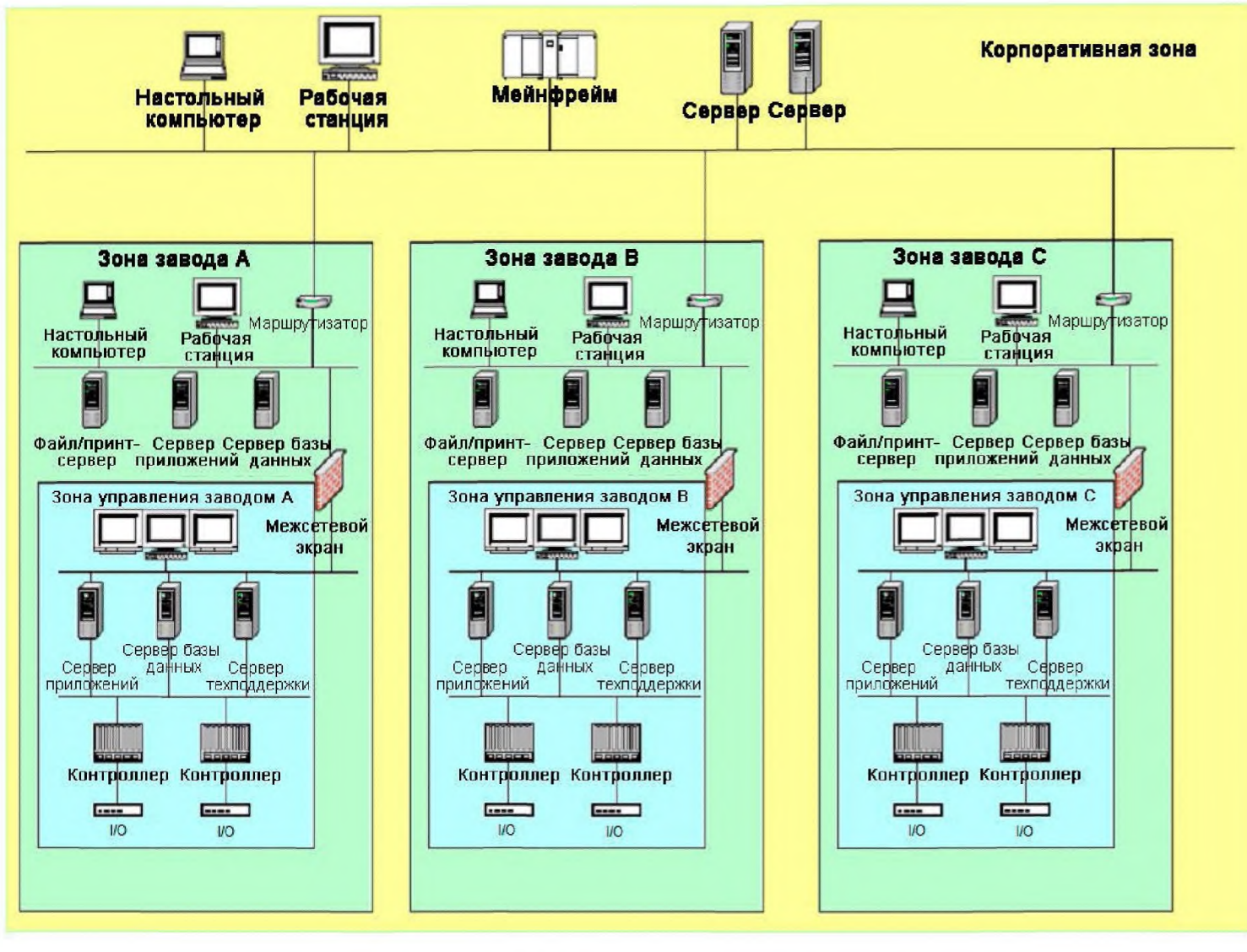

Рисунок 17 — Пример мультизаводских зон

Единая архитектура предприятия может быть подразделена на отдельные зоны, как показано на рисунке 18. В такой модели политика зон будет независимой и каждой зоне может соответствовать совершенно разная политика безопасности.

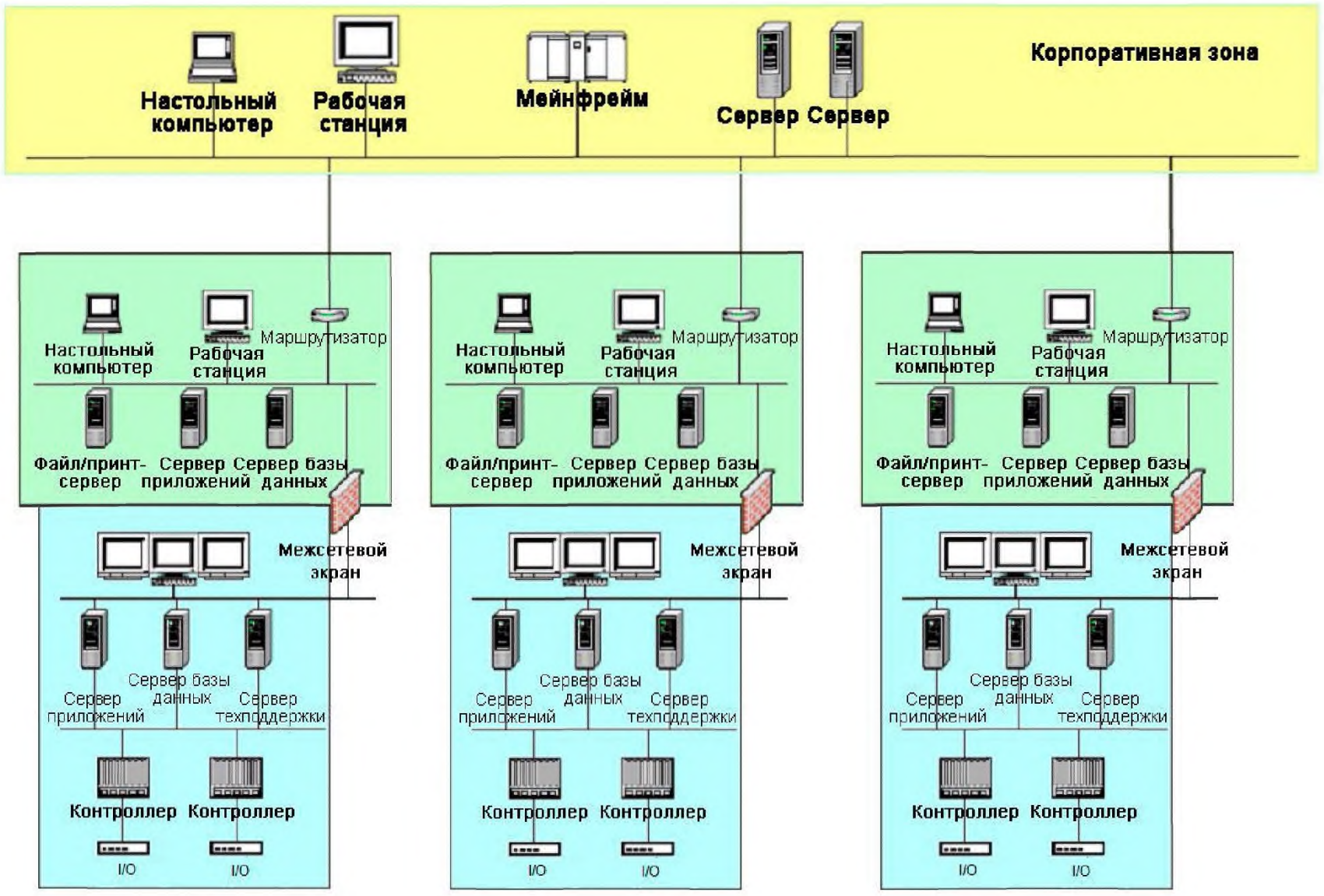

Рисунок 18 — Пример отдельных зон

Аналогичные модели могут быть построены для приложений SCADA, как показано на рисунках 19 и 20.

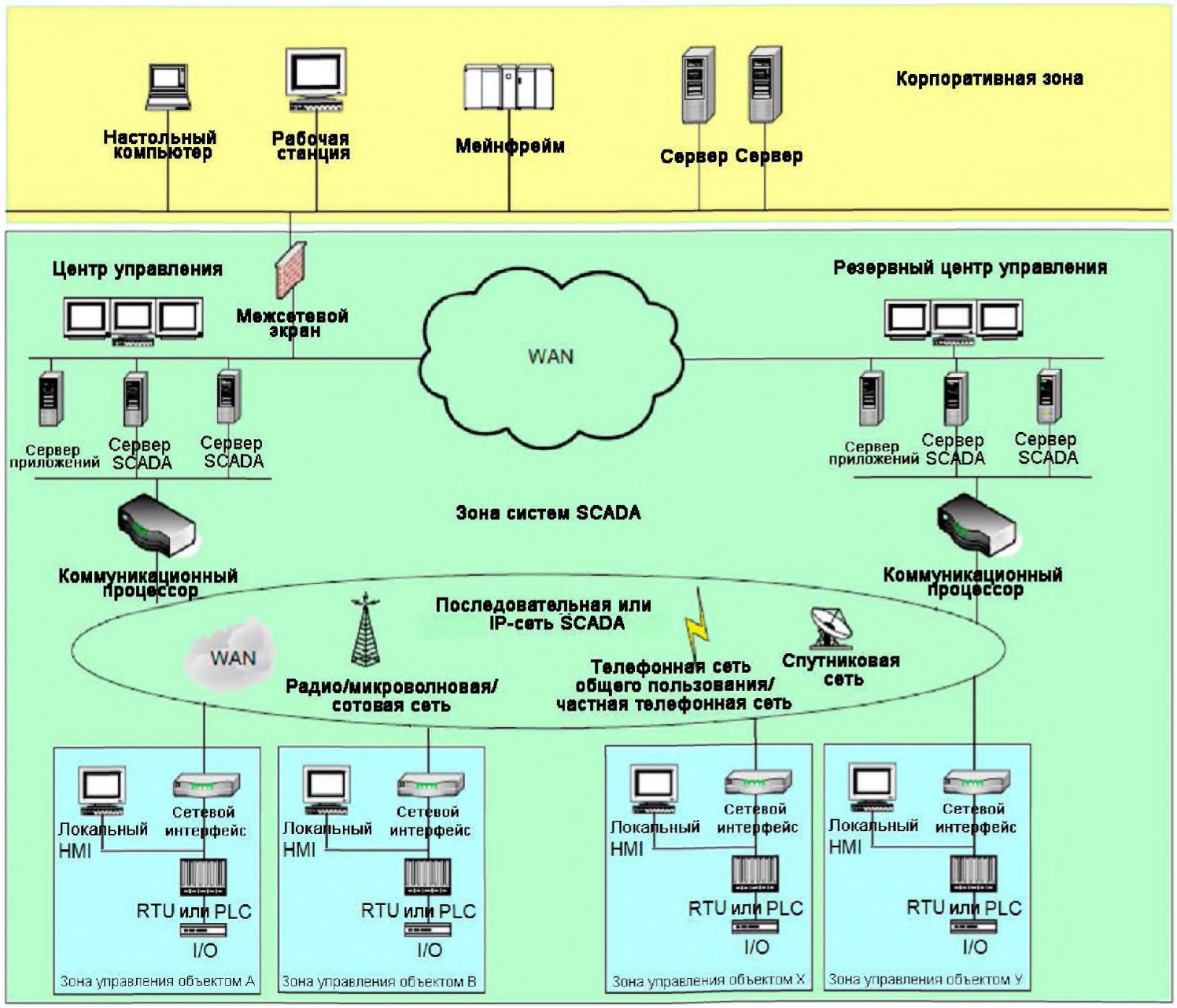

Рисунок 19 — Пример зоны SCADA

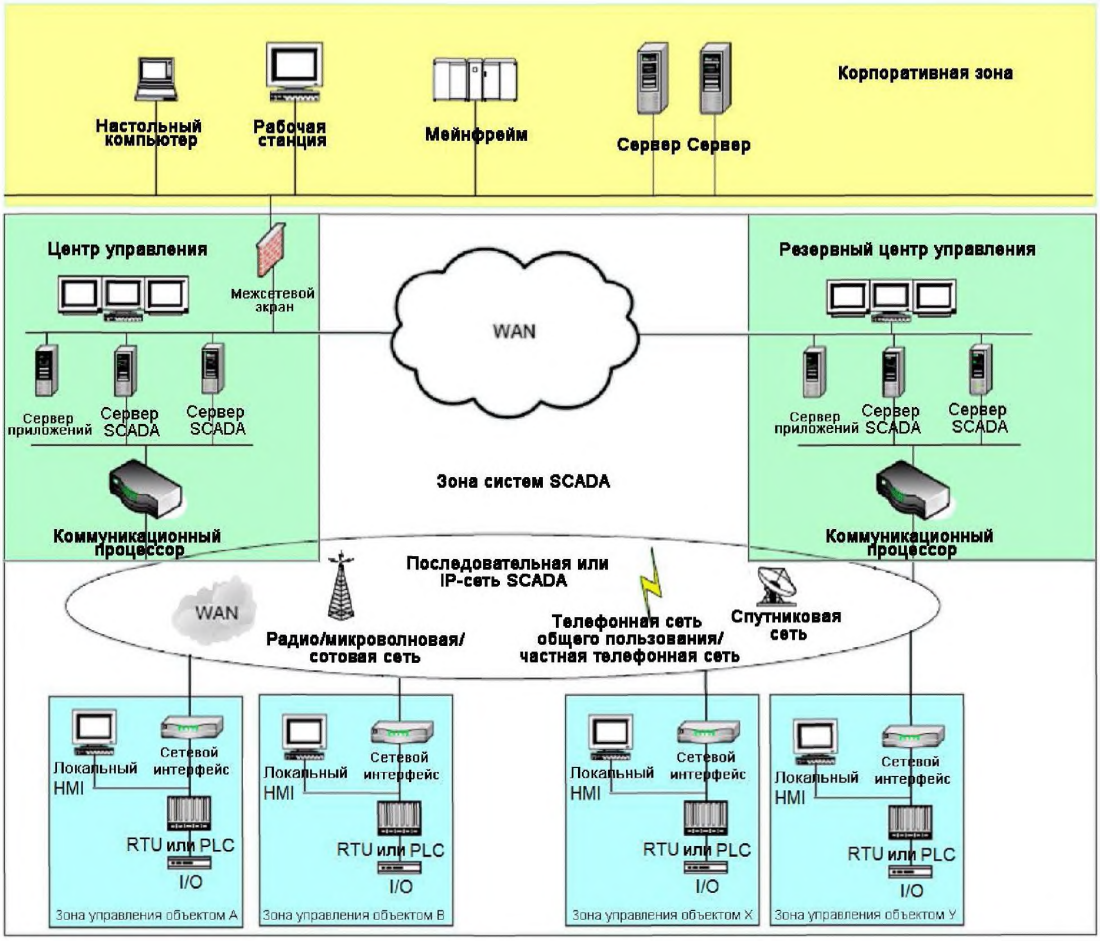

Рисунок 20 — Пример независимых зон SCADA

6.5.4 Характеристики зон

6.5.4.1 Общие положения

Каждой зоне соответствует некий набор характеристик и требований безопасности, которые являются ее атрибутами:

a) политика безопасности;

b) перечень имущественных объектов;

c) требования к доступу и меры управления доступом;

d) угрозы и уязвимости;

e) последствия нарушения безопасности;

f) авторизованная технология;

g) порядок управления изменениями.

Указанные атрибуты описаны подробнее в 6.5.4.2–6.5.4.7.

6.5.4.2 Политика безопасности

К каждой зоне прикреплен контрольный документ, в котором описаны общие цели безопасности и способ обеспечения целевого уровня безопасности. Контрольный документ включает в себя:

a) границы зоны;

b) уровень безопасности зоны;

c) организационную структуру и обязанности по обеспечению выполнения политики безопасности;

d) риски, относящиеся к зоне;

e) стратегию безопасности, направленную на достижение необходимых целей;

f) меры безопасности, подлежащие исполнению;

g) виды деятельности, разрешенной в пределах зоны;

h) виды доступа к зоне, получаемого посредством коммуникации;

i) документацию, раскрывающую атрибуты зоны.

Перечисленная выше информация документируется и объединяется в политику безопасности зоны, используемую в качестве руководства и критериев оценки для конструирования и обслуживания объектов, которые содержатся в зоне.

6.5.4.3 Перечень имущественных объектов

Для поддержания безопасности в пределах зоны организация должна вести список всех ее имущественных объектов (физических и логических). Такой список служит для оценки риска и уязвимостей, а также определения и контроля соблюдения соответствующих мер безопасности, необходимых для достижения целей политики безопасности. Точность инвентарной ведомости — это ключевой фактор в достижении целей безопасности, обозначенных в политике безопасности. Список следует дорабатывать при изменениях имущественных объектов внутри зоны или изменениях электронных связей между ними, а также в случае включения в состав зоны новых объектов, чтобы достигались цели безопасности.

Физические объекты и компоненты — это физические устройства, находящиеся внутри зоны. Некоторые примеры таких устройств приведены ниже:

a) компьютерное аппаратное обеспечение (например, рабочие станции, серверы, инструменты, элементы управления, источники электропитания, дисковые накопители или резервные архиваторы на магнитной ленте);

b) сетевое оборудование (например, маршрутизаторы, коммутаторы, концентраторы, межсетевые экраны или механические кабели);

c) коммуникационные звенья (например, шины, линии, модемы и другие сетевые интерфейсы, антенны);

d) оборудование для аутентификации и авторизации доступа (например, контроллеры доменов, RADIUS-серверы, считыватели и сканеры);

e) аппаратное обеспечение опытных систем;

f) аппаратное обеспечение моделирующих и обучающих систем;

g) аппаратное обеспечение внешних систем;

h) запасы запчастей;

i) устройства контроля и управления (например, датчики, переключатели и контроллеры);

j) справочная информация и руководства.

Логические объекты включают в себя любое программное обеспечение и данные, используемые в зоне. Вот некоторые примеры:

k) программное обеспечение компьютерных систем (например, программные приложения, операционные системы, коммуникационные интерфейсы, таблицы конфигураций, инструменты для разработки и анализа, и утилиты);

l) патчи и обновления для операционных систем и прикладных инструментариев;

m) базы данных;

n) архивы данных;

o) файлы конфигураций оборудования;

p) копии программного обеспечения и данных, предназначенные для целей резервирования и восстановления;

q) документация по обоснованию проекта (например, функциональные требования к информации, объектам и др., классификация безопасности и уровни защиты, физический и программный проект, оценка уязвимостей, периметр безопасности, документацию по оценочным испытаниям, сборке и монтажу);

r) дополнительно поставляемые ресурсы (например, обновления продуктов, патчи, пакеты обновления, утилиты и результаты проверочных испытаний).

6.5.4.4 Требования к доступу и меры управления доступом

Понятие зоны по сути подразумевает, что доступ к ней ограничен в пользу незначительной совокупности всех возможных субъектов, которые наделены правом доступа. Политика безопасности зоны должна прописывать условия доступа к зоне, чтобы выполнялись ее бизнес-цели и способ регулирования этого доступа.

6.5.4.5 Оценка угроз и уязвимостей

В пределах заданной зоны существуют угрозы и соответствующие им уязвимости. Организации должны выявлять и оценивать эти угрозы и уязвимости, чтобы определять вероятность провоцирования ими ситуации, в которой объекты внутри зоны больше не служат своим бизнес-целям. Процесс документирования угроз и уязвимостей выполняется в ходе оценки угроз и уязвимостей, которая является частью политики безопасности зоны.

Существует множество возможных контрмер для уменьшения риска того, что определенная угроза воспользуется конкретной уязвимостью внутри зоны. Политика безопасности должна по возможности прописывать, какие виды контрмер применимы для достижения целевого уровня безопасности зоны в рамках оптимального соотношения издержек и риска.

6.5.4.6 Авторизованная технология

Системы промышленной автоматики и контроля эволюционируют в соответствии с меняющимися бизнес-требованиями, поэтому необходимо контролировать технологию реализации изменений системы. Любая технология, используемая в таких системах, влечет за собой серию уязвимостей и соответствующие им риски. В целях минимизации рисков для конкретной зоны политика безопасности этой зоны должна предусматривать действующий список технологий, приемлемых в зоне, а также неприемлемых в ней.

6.5.4.7 Порядок управления изменениями

Необходима формализованная и четкая методика, которая обеспечивает точность инвентарной ведомости отдельно взятой зоны и порядок внесения изменений в политику безопасности зоны. Формализованная методика гарантирует, что изменения и дополнения зоны не отразятся отрицательно на целях безопасности. Кроме того, необходима методика приспособления к меняющимся угрозам и целям безопасности. Угрозы и уязвимости, а также связанные с ними риски, со временем меняются.

6.5.5 Определение трактов

Тракты — это зоны безопасности, которые привязаны к конкретным коммуникационным процессам. Как и зоны безопасности, тракты представляют собой логическое объединение имущественных объектов (в данном случае — коммуникационных объектов). Тракт безопасности обеспечивает безопасность каналов, которые он содержит, точно так же, как физический тракт защищает кабели от механического повреждения. Тракты можно представить как трубы, соединяющие между собой зоны или используемые для коммуникации в пределах одной зоны. Внутренние (в пределах зоны) и внешние (за пределами зоны) тракты вмещают в себя или защищают коммуникационные каналы (по сути кабели), которые обеспечивают связи между объектами. Чаще всего, в контексте IACS, тракт — это то же самое, что сеть, т. е. тракт представляет собой проводку, маршрутизаторы, коммутаторы и устройства управления сетью, которые образуют рассматриваемые коммуникационные линии. Тракты могут представлять собой объединения разнотипных сетевых технологий, а также разнотипных коммуникационных каналов, которые могут присутствовать в одном компьютере. Тракты используются для анализа угроз коммуникации и ее уязвимостей, которые могут присутствовать в коммуникационных линиях внутри зон и между ними.

Тракты можно рассматривать как трубы, которые содержат данные и/или обеспечивают физические соединения, необходимые для коммуникации между зонами. Тракт может содержать подтракты, которые обеспечивают коммуникацию между зонами по типу «один-к-одному» или «один-ко-многим». Надежность коммуникации для тракта может достигаться за счет соблюдения политики безопасности соответствующих зон.

6.5.6 Характеристики трактов

6.5.6.1 Общие положения

В физическом смысле тракт может являться кабелем, который соединяет между собой зоны, обеспечивая коммуникацию между ними.

Тракт — это разновидность зоны, которая не может иметь подзон, т. е. тракт не образован подтрактами. Тракты определяются совокупностью всех зон, которые совместно используют конкретные коммуникационные каналы. Оконечные точки тракта образованы как физическими устройствами, так и приложениями, которые используют каналы, содержащиеся в тракте. На рисунке 21 показан тракт масштаба предприятия.

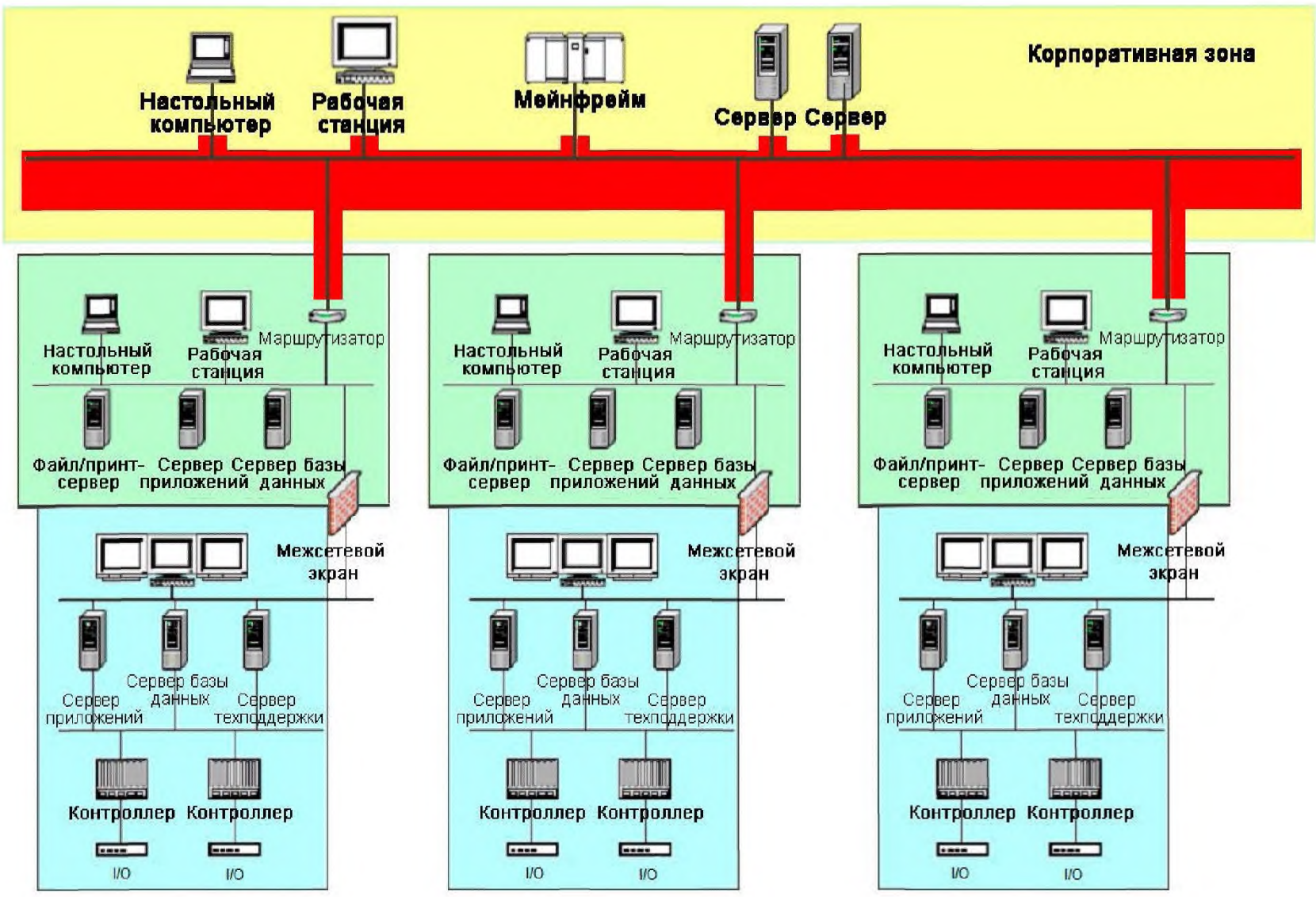

Рисунок 21 — Корпоративный тракт

Как и в случае с зонами, аналогичное изображение может быть построено и применительно к прикладным системам SCADA. Пример проиллюстрирован на рисунке 22.

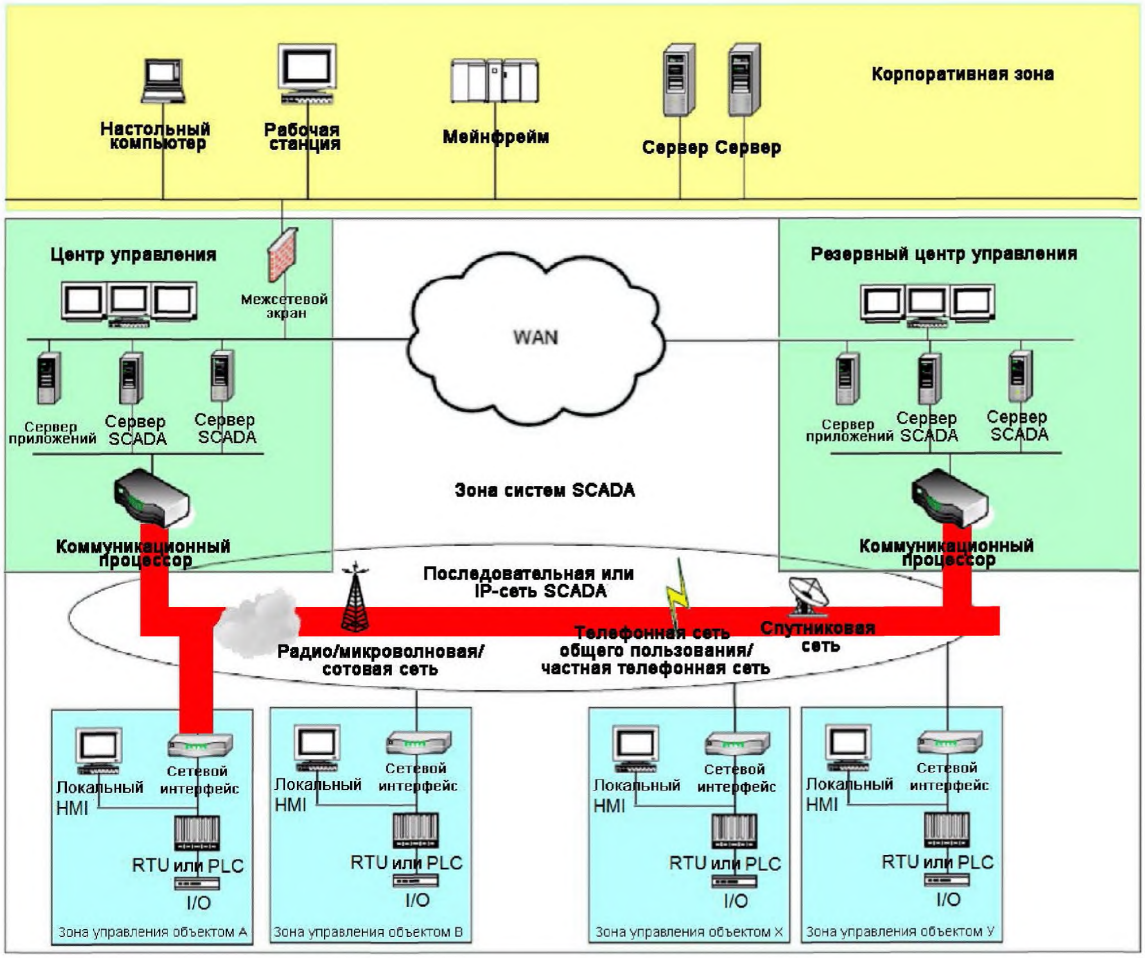

Рисунок 22 — Пример тракта SCADA

Как и в случае с зоной, любому тракту соответствует набор характеристик и требований безопасности, которые являются его атрибутами:

a) политика безопасности;

b) перечень объектов;

c) требования к доступу и меры управления доступом;

d) угрозы и уязвимости;

e) последствия нарушения безопасности

f) авторизованные технологии;

g) порядок управления изменениями;

h) зоны, связываемые между собой трактом.

6.5.6.2 Политика безопасности

За каждым трактом закреплен контрольный документ, в котором описаны общие цели безопасности и способ обеспечения целевого уровня безопасности. Контрольный документ содержит следующую информацию:

a) границы тракта;

b) уровень безопасности тракта;

c) организационную структуру и обязанности по соблюдению политики безопасности тракта;

d) риски, относящиеся к тракту;

e) стратегию безопасности, направленную на достижение необходимых целей;

f) меры безопасности, подлежащие соблюдению;

g) типы каналов, разрешенные в пределах тракта;

h) документацию, раскрывающую атрибуты тракта.

Перечисленная выше информация документируется и объединяется в политику безопасности тракта, используемую в качестве руководства и критериев оценки для конструирования и обслуживания объектов, которые содержатся в тракте.

6.5.6.3 Перечень объектов

Как и в случае с зоной, необходим точный список коммуникационных объектов.

6.5.6.4 Требования к доступу и меры управления доступом

Понятие тракта подразумевает, что доступ к нему ограничен в пользу некоторой совокупности всех возможных субъектов, наделенных правом доступа. Политика безопасности тракта должна прописывать условия доступа к тракту, при которых он служит своим бизнес-целям, и способ регулирования этого доступа.

6.5.6.5 Оценка угроз и уязвимостей

Для отдельно взятого тракта существуют угрозы и соответствующие им уязвимости. Организациям следует выявлять и оценивать эти угрозы и уязвимости, чтобы определять вероятность провоцирования ими ситуации, когда объекты внутри тракта больше не служат своим бизнес-целям. Процесс документирования угроз и уязвимостей выполняется в ходе оценки угроз и уязвимостей, которая является частью политики безопасности тракта.

Существует множество возможных контрмер для уменьшения риска того, что определенная угроза воспользуется конкретной уязвимостью внутри тракта. Политика безопасности должна по возможности прописывать, какие виды контрмер применимы в рамках оптимального соотношения затрат и риска.

6.5.6.6 Авторизованная технология

Системы промышленной автоматики и контроля эволюционируют в соответствии с меняющимися бизнес-требованиями, поэтому необходимо контролировать технологию реализации изменений системы. Любая технология, используемая в таких системах, влечет за собой серию уязвимостей и соответствующие им риски. В целях минимизации рисков для отдельно взятого тракта политика безопасности тракта должна предусматривать действующий список технологий, приемлемых в тракте.

6.5.6.7 Порядок управления изменениями

Необходима формализованная и четкая методика, которая обеспечивает точность политики отдельно взятого тракта и порядок внесения изменений в эту политику. Формализованная методика гарантирует, что изменения и дополнения тракта не отразятся отрицательно на целях безопасности. Кроме того, необходима методика приспособления к меняющимся угрозам и целям безопасности. Угрозы и уязвимости, а также связанные с ними риски, со временем меняются.

6.5.6.8 Присоединенные зоны

Тракт может быть описан и относительно зон, с которыми он соединен.

6.6 Взаимосвязи моделей

Модели, описанные на разделе 6, связаны между собой, а также с политиками безопасности, регламентами и директивами, составляющими программу безопасности. Взаимосвязи моделей показаны на рисунке 23.

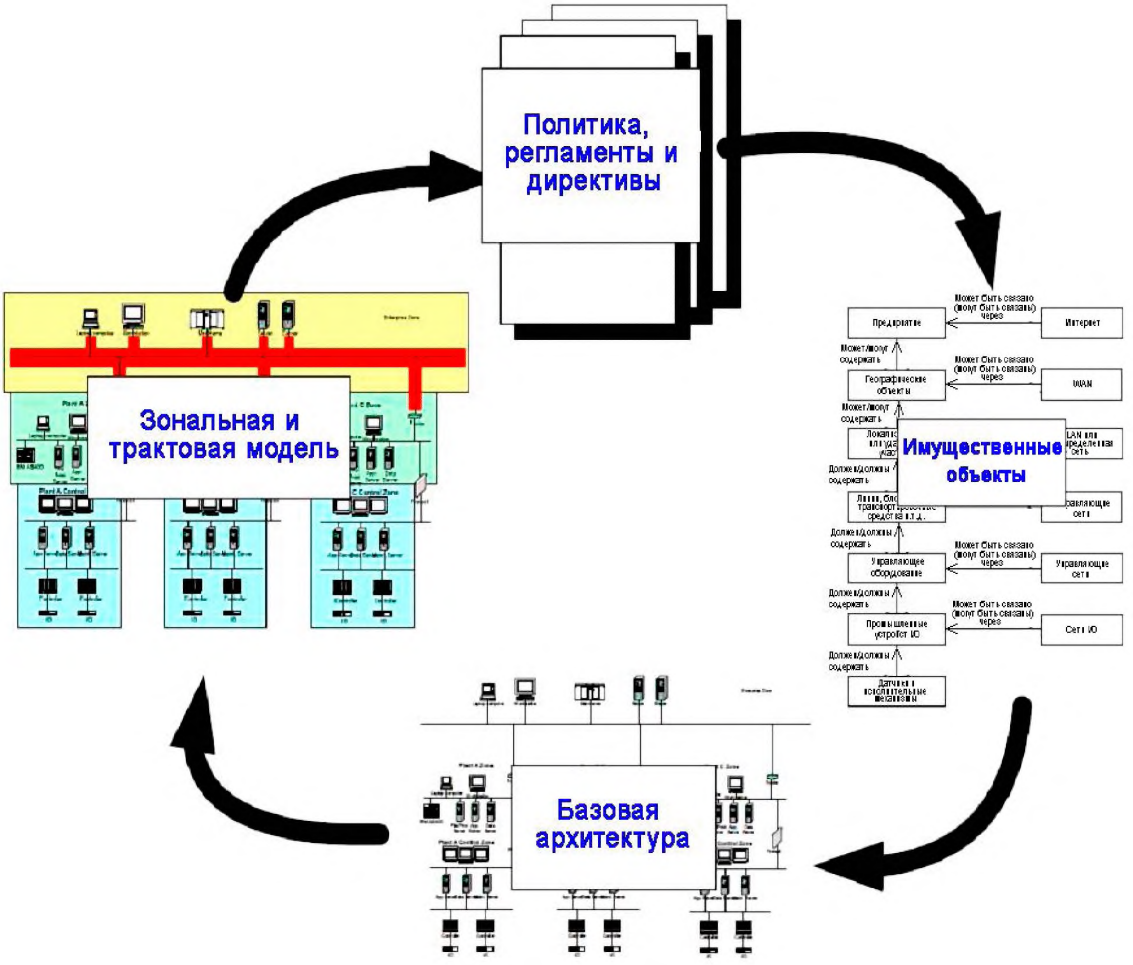

Рисунок 23 — Взаимосвязи моделей

Более подробная информация, касающаяся порядка разработки такой программы, приведена в МЭК 62443-2-1.

Приложение ДА
(справочное)

Алфавитный указатель терминов

Автоматизированная система безопасности (safety-instrumented system)	3.2.95
Автоматизированный подвижный объект (automated vehicle)	3.2.15
Авторизация (санкционирование, санкция, наделение правами, авторизационные данные) (authorization)	3.2.14
Анализ трафика (traffic analysis)	3.2.128
Архитектура безопасности (security architecture)	3.2.100
Ассоциация (association)	3.2.7
Атака (attack)	3.2.9
Аудит (audit)	3.2.11
Аудит безопасности (security audit)	3.2.101
Аутентификация (authentication)	3.2.13
Аутсайдер (outsider)	3.2.74
Базовая модель (reference model)	3.2.81
Безопасность (safety)	3.2.94
Безопасность коммуникации (communication security)	3.2.24
Ботнет (botnet)	3.2.18
Вариант использования (use case)	3.2.132
Взлом системы безопасности (security intrusion)	3.2.107
Вирус (virus)	3.2.134
Вредоносный код (malicious code)	3.2.70
Выполнять аутентификацию (authenticate)	3.2.12
Географический объект (geographic site)	3.2.54
Глобальная вычислительная сеть (wide area network)	3.2.136
Граница (border)	3.2.17
Датчики и исполнительные механизмы (sensors and actuators)	3.2.118
Демилитаризованная зона (demilitarized zone)	3.2.41
Детектирование несанкционированных проникновений (intrusion detection)	3.2.64
Домен (domain)	3.2.45
Доступ (access)	3.2.1
Доступность (работоспособность) (availability)	3.2.16
Защита (security)	3.2.99
Защита от непризнания участия (гарантия сохранения авторства) (nonrepudiation)	3.2.72
Зона (zone)	3.2.139
Зона безопасности (security zone)	3.2.117
Издержки (cost)	3.2.32
Имущественный объект (объект) (asset)	3.2.6
Инсайдер (insider)	3.2.59
Интерфейс (interface)	3.2.62
Инцидент безопасности (security incident)	3.2.106
ИСО (ISO)	3.2.66
Исходный риск (initial risk):	3.2.58
Канал (channel):	3.2.20
Кибербезопасность (киберзащита) (cybersecurity)	3.2.36
Клиент (client)	3.2.22
Коммуникационная система (communication system)	3.2.25

Коммуникационный путь (communication path)	3.2.23
Компоненты безопасности (security components)	3.2.102
Контрмера (countermeasure)	3.2.33
Конфиденциальность (confidentiality)	3.2.28
Конфиденциальность данных (data confidentiality)	3.2.37
Криптограмма, (за)шифрованный текст (ciphertext)	3.2.21
Криптографический алгоритм (cryptographic algorithm)	3.2.34
Криптографический ключ (cryptographic key)	3.2.35
Линии, блоки, ячейки (lines, units, cells)	3.2.68
Локальная вычислительная сеть (local area network):	3.2.69
Маршрутизатор (router)	3.2.93
Межсетевой экран (firewall)	3.2.52
Меры смягчения риска (risk mitigation controls)	3.2.90
Надежный канал (trusted channel)	3.2.130
Нарушение безопасности (security violation)	3.2.116
Ненадежный канал (untrusted channel)	3.2.131
Непризнание участия (repudiation)	3.2.85
Несанкционированное извлечение информации (eavesdropping)	3.2.46
Несанкционированное проникновение (intrusion)	3.2.63
Несанкционированный анализ трафика (сниффинг) (sniffing)	3.2.120
Ограничение доступа (boundary):	3.2.19
OPC (OPC)	3.2.73
Остаточный риск (residual risk)	3.2.86
Отказ в обслуживании (denial of service)	3.2.42
Открытый текст (plaintext)	3.2.77
Отслеживаемость (accountability)	3.2.3
Оценка риска (risk assessment)	3.2.88
Перехват (interception)	3.2.61
Перехват информации (wiretapping)	3.2.137
Периметр безопасности (security perimeter)	3.2.110
Политика безопасности (security policy)	3.2.112
Пользователь (user)	3.2.133
Привилегия (privilege)	3.2.78
Приложение (application)	3.2.4
Предприятие (enterprise)	3.2.48
Преодоление защиты (penetration)	3.2.75
Программа безопасности (security program)	3.2.114
Производственные операции (manufacturing operations)	3.2.7
Промышленная сеть ввода/вывода (field I/O network)	3.2.51
Протокол (protocol)	3.2.80
Процедуры безопасности (security procedures)	3.2.113
Процесс (process)	3.2.79
Распределенная система управления (distributed control system)	3.2.44
Расшифровка (decryption)	3.2.39
Риск (risk)	3.2.87
Ролевая модель управления доступом (role-based access control)	3.2.92
Секретность (secret)	3.2.98
Сервер (server)	3.2.119
Сервисы безопасности (security services)	3.2.115
Сеть безопасности (safety network)	3.2.97
Система (system)	3.2.123

Система диспетчерского контроля и сбора данных (supervisory control and data acquisition system), система SCADA (SCADA system)	3.2.122
Система масштаба предприятия (enterprise system)	3.2.49
Системное программное обеспечение (system software)	3.2.124
Системы промышленной автоматики и контроля (industrial automation and control systems), IACS	3.2.57
Событие безопасности (security event)	3.2.104
Страж (guard)	3.2.55
Схема атаки (attack tree)	3.2.10
Тракт (conduit)	3.2.27
Троянский конь (Trojan horse)	3.2.129
Уверенность (assurance)	3.2.8
Угрожающее действие (threat action)	3.2.126
Угроза (threat)	3.2.125
Удаленный доступ (remote access)	3.2.83
Удаленный клиент (remote client)	3.2.84
Уровень безопасности (security level)	3.2.108
Уровень допустимости риска (risk tolerance level)	3.2.91
Управление безопасностью (security control)	3.2.103
Управление доступом (access control)	3.2.2
Управление ключами (key management)	3.2.67
Управление риском (risk management)	3.2.89
Управляемое оборудование (equipment under control)	3.2.50
Управляющая сеть (control network)	3.2.31
Управляющее оборудование (control equipment)	3.2.30
Уровень целостности безопасности (safety integrity level)	3.2.96
Утечка информации (compromise)	3.2.26
Участок (area)	3.2.5
Уязвимость (vulnerability)	3.2.135
Фактор угрозы (threat agent)	3.2.127
Фиктивная авторизация (spoof)	3.2.121
Фишинг (phishing)	3.2.76
Функциональная надежность (надежность) (reliability)	3.2.82
Функция безопасности (security function)	3.2.105
Хост (host)	3.2.56
Целостность (integrity)	3.2.60
Цель безопасности (security objective)	3.2.109
Целостность данных (data integrity)	3.2.38
Центр управления (control center)	3.2.29
Цифровая подпись (digital signature)	3.2.43
Червь (worm)	3.2.138
Шифрование (encryption)	3.2.47
Шлюз (gateway)	3.2.53
Эффективность безопасности (security performance)	3.2.111
Эшелонированная защита (defence in depth)	3.2.40
IP-адрес (IP address)	3.2.65

Приложение ДБ
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам Российской Федерации

Таблица ДБ.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
МЭК 62264-1	IDT	ГОСТ Р МЭК 62264-1–2010 «Интеграция систем управления предприятием. Часть 1. Модели и терминология»
ИСО/МЭК 15408-1	IDT	ГОСТ Р ИСО/МЭК 15408-1–2012 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель»
Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов: IDT — идентичные стандарты.		

Библиография

[1]	IEC 60050	International Electrotechnical Vocabulary <http://www.electropedia.org>
[2]	IEC 61508-4	Functional safety of electrical/electronic/programmable electronic safetyrelated systems — Part 4: Definitions and abbreviations
[3]	IEC 61511-1	Functional safety — Safety instrumented systems for the process industry sector — Part 1: Framework, definitions, system, hardware and software requirements
[4]	IEC 61511-3	Functional safety — Safety instrumented systems for the process industry sector — Part 3: Guidance for the determination of the required safety integrity levels
[5]	IEC 61512-1	Batch control — Part 1: Models and terminology
[6]	IEC 61513	Nuclear power plants — Instrumentation and control for systems important to safety — General requirements for systems
[7]	IEC 62264-3	Enterprise-control system integration — Part 3: Activity models of manufacturing operations management
[8]	IEC 62443-2-1	Industrial communication networks — Network and system security — Part 2-1: Establishing an industrial automation and control system security program[6]
[9]	IEC Glossary, available at <http://std.iec.ch/glossary>	
[10]	ISO 7498-2	Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture
[11]	RFC 2828, Internet Security Glossary, <http://www.faqs.org/rfcs/rfc2828.html>	
[12]	FIPS PUB 140-2, Security requirements for cryptographic modules, <http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>	
[13]	CNSS Instruction No. 4009, National Information Assurance Glossary (AI), <http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf>	
[14]	NASA/Science Office of Standards and Technology (NOST), ISO Archiving Standards — Fourth US Workshop — Reference Model Definitions, <http://ssdoo.gsfc.nasa.gov/nost/isoas/us04/defn.html>	
[15]	SANS, Glossary of Terms used in Security and Intrusion Detection, <http://www.sans.org/resources/glossary.php>	

УДК 004.056.5

ОКС 25.040.40;
33.040.40;
35.040

Ключевые слова: промышленные коммуникационные сети, сети и системы, защищенность, кибербезопасность, эшелонированная защита, уязвимости, риски, угрозы, контрмеры, программа безопасности, политика безопасности, зоны безопасности, тракты, уровни безопасности, жизненный цикл уровня безопасности, модели

Подписано в печать 02.12.2014. Формат 60x84⅛.
Усл. печ. л. 9,30. Тираж 32 экз. Зак. 5154

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

ФГУП «СТАНДАРТИНФОРМ»,
123995 Москва, Гранатный пер., 4.
www.gostinfo.ru info@gostinfo.ru