ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 71843— 2024 (IEC/TR 63283-3: 2022)

Цифровая промышленность

УМНОЕ ПРОИЗВОДСТВО

Часть 3

Рекомендации по кибербезопасности

(IEC/TR 63283-3:2022, Industrial-process measurement, control and automation — Smart Manufacturing — Part 3: Challenges for cybersecurity, MOD)

Издание официальное

Москва
Российский институт стандартизации
2025

gost.e-ecolog.ru

Предисловие

1 ПОДГОТОВЛЕН Ассоциацией «Цифровые инновации в машиностроении» (АЦИМ) и Федеральным государственным бюджетным учреждением «Российский институт стандартизации» (ФГБУ «Институт стандартизации») на основе собственного перевода на русский язык англоязычной версии документа, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 459 «Информационная поддержка жизненного цикла изделий»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 29 ноября 2024 г. № 1810-ст

4 Настоящий стандарт является модифицированным по отношению к международному документу IEC/TR 63283-3:2022 «Измерение, управление и автоматизация промышленного процесса. Умное производство. Часть 3. Проблемы кибербезопасности» (IEC/TR 63283-3:2022 «Industrial-process measurement, control and automation — Smart Manufacturing — Part 3: Challenges for cybersecurity», MOD) путем изменения отдельных фраз (слов, значений показателей, ссылок), которые выделены в тексте курсивом. Внесение указанных технических отклонений направлено на учет потребностей национальной экономики Российской Федерации.

Наименование настоящего стандарта изменено относительно наименования международного документа для приведения в соответствие с ГОСТ Р 1.5—2012 (пункт 3.5).

Сведения о соответствии ссылочных национальных стандартов международным стандартам, использованным в качестве ссылочных в примененном международном документе, приведены в дополнительном приложении ДА.

Сопоставление структуры настоящего стандарта со структурой примененного в нем международного документа приведено в дополнительном приложении ДБ

5 ВВЕДЕН ВПЕРВЫЕ

*Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». 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 ежемесячного 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.e-ecolog.ru

© Оформление. ФГБУ «Институт стандартизации», 2025

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
2 Нормативные ссылки 1
3 Термины, определения и сокращения 2
3.1 Термины и определения 2
3.2 Сокращения 7
4 Задачи кибербезопасности в цифровом производстве 8
5 Системная инженерия 9
6 Применение серии стандартов МЭК 62443 [6] к цифровому производству 17
6.1 Общие положения 17
6.2 Соответствие *ГОСТ Р ИСО/МЭК 27000* 18
6.3 Эталонная модель 19
6.4 Основополагающие требования 19
6.5 Зоны и трубопроводы в системе систем 19
6.6 Оценка рисков для безопасности и уровни защиты 20
6.7 Жизненный цикл системы безопасности 20
6.8 Аудит и ведение журнала 20
6.9 Заключение 20
7 Угрозы безопасности цифрового производства 21
7.1 Общие положения 21
7.2 Обзор вариантов использования в области кибербезопасности 21
7.3 Взгляд на кибербезопасность в рамках жизненного цикла цифрового производства 36
8 Краткое изложение проблем 37
8.1 Общие положения 37
8.2 Контроль идентификации и аутентификации (AC) 38
8.3 Целостность данных и системы (DI) 40
8.4 Конфиденциальность данных (DC) 41
8.5 Ограниченный поток данных (RDF) 42
8.6 Своевременное реагирование на события (TRE) 43
8.7 Доступность ресурсов (RA) 44
Приложение ДА (информационное) Сведения о соответствии ссылочных национальных стандартов международным стандартам, использованным в качестве ссылочных в примененном международном документе 45
Приложение ДБ (справочное) Сопоставление структуры настоящего стандарта со структурой примененного в нем международного документа 46
Библиография 47

Введение

Умное производство является компонентом цифровой промышленности, обеспечивающим изготовление продукции на основе высокотехнологичных комплексов и автоматизированных систем управления. В условиях распределенного производства и создания сквозных цепочек добавленной стоимости повышается интенсивность информационного обмена между участниками производственного процесса, что обусловливает риски в области кибербезопасности. Новый этап развития умного производства характеризуется высоким уровнем самоорганизации производственных систем, что повышает риски в области кибербезопасности.

Настоящий стандарт устанавливает рекомендации по кибербезопасности для умного производства, учитывающие лучшие международные практики и специфику развития отечественной цифровой промышленности.

Настоящий стандарт входит в систему стандартов цифровой промышленности.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Цифровая промышленность

УМНОЕ ПРОИЗВОДСТВО

Часть 3

Рекомендации по кибербезопасности

Digital industry. Smart Manufacturing. Part 3. Challenges for cybersecurity

Дата введения — 2025—07—01

1 Область применения

Настоящий стандарт устанавливает рекомендации по кибербезопасности для сферы умного производства и цифровой промышленности.

Установленные настоящим стандартом термины рекомендуются для применения во всех видах документации и научно-технической литературы в области цифровой трансформации промышленности и создания умных производств.

Настоящий стандарт должен применяться совместно с другими документами системы стандартов в цифровой промышленности.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

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

ГОСТ Р 70988 Система стандартов в цифровой промышленности. Основные положения. Общие требования к системе

ГОСТ Р 70992 Цифровая промышленность. Интеграция и интероперабельность систем. Термины и определения

ГОСТ Р ИСО/МЭК 27000 Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология

ГОСТ Р ИСО/МЭК 27001 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования

ГОСТ Р ИСО/МЭК 27002 Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности

ГОСТ Р МЭК 62443-2-1 Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 2-1. Составление программы обеспечения защищенности (кибербезопасности) системы управления и промышленной автоматики

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам

Издание официальное

ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3 Термины, определения и сокращения

3.1 Термины и определения

В настоящем стандарте применены термины по [1], а также следующие термины с соответствующими определениями.

3.1.1

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

[ГОСТ Р 56205—2014, пункт 3.2.14]

3.1.2 **администратор** (administrator): Роль пользователя, в обязанности которого входит контроль доступа к системе и внедрение политик безопасности для нее.

3.1.3 **актив** (asset): Объект, принадлежащий организации или находящийся под ее опекой, который имеет либо предполагаемую, либо фактическую ценность для организации.

3.1.4

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.

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.

[ГОСТ Р 56205—2014, пункт 3.2.9]

3.1.5 **атрибут** (attribute): Свойство или характеристика объекта.

3.1.6

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.

[ГОСТ Р 56205—2014, пункт 3.2.13]

3.1.7 **варианты использования** (use case): Спецификация набора действий, выполняемых системой, которые дают наблюдаемый результат, который обычно имеет ценность для одного или нескольких участников или других заинтересованных сторон системы.

3.1.8 **влияние** (impact): Оцененные последствия конкретного события.

Примечание — Воздействие может быть выражено в количестве травм и/или смертельных исходов, масштабах экологического ущерба и/или масштабах потерь, таких как материальный ущерб, ущерб интеллектуальной собственности, производственные потери, потеря доли рынка и затраты на восстановление.

3.1.9

выполнять аутентификацию (authenticate): Проверять идентификационную информацию пользователя, устройства на стороне пользователя или другого субъекта, или целостность данных, сохраняемых, передаваемых или подверженных иным образом риску несанкционированного преобразования в информационной системе, или устанавливать правомерность передачи данных.

[ГОСТ Р 56205—2014, пункт 3.2.12]

3.1.10 **девайс** (device): Независимый физический объект, способный выполнять одну или несколько определенных функций в определенном контексте и ограниченный своими интерфейсами.

3.1.11 **дискретное производство** (discrete manufacturing): Способ производства, при котором продукцию изготавливают непрерывно, например автомобили, бытовую технику, компьютеры.

3.1.12

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).

[ГОСТ Р 56205—2014, пункт 3.2.1]

3.1.13

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.

Примечания

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

2 Необходимые внешние ресурсы, отличные от ресурсов технического обслуживания, не влияют на показатель доступности компонента.

3 Во французском языке используется также термин «disponibilit» в значении «текущая доступность».

[ГОСТ Р 56205—2014, пункт 3.2.16]

3.1.14 **журнал аудита** (audit log): Отслеживаемая запись, требующая более высокого уровня защиты целостности, чем в обычных журналах событий.

Примечание — Журналы аудита используются для защиты от претензий, которые снимают с вас ответственность за какое-либо действие.

3.1.15

защита (security):

a) меры, предпринимаемые для защиты системы;

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

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;

е) 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).

[ГОСТ Р 56205—2014, пункт 3.2.99]

3.1.16

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

[ГОСТ Р 56205—2014, пункт 3.2.72]

3.1.17 **зона** (zone): Группировка логических или физических активов на основе риска или других критериев, таких как критичность активов, эксплуатационная функция, физическое или логическое расположение, требуемый доступ (например, принципы минимальных привилегий) или ответственная организация.

Примечание — Все неквалифицированные использования термина «зона» в этом документе следует считать относящимися к зоне безопасности.

3.1.18 **идентификатор**; ID (identifier): Информация, которая недвусмысленно отличает один объект от других в данном контексте идентификации.

3.1.19 **инцидент** (incident): Событие, не являющееся частью ожидаемой работы системы или сервиса, которое вызывает или может вызвать прерывание или снижение качества сервиса, предоставляемого системой управления.

3.1.20

кибербезопасность (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.

[ГОСТ Р 56205—2014, пункт 3.2.36]

3.1.21

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

[ГОСТ Р 56205—2014, пункт 3.2.28]

3.1.22

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

[ГОСТ Р 56205—2014, пункт 3.2.37]

3.1.23

непрерывное производство (continuous production): Производство, которое функционирует с постоянной интенсивностью.

Примечание — Производство считают непрерывным, если оно функционирует в течение указанного периода с указанной интенсивностью. Непрерывное производство считают фактором стабильности производственного процесса или набора процессов.

[ГОСТ Р ИСО 2859-3—2009, пункт 3.1.1]

3.1.24

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.

[ГОСТ Р 56205—2014, пункт 3.2.42]

3.1.25

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.

Примечания

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

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.

[ГОСТ Р 56205—2014, пункт 3.2.88]

3.1.26

привилегия (privilege): Авторизация или набор авторизации на выполнение определенных функций, особенно в контексте операционной системы компьютера.

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

[ГОСТ Р 56205—2014, пункт 3.2.78]

3.1.27 **продукт** (product): Результат труда, природного или промышленного процесса.

3.1.28 **производство** (manufacturing): Все виды деятельности и процедуры жизненного цикла, связанные с проектированием, производством и поддержкой производственных систем и выпускаемой продукции.

3.1.29

процесс (process): Комплекс работ, выполняемых с использованием набора ресурсов, которые предназначены для реализации поставленной задачи в установленные сроки.

[ГОСТ Р ИСО 22400-1—2016, пункт 2.1.8]

3.1.30 **риск** (risk): Сочетание вероятности причинения вреда и тяжести этого вреда.

3.1.31 **серийное производство** (batch production): Производственный процесс, при котором продукты или компоненты производятся партиями и каждая отдельная партия состоит из нескольких одинаковых продуктов или компонентов.

3.1.32 **сертификат открытого ключа** (public key certificate): Набор данных, который однозначно идентифицирует объект, содержит открытый ключ объекта и имеет цифровую подпись доверенной стороны, тем самым привязывая открытый ключ к объекту.

3.1.33 **система** (system): Совокупность взаимосвязанных элементов, рассматриваемых в определенном контексте как единое целое и отделенных от окружающей среды

Примечания

1 Такими элементами могут быть как материальные объекты и понятия, так и их результаты (например, формы организации, математические методы и языки программирования).

2 Считается, что система отделена от окружающей среды и других внешних систем воображаемой поверхностью, которая может разорвать связи между ними и рассматриваемой системой.

3.1.34 **система систем** (system of systems): Совокупность или расположение систем, возникающее в результате интеграции независимых систем в более крупную систему.

3.1.35

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.

[ГОСТ Р 56205—2014, пункт 3.2.57]

3.1.36 **сущность** (entity): Вещь (физическая или нефизическая), имеющая особое существование.

3.1.37

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

Примечание — Это аналогично тому, как физический кабелепровод защищает кабели от физических повреждений.

[ГОСТ Р 56205—2014, пункт 3.2.27]

3.1.38

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

[ГОСТ Р 56205—2014, пункт 3.2.125]

3.1.39

умное производство: *Взаимодействие между умным предприятием и умной продукцией.*

Примечания

1 В научно-технической литературе и международных стандартах также используется термин «цифровая фабрика», являющийся синонимом «умного предприятия».

2 Термин «умное» в данном контексте может обозначать «интеллектуальное» или «цифровое».

[Адаптировано из ГОСТ Р 70990—2023, статья 21]

3.1.40 **умный** (smart): Способный на некоторые самостоятельные действия.

Примечание — В контексте обеспечения самостоятельных действий может рассматриваться применение технологий искусственного интеллекта, в этом случае термин умный является синонимом термина «интеллектуальный».

3.1.41

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.

[ГОСТ Р 56205—2014, пункт 3.2.2]

3.1.42 **устойчивость** (resilience): Способность организации, технологического подразделения или системы IACS противостоять влиянию сбоев.

3.1.43 **функциональные требования** (functional requirement): Спецификация требований, которые должны обеспечивать выполнение функций или их частей.

3.1.44

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

[ГОСТ Р 56205—2014, пункт 3.2.56]

3.1.45

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.

[ГОСТ Р 56205—2014, пункт 3.2.38]

3.1.46

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.

[ГОСТ Р 56205—2014, пункт 3.2.43]

3.2 Сокращения

В настоящем стандарте использованы следующие сокращения:

AC — контроль идентификации и аутентификации (Identification and Authentication Control);

ACS — система автоматизации и управления (Automation and Control System);

CAD — системы автоматизированного проектирования (Computer Aided Design);

CAPP — компьютерное планирование производства (Computer Aided Production Planning);

DC — конфиденциальность данных (Data Confidentiality);

FMEA — анализ видов и последствий отказов (Failure Mode and Effects Analysis);

FR — основное требование (Foundational Requirement);

IACS — система промышленной автоматизации и управления (Industrial Automation and Control System);

IP — интеллектуальная собственность (Intellectual Property);

ISMS — система менеджмента информационной безопасности (Information Security Management System);

KPI — ключевой показатель (Key Performance Indicator);

RA — доступность ресурсов (Resource Availability);

RDF — ограниченный поток данных (Restricted Data Flow);

SM — умное производство (Smart Manufacturing);

TRE — своевременное реагирование на события (Timely Response to Events);

UC — пользовательский контроль (Use Control).

4 Задачи кибербезопасности в цифровом производстве

Развитие цифровой промышленности и создание цифровых и умных производств согласно *ГОСТ Р 70988, ГОСТ Р 70992, ГОСТ Р 59799,* обусловливают ряд новых проблем, связанных с обеспечением безопасности ACS. По сравнению с классическими производственными системами на кибербезопасность влияют следующие характеристики цифровых производственных систем:

- множество заинтересованных сторон: ACS больше не находится под контролем одной заинтересованной стороны. Вместо этого необходимо взаимодействие нескольких заинтересованных сторон, например владельца продукта, производственного оборудования, производственного процесса, поставщиков услуг по анализу данных. Используемые механизмы безопасности должны быть способны поддерживать заинтересованные стороны, уравновешивать и защищать их различные интересы;

- непрерывные изменения: цифровая производственная система подвержена постоянным изменениям и реконфигурации, например, функциональным усовершенствованиям, замене производственного оборудования, изменению выпускаемого продукта, оптимизации процессов. Границы между различными этапами жизненного цикла становятся размытыми (особенно это касается проектирования продукта, инжиниринга, эксплуатации). Безопасность системы должна соответствовать этим изменениям, в том числе в переходный период, и соответствующим образом корректироваться;

- интенсивное использование цифровых данных (оцифровка): цифровые производственные системы производят и обрабатывают огромное количество управляющих и других цифровых данных. Данные о проектировании изделий и процессов [например, системы автоматизированного проектирования (CAD), системы автоматизированного планирования производства (CAPP)], данные датчиков, инженерные данные, самоописательные данные об оборудовании, данные имитационных моделей, которые ранее хранились в отдельных системах, теперь являются неотъемлемой частью производственной системы. Это увеличивает доступ к данным и делает их более уязвимыми для атак. Потенциальные злоумышленники либо извлекают прямую выгоду из этих данных [например, о продукте или процессе/алгоритмической интеллектуальной собственности (IP)], получают конкурентные преимущества [данные о ключевых показателях эффективности (KPI)], либо используют захваченные данные для разработки более сложных атак (например, работая с имитационными моделями, которые сами должны иметь ограниченный доступ);

- архитектура: классическая пирамида автоматизации распадается и трансформируется в структурированную сеть автоматизации, основанную на сервис-ориентированных парадигмах. Новые архитектурные концепции основаны на *ГОСТ Р 59799, [1]* и *[2]*. Это требует внесения изменений в соответствующую архитектуру безопасности;

- применение новых коммуникационных технологий на производстве: адаптация беспроводных сетей, таких как Wi-Fi и технологии 3GPP (LTE, 5G), для умного производства позволяет повысить гибкость (например, упростить перемещение производственного оборудования). Однако беспроводные

сети должны обеспечивать высокую производительность. Благодаря новым парадигмам коммуникационной инфраструктуры, таким как программно-определяемые сети (SDN) и 5G, обеспечивается простая удаленная связь, а в некоторых случаях и связь на уровнях *ГОСТ Р 59799* в соответствии с *[3]* или *[4]*. Например, датчики полевых устройств (уровень 1) потенциально могут напрямую взаимодействовать с корпоративным/подключенным миром (уровень 4), минуя традиционные уровни пирамиды.

Этот отчет основан на оценке подмножества вариантов использования цифрового производства. Требуется дальнейшая работа, но не ограничивающаяся, например, расширением оценки на более широкий набор вариантов использования. Кроме того, эта работа должна быть согласована с другой работой, проводимой в быстро развивающейся области кибербезопасности цифрового производства.

5 Системная инженерия

Цифровые производственные объекты — это сложные интегрированные системы систем. Они проектируются путем внедрения процессов, видов деятельности и задач, определенных в *[5]*. Некоторые процессы системной инженерии требуют особого рассмотрения с точки зрения кибербезопасности. Это происходит, когда в рамках этих процессов используются входные данные, связанные с кибербезопасностью, или создаются выходные данные, связанные с кибербезопасностью. В таблицах 1 и 2 представлены соответствующие процессы и действия, предлагаются конкретные аспекты, которые необходимо принимать во внимание с точки зрения кибербезопасности.

Таблица 1 — Процессы технического управления в рамках проектирования системы согласно *[5]*

Процессы согласно *[5]*	Цель	Аспекты безопасности результатов проектирования	Мероприятия, связанные с деятельностью по обеспечению безопасности
Процесс планирования проекта	Целью процесса планирования проекта является разработка и координация эффективных и выполнимых планов. Данный процесс определяет масштаб управленческой и технической деятельности по проекту, выходные данные процесса, задачи и конечные результаты, устанавливает графики выполнения задач, включая критерии достижения результатов, и необходимые ресурсы для выполнения задач. Это непрерывный процесс, который продолжается на протяжении всего проекта, с регулярным пересмотром планов	Определены цели и планы обеспечения безопасности; определены роли, обязанности, подотчетность, полномочия по аспектам безопасности; ресурсы и услуги, необходимые для достижения целей безопасности, запрашиваются официально и предоставляются в обязательном порядке	
Процесс оценки и контроля проекта	Процесс оценки и контроля проекта предусматривает мониторинг степени достижения требований и критических характеристик качества и доведение результатов до заинтересованных сторон и руководителей	Доступны показатели эффективности безопасности или результаты оценки; оценивается адекватность ролей, обязанностей, подотчетности и полномочий по аспектам безопасности; оценивается достаточность ресурсов, связанных с обеспечением безопасности; проводятся обзоры технического прогресса, включая достижение целей в области безопасности;	Определение плана обеспечения безопасности для описания стратегии обеспечения безопасности в связи с планом управления системным проектированием

Продолжение таблицы 1

Процессы согласно *[5]*	Цель	Аспекты безопасности результатов проектирования	Мероприятия, связанные с деятельностью по обеспечению безопасности
		исследуются и анализируются отклонения показателей безопасности от запланированных; заинтересованные стороны, затронутые проблемами безопасности, информируются о статусе проекта; корректирующие действия определяются и направляются, когда достижение безопасности не соответствует поставленным целям; цели в области безопасности достигнуты	
Процесс управления решениями	Процесс управления решениями обеспечивает оценку альтернативных требований, характеристик архитектуры и характеристик дизайна по критериям принятия решения, включая критическое качество характеристики. Результаты этих сравнений ранжированы с помощью подходящей модели выбора, а затем используются для принятия решения об оптимальном решении	Решения, требующие альтернативного анализа безопасности; выбор предпочтительной стратегии безопасности	Поиск компромисса между ограничениями и требованиями безопасности на стадии концепции и разработки для оптимизации удовлетворения потребностей заинтересованных сторон
Процесс управления рисками	Процесс управления рисками в целом предусматривает выявление, оценку и управление рисками системы, в том числе связанными с соблюдением критических характеристик качества	Выявление уязвимости в системе безопасности, приводящей к возникновению рисков; для устранения уязвимостей в системе безопасности определяют, приоритизируют и выбирают варианты устранения рисков; соответствующие меры безопасности по мере их принятия	Выявление, оценивание и снижение рисков, связанных с безопасностью, на протяжении всего жизненного цикла системы
Процесс управления конфигурацией	Целью процесса управления конфигурацией является управление элементами системы и конфигурациями на протяжении всего жизненного цикла. Управление конфигурацией также обеспечивает согласованность между продуктом и соответствующим определением конфигурации	Определены элементы, связанные с безопасностью, требующие управления конфигурацией; изменения в элементах, связанных с безопасностью, контролируют в разделе «Управление конфигурацией»	

Окончание таблицы 1

Процессы согласно *[5]*	Цель	Аспекты безопасности результатов проектирования	Мероприятия, связанные с деятельностью по обеспечению безопасности
Управление информацией	Процесс управления информацией в целом предусматривает спецификацию, разработку и сопровождение информационных элементов для документирования и распространения информации о степени достижения результатов. Информационные элементы, используемые для определения критических характеристик качества, носят специализированный характер. Источниками для их описания являются отраслевые ассоциации и др.	Идентифицируют информацию, связанную с безопасностью, которой необходимо управлять; определены представления информации, связанной с безопасностью; информацию, связанную с безопасностью, разрабатывают, преобразуют, хранят, проверяют, представляют и удаляют; информация, связанная с безопасностью, доступна для определенных заинтересованных сторон	Документирование результатов работы системы безопасности на протяжении всего жизненного цикла системы
Процесс измерения	Целью процесса измерения является сбор, анализ и представление объективных данных и информации для поддержки эффективного управления и демонстрации качества продуктов, услуг и процессов	Определение или разработка соответствующего набора показателей безопасности, основанного на потребностях в информации, связанной с безопасностью; необходимые данные о безопасности собирают, проверяют и хранят; данные о безопасности анализируют и результаты интерпретируют; информационные элементы, связанные с безопасностью, предоставляют объективную информацию, которая помогает принимать решения	
Процесс гарантии качества	Цель процесса заключается в обеспечении эффективного применения процесса управления качеством организации к проекту. Обеспечение качества направлено на обеспечение уверенности в том, что требования к качеству будут выполнены Проводят анализ процессов и результатов проектного цикла, чтобы гарантировать, что производимый продукт будет иметь желаемое качество, а также соблюдение организационной политики и процедур проекта	Оценку продуктов, услуг и процессов, связанных с безопасностью проекта, выполняют в соответствии с политиками, процедурами и требованиями управления качеством; результаты оценок безопасности предоставляют соответствующим заинтересованным сторонам; устранение инцидентов безопасности	

Таблица 2 — Технические процессы в рамках проектирования системы по *[5]*

Процессы согласно *[5]*	Цель	Аспекты безопасности результатов проектирования	Мероприятия, связанные с деятельностью по обеспечению безопасности
Анализ бизнеса или назначения	Процесс анализа бизнеса и назначения предусматривает определение проблемного пространства и характеристику пространства решений, включая соответствующие факторы торгового пространства и предварительные концепции жизненного цикла. Это включает в себя развитие понимания контекста и любых ключевых параметров, таких как критические характеристики качества (например, угрозы безопасности, взаимодействие с пользователем и др.)	Определены аспекты безопасности пространства проблем или возможностей; пространство решений для обеспечения безопасности характеризуется; определены предварительные концепции эксплуатационной безопасности и другие концепции на этапах жизненного цикла; определены и проанализированы возможные альтернативные классы решений для обеспечения безопасности; выбирают предпочтительные классы альтернативных решений для обеспечения безопасности; устанавливают возможность отслеживания проблем и возможностей бизнеса или миссии, связанных с обеспечением безопасности, а также предпочтительных альтернативных классов решений для обеспечения безопасности	Фиксируют бизнес- и операционный контекст, определяют задачи и возможности, операционные сценарии. Определяют предварительные цели заинтересованных сторон в предметной области (бизнес, безопасность, имидж и т. д.) в отношении операционных сценариев, проводят предварительный анализ уязвимостей кибербезопасности
Определение потребностей и требований заинтересованной стороны	Процесс определения потребностей и требований заинтересованных сторон предусматривает отбор и определение характеристик, в том числе критических характеристик качества, и связанных с ними информационных элементов. Мероприятия и документация полезны для выявления, расстановки приоритетов, определения и регистрации требований к критическим характеристикам качества	Определены стороны системы, заинтересованные в обеспечении безопасности; определены необходимые характеристики безопасности и контекст использования возможностей и концепций на этапах жизненного цикла, включая операционные концепции; определены ограничения безопасности системы; определены потребности заинтересованных сторон в обеспечении безопасности; потребности заинтересованных сторон в обеспечении безопасности определяют по приоритетам и преобразуют в четко определенные требования заинтересованных сторон; определены критические показатели эффективности системы безопасности; достигнуто согласие заинтересованных сторон с тем, что их потребности и ожидания в области безопасности адекватно отражены в требованиях; доступны любые вспомогательные системы или услуги, необходимые для удовлетворения потребностей заинтересованных сторон; установлена прослеживаемость требований заинтересованных сторон к заинтересованным сторонам и их потребностям	Предварительный анализ; определение целей домена для заинтересованных сторон и предварительных требований к каждому домену. Разработка плана обеспечения безопасности системы (Ssp) для формализации стратегии безопасности в контексте системы

Продолжение таблицы 2

Процессы согласно *[5]*	Цель	Аспекты безопасности результатов проектирования	Мероприятия, связанные с деятельностью по обеспечению безопасности
Определение системных требований	Процесс определения системных требований предусматривает определение параметров для критических характеристик качества и выбор мер для отслеживания достижения этих требований в отношении конкретной разрабатываемой системы	Определено описание системы, включая системные интерфейсы, функции безопасности и границы, для системного решения; определены системные требования, связанные с безопасностью (функциональные, производительные, технологические, нефункциональные и интерфейсные), а также конструктивные ограничения; определены критические показатели эффективности системы безопасности; проанализированы требования к системе безопасности; разработана возможность сопоставления требований к системе безопасности с требованиями заинтересованных сторон к безопасности	Определение цели обеспечения безопасности с помощью матрицы вероятности/серьезности для различных нежелательных поведений системы в различных сценариях эксплуатации. Нежелательное поведение должно быть определено для каждого операционного сценария с учетом также нежелательных управляющих воздействий. Проверка правильности плана обеспечения безопасности системы
Определение архитектуры	Процесс определения архитектуры предусматривает выявление проблем заинтересованных сторон с точки зрения архитектуры. Эти опасения часто приводят к ожиданиям или ограничениям на этапах жизненного цикла, которые касаются критических характеристик качества, таких как использование (например, доступность, безопасность, эффективность, удобство использования), поддержка (например, ремонтопригодность, управление устареванием), эволюция системы и среды (например, адаптивность, масштабируемость, живучесть), производство (например, технологичность, тестируемость), вывод из эксплуатации (например, воздействие на окружающую среду, транспортабельность) и т. д. В ходе этого процесса дополнительно учитываются те критические требования к характеристикам качества, которые лежат в основе архитектурных решений, включая оценку архитектуры с точки зрения проблем и связанных с ними характеристик	Выявленные заинтересованными сторонами проблемы безопасности решаются с помощью архитектуры; разработана точка зрения на архитектуру безопасности; для системы разработана модель архитектуры безопасности; концепции, свойства, характеристики, поведение, функции или ограничения, которые важны для принятия решений по архитектуре безопасности системы, распределяют между архитектурными объектами; определены системные элементы, связанные с безопасностью, и их интерфейсы; проводят оценку кандидатов на архитектуру безопасности; достигается архитектурная основа безопасности для процессов на протяжении всего жизненного цикла; достигается согласование архитектуры безопасности с требованиями безопасности и конструктивными особенностями; разработана возможность отслеживания элементов архитектуры, связанных с безопасностью, в соответствии с требованиями заинтересованных сторон и безопасности системы	Проведение предварительного анализа мер противодействия безопасности. Проверка требований, вытекающих из разработанной архитектуры безопасности, с учетом не только того, что требуется для номинальных контрмер в каждом из операционных сценариев, но и того, что требуется в случае, если контрмера не применяется или применяется слишком рано, слишком поздно или ненадлежащим образом [анализ режимов сбоев и последствий (FMEA)]

Продолжение таблицы 2

Процессы согласно *[5]*	Цель	Аспекты безопасности результатов проектирования	Мероприятия, связанные с деятельностью по обеспечению безопасности
Определение проекта	Процесс определения проекта предусматривает определение необходимых проектных характеристик, которые включают в себя критические характеристики качества, такие как соответствие проектных критериев специальным характеристикам и оценка альтернативных проектов в соответствии с этими критериями	Определены конструктивные характеристики каждого элемента системы безопасности; требования к системе безопасности распределяют по элементам системы; уточняют интерфейсы между элементами системы, связанными с безопасностью; оценивают альтернативные варианты проектирования элементов системы безопасности; установлена прослеживаемость конструктивных характеристик элементов, связанных с безопасностью, до архитектурных объектов архитектуры системы	Анализ безопасности на системном и подсистемном уровнях, включая операционную, функциональную и физическую архитектуру
Системный анализ	Процесс системного анализа обеспечивает уровень анализа, необходимый для понимания торгового пространства с точки зрения критических характеристик качества, посредством проведения математического анализа, моделирования, экспериментирования и других методов. Результаты анализа используются для принятия компромиссных решений в рамках процесса управления решениями в поддержку других технических процессов	Определены необходимые параметры анализа безопасности системы; допущения и результаты анализа безопасности системы подтверждены; результаты анализа безопасности системы предоставлены для принятия решений; установлена прослеживаемость результатов анализа безопасности системы	Обеспечение уверенности в том, что вероятность критического сбоя системы безопасности соответствует целям заинтересованных сторон. Полный анализ безопасности системы и анализ безопасности подсистемы, обеспечивающий согласованность с помощью системы отслеживания угроз и уязвимостей
Реализация	Процесс внедрения предусматривает регистрацию доказательств того, что были выполнены важнейшие требования к качеству	Выявлены ограничения реализации, влияющие на требования к безопасности системы, архитектуру или дизайн	Для разработки сложных компонентов, как только контрмеры будут определены, можно добавить индивидуальный уровень обеспечения процесса. Особая целостность или уровень доверия присваивается сложным компонентам посредством ссылки на существующие стандарты, согласованные в процессе соглашения

Продолжение таблицы 2

Процессы согласно *[5]*	Цель	Аспекты безопасности результатов проектирования	Мероприятия, связанные с деятельностью по обеспечению безопасности
Интеграция	Процесс интеграции предусматривает планирование интеграции, включая рассмотрение критических характеристик качества, а также обеспечение того, чтобы достижение этих характеристик было определено и зарегистрировано	Определены ограничения интеграции, которые влияют на требования к безопасности системы, архитектуру или дизайн, включая интерфейсы; определены подходы и контрольные точки для безопасной работы собранных интерфейсов и системных функций; проверены интерфейсы между элементами реализованной системы, связанными с безопасностью, которые составляют систему; выявлены результаты обеспечения безопасности интеграции и аномалии; установлена прослеживаемость элементов, связанных с безопасностью интегрированной системы	Полный анализ безопасности системы и анализ безопасности подсистемы, обеспечивающий согласованность с помощью системы отслеживания угроз и уязвимостей
Верификация	Процесс верификации предусматривает планирование и реализацию стратегии проведения верификации, включая критические характеристики качества. Выбранная стратегия верификации может вводить конструктивные ограничения, которые могут повлиять на достижение заданных характеристик	Определены ограничения проверки, которые влияют на требования к безопасности системы, архитектуру безопасности или дизайн; проверена система или элемент, связанный с безопасностью системы; представлены объективные доказательства того, что реализованная система соответствует требованиям безопасности, архитектуре и дизайну; результаты проверки аспектов безопасности и выявленные аномалии	Полный анализ безопасности системы и подсистемы, обеспечивающий согласованность с помощью системы отслеживания опасных факторов и уязвимостей. Проверяют требования к безопасности и составляют отчет об оценке безопасности
Передача	Процесс передачи предусматривает установку системы в рабочей среде. Поскольку некоторые специальные свойства требуют компромисса между конструктивными и эксплуатационными ограничениями, часто важно уделить внимание установке	Определены ограничения перехода, влияющие на требования безопасности системы, архитектуру или дизайн; операторы, пользователи и другие заинтересованные стороны, необходимые для использования и поддержки системы, проходят обучение по аспектам безопасности; выявлены результаты перехода на систему безопасности и аномалии; установленная система активирована и готова к безопасной работе	Полный анализ безопасности системы и подсистемы, обеспечивающий согласованность с помощью системы отслеживания опасных факторов и уязвимостей. Проверка требований к безопасности и составление отчета об оценке безопасности

Окончание таблицы 2

Процессы согласно *[5]*	Цель	Аспекты безопасности результатов проектирования	Мероприятия, связанные с деятельностью по обеспечению безопасности
Валидация	Процесс валидации *предоставляет* доказательства того, что услуги, *оказываемые* системой, отвечают потребностям заинтересованных сторон, включая важнейшие характеристики качества	Определены критерии валидации требований безопасности заинтересованных сторон; подтверждена доступность услуг безопасности, требуемых заинтересованными сторонами; определены ограничения безопасности при проверке, которые влияют на системные требования, архитектуру или дизайн; система или элемент, связанный с безопасностью системы, проверены; выявлены результаты проверки аспектов безопасности и аномалии; предоставлены объективные доказательства того, что реализованная система или элементы системы удовлетворяют потребностям заинтересованных сторон в области безопасности	Проверка и обоснование требований к безопасности, заполнение отчета об оценке безопасности
Функционирование	Использование системы для предоставления своих услуг	Выявлены операционные ограничения, влияющие на требования к безопасности системы, архитектуру или дизайн; обученные технике безопасности квалифицированные операторы; предоставляют услуги по обеспечению системной безопасности, соответствующие требованиям заинтересованных сторон; во время работы контролируют эффективность системы безопасности	Своевременное реагирование на события безопасности, защищающие конфиденциальность, целостность и доступность системы управления
Сопровождение	Поддержание способности системы предоставлять услуги	Выявлены ограничения на техническое обслуживание, влияющие на требования к безопасности системы, архитектуру или дизайн; доступны заменяемые, отремонтированные или пересмотренные элементы системы безопасности; сообщают о необходимости внесения изменений в систему безопасности для корректирующего, усовершенствованного или адаптивного обслуживания; регистрируют данные о сбоях и сроке службы системы безопасности, включая связанные с этим расходы	Тестирование и внедрение исправлений безопасности для устранения уязвимостей
Изъятие и списание	Поддержание способности системы предоставлять услуги	Ограничения по безопасности утилизации являются исходными данными для требований, архитектуры, проектирования и реализации	Удаление конфиденциальной информации из выведенных из эксплуатации частей системы и обеспечение того, чтобы оставшиеся части продолжали соответствовать своим требованиям безопасности

6 Применение серии стандартов МЭК 62443 [6] к цифровому производству

6.1 Общие положения

[6] — серия стандартов промышленной кибербезопасности. Многие отрасли, работающие в сфере автоматизации (например, автоматизация, распределение электроэнергии, мобильность и т. д.), заинтересованы в использовании *[6]*. Данная серия распространяется на весь жизненный цикл производственной системы и содержит требования к поставщикам продукции, интеграторам, поставщикам услуг, а также системным операторам. Такой подход делает *[6]* подходящим документом для определения требований к безопасности интеллектуальных производственных систем, которые либо состоят из компонентов из разных областей, либо должны взаимодействовать с ними. На рисунке 1 показаны опубликованные и одобренные голосованием части *[6]*, другие части и обновления находятся в стадии разработки.

Основные концепции, приведенные в *[6]*, также применимы к реализации программы обеспечения безопасности (*ГОСТ Р 56205, ГОСТ Р ИСО/МЭК 27000*) для интеллектуальных производственных систем. Настоящий стандарт содержит рекомендации по применению *[6]* в интеллектуальных производственных системах. В рамках умного производства стандарт может применяться к компонентам, устройствам, системам, комплексам систем, предприятиям и артефактам умного производства (например, к продуктам). На рисунке 2 показано, как *[6]* применяется в деталях в течение отдельных жизненных циклов средств автоматизации (поставка, интеграция, эксплуатация).

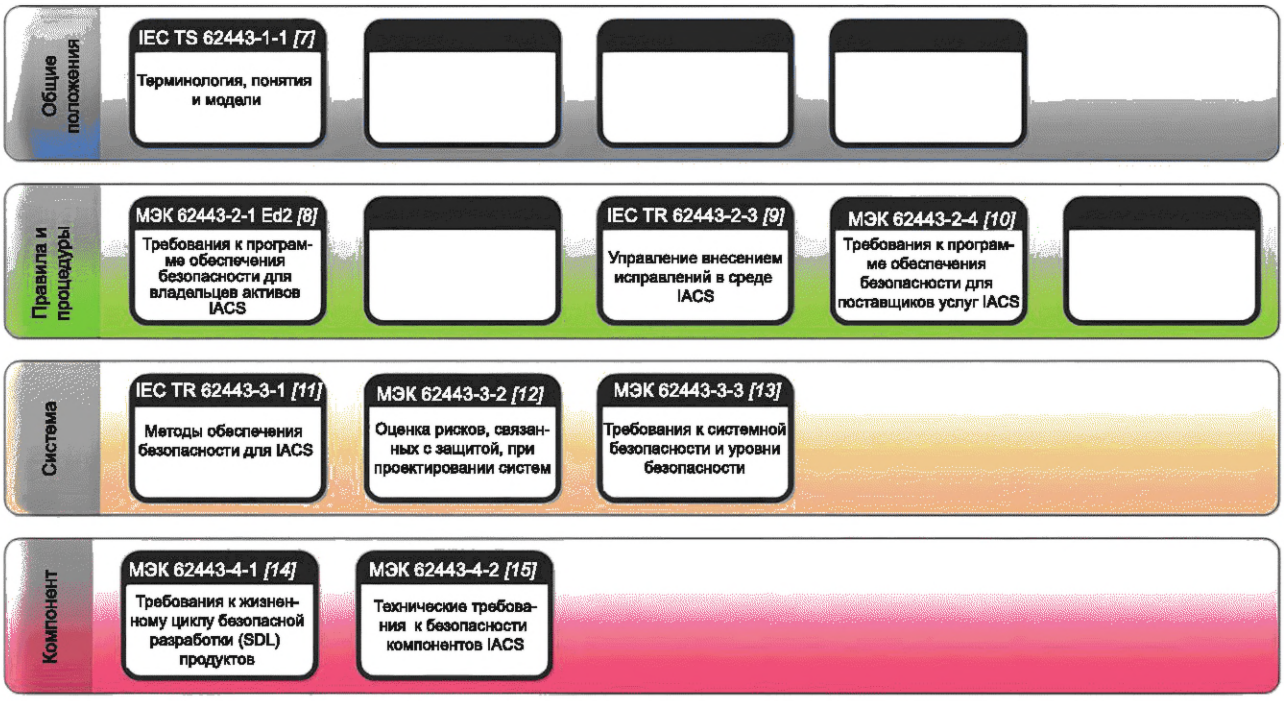

Рисунок 1 — Серия стандартов *[6]*

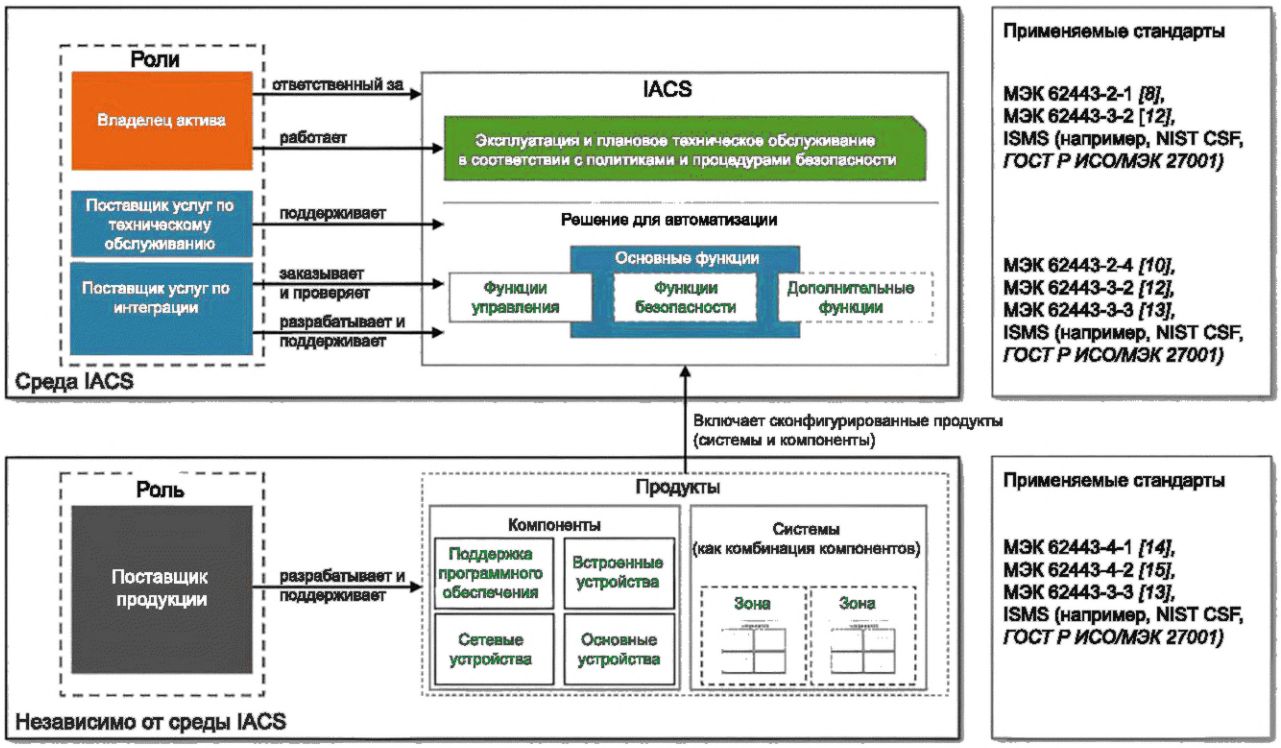

Рисунок 2 — Подробная информация о применении отдельных частей *[6]* для выполнения различных функций в течение отдельных жизненных циклов средств автоматизации

На рисунке 2 показано, как серия стандартов *[6]* ориентирована на различные заинтересованные стороны, такие как поставщики продукции, интеграторы, поставщики услуг, а также системные операторы. Этот целостный подход, соответствующий *[6]*, также делает данную серию стандартов подходящей для интеллектуальных производственных систем, поскольку границы между отдельными этапами (особенно интеграцией и эксплуатацией) будут размыты.

6.2 Соответствие *ГОСТ Р ИСО/МЭК 27000*

Безопасность в организации очень часто сначала внедряется с точки зрения безопасности ISMS (системы менеджмента информационной безопасности) с использованием *ГОСТ Р ИСО/МЭК 27001* и *ГОСТ Р ИСО/МЭК 27002* в дополнение к отраслевому документу. Процесс построен на анализе рисков и внедрении программы управления рисками. В случае промышленной деятельности в сферу применения часто входит IACS (система промышленной автоматизации и управления) с некоторыми специфическими ограничениями в отношении эксплуатации, безопасности и доступности. Подход к кибербезопасности, применяемый в этой ACS, очень часто рассматривается независимо от ISMS.

С точки зрения углубленной кибербезопасности системы ACS и ISMS необходимо рассматривать как систему систем, в которых происходит оценка безопасности. С точки зрения кибербезопасности объединенные отдельные системы предъявляют различные требования, ограничения и риски (например, конфиденциальность, целостность). Действительно, существует множество системных функций, которые часто выполняются ISMS и непосредственно влияют на кибербезопасность операционной части.

Первый подход к этому описан в *ГОСТ Р МЭК 62443-2-1*, который обеспечивает соответствие элементов управления *ГОСТ Р ИСО/МЭК 27001* и *ГОСТ Р ИСО/МЭК 27002* требованиям *[6]*, охватывая аспекты, касающиеся системы, продукта или поставщика услуг. В случае критически важных объектов инфраструктуры необходимо провести более углубленный анализ и оценку рисков, чтобы также решить вопросы безопасности, доступности и эксплуатации в режиме реального времени.

6.3 Эталонная модель

Хотя общая эталонная модель, приведенная в разделе 6 *ГОСТ Р 56205—2014*, обеспечивает хорошую основу для организации различных функциональных аспектов цифровой производственной системы, было бы полезно также рассмотреть примеры архитектур подключенных цифровых производственных систем, отличающихся от классической пирамиды автоматизации, показанной в *ГОСТ Р 56205—2014*, рисунок 16.

6.4 Основополагающие требования

Серия стандартов *[6]* определяет семь основополагающих требований (FRs), которые необходимо соблюдать для обеспечения кибербезопасности систем управления доступом. Эти основополагающие требования также применимы к интеллектуальным производственным системам. Основными требованиями, приведенными в *ГОСТ Р 56205—2014*, являются:

1) контроль доступа (AC): управление доступом к выбранным устройствам, информации или к тому и другому вместе для защиты от несанкционированного доступа к устройству или информации;

2) управление использованием (UC): управление использованием выбранных устройств, информации или того и другого вместе для защиты от несанкционированного использования устройства или информации;

3) целостность данных (DI): обеспечение целостности данных по выбранным каналам связи для защиты от несанкционированных изменений;

4) конфиденциальность данных (DC): обеспечение конфиденциальности данных по выбранным каналам связи для защиты от подслушивания;

5) ограничение потока данных (RDF): ограничение потока данных по каналам связи для защиты от публикации информации неавторизованным источником;

6) своевременное реагирование на события (TRE): реагирование на нарушения безопасности, с уведомлением соответствующих органов, сообщая о необходимых судебных доказательствах нарушения и автоматически принимая своевременные корректирующие меры в критически важных для миссии ситуациях или ситуациях, связанных с безопасностью;

7) доступность ресурсов (RA): обеспечивают доступность всех сетевых ресурсов для защиты от атак типа «отказ в обслуживании».

В то время как в классических системах конфиденциальные пользовательские данные, как правило, не передаются системе автоматизации, с появлением умного производства ситуация изменится. Важность защиты конфиденциальности пользовательских данных возрастет в системах умного производства (например, в фармацевтике). Не требуется устанавливать совершенно новые основополагающие требования к конфиденциальности, поскольку они могут быть учтены в FR4 (конфиденциальность данных) и FR5 (ограничение потока данных) для интеллектуальных производственных систем. При появлении новых угроз может потребоваться разработка других FR. Такие другие FR должны быть разработаны в сотрудничестве с ТС 65/WG 10.

6.5 Зоны и трубопроводы в системе систем

Зоны и трубопроводы являются важной концепцией *[6]*. Идея зон и трубопроводов заключается в разделении сложной системы автоматизации на несколько (вложенных) подсистем. Зона — это группа/подсистема, состоящая из средств автоматизации (устройств), основанных на риске или других критериях, таких как критичность активов, операционные функции, физическое или логическое местоположение, требуемый доступ (например, принципы наименьших привилегий) или ответственная организация. Связь между устройствами внутри зоны или между зонами осуществляется с помощью так называемых каналов (примеры приведены в *ГОСТ Р 56205*).

В то время как зоны могут быть определены в соответствии с различными характеристиками, типичные реализации/установки пытаются сгруппировать производственную систему, принадлежащую зоне, в замкнутом физическом пространстве (например, несколько устройств, локально организованных в производственной линии, организованы в пределах зоны). Интеллектуальные производственные устройства в интеллектуальных системах автоматизации, скорее всего, будут внедряться более гибко. Например, робот участвует в производственном процессе на нескольких производственных линиях, автоматизированные интеллектуальные транспортные средства, перемещающиеся по всему заводу, заменяют стационарную установку конвейерных лент, программные сервисы, используемые в системе автоматизации, развертываются удаленно (в облаке).

Более того, интеллектуальные производственные системы могут использовать измененные архитектурные чертежи. Новые технологии, такие как беспроводные сети, 5G и программно-определяемые сети, позволяют уменьшить физическую иерархию и сложность и отделить физическую топологию сети от функциональной иерархии, как это определено в *[3]*. Зоны и каналы связи должны быть адаптированы к такого рода архитектурам и коммуникационным инфраструктурам.

В *ГОСТ Р 56205* упоминаются виртуальные зоны и трубопроводы. Виртуальные зоны и трубопроводы не привязаны к физическому местоположению. Виртуальные зоны и трубопроводы — это потенциальная концепция для использования в интеллектуальных производственных системах.

В *[12]* пока нет подробных сведений о виртуальных зонах и трубопроводах и нет никаких указаний на то, как зоны и трубопроводы применяются в интеллектуальных производственных системах.

При сегментации интеллектуальных производственных систем необходимо сместить акцент с физического доступа и близости к логическому разделению, основанному на контроле доступа и изоляции виртуальной сети, поддерживаемой криптографическими средствами. Необходимы дополнительные рекомендации по определению и внедрению виртуальных зон и каналов.

6.6 Оценка рисков для безопасности и уровни защиты

Целью оценки рисков безопасности является определение объема и степени необходимых мероприятий по обеспечению безопасности и механизмов для защиты основных функций производственной системы (см. рисунок 2). Оценка рисков безопасности для цифровой производственной системы больше не фокусируется на конкретном продукте и производственном процессе — рейтинги безопасности и требования к безопасности необходимо динамически корректировать в зависимости от фактического использования производственной системы. Необходимым условием для предполагаемого гибкого производства является то, что интеллектуальная производственная система может обеспечивать требуемый уровень безопасности и адаптироваться к нему. Интеллектуальная производственная система представляет собой систему систем. Интеллектуальные компоненты интегрируются в интеллектуальные устройства, образуя интеллектуальную систему, и так далее. Необходим эффективный и четко определенный процесс определения уровня безопасности составной системы.

6.7 Жизненный цикл системы безопасности

Жизненный цикл безопасности цифровой производственной системы должен быть согласован с моделью жизненного цикла цифровой производственной системы. Как отмечалось выше, границы между фазами жизненного цикла исчезнут. Необходимо определить, как модель жизненного цикла системы безопасности *[6]* (см. *ГОСТ Р 56205*) интегрируется с гибкими жизненными циклами цифровой производственной системы, подвергающейся непрерывной реконфигурации. Полный путь на протяжении всех этих переходов должен быть безопасным.

6.8 Аудит и ведение журнала

Аудит и ведение журнала для сценариев умного производства требуют дальнейшего изучения. Компоненты (включая продукты) динамически добавляются и удаляются из производственной системы и/или перемещаются между различными производственными системами. Аудит и ведение журнала необходимы для отслеживания этих операций. Кроме того, необходимо убедиться, что данные аудита и протоколирования, хранящиеся в этих компонентах, остаются доступными, когда какой-либо компонент больше не доступен. Необходимо учитывать, по крайней мере, стандарты *[10]* и *[15]*. Применимость других стандартов нуждается в дальнейшей оценке.

6.9 Заключение

В следующих разделах кратко излагаются рекомендации, касающиеся дальнейшего совершенствования *[6]* для умного производства:

1) согласовывать использование конкретных терминов и определений, особенно в отношении компонентов, продуктов и систем, чтобы избежать недоразумений (см. *[16]*);

2) расширение концепции виртуальных зон и каналов в соответствии с *[6]* для внедрения логических/виртуальных топологий, которые эквивалентны топологиям физической производственной системы;

3) корректировка оценки рисков и уровней безопасности в соответствии с *[6]*, например производственная система позволяет переключаться между различными (предопределенными) уровнями

безопасности в зависимости от фактического производственного контекста (например, производимого продукта);

4) приведение мероприятий по управлению безопасностью в соответствие с требованиями *[6]* с жизненным циклом интеллектуальных производственных систем, особенно с указанием того, в какой степени гибкая реконфигурация должна учитываться при первоначальном проектировании системы и может выполняться в процессе технического обслуживания;

5) т. к. продукт и его данные являются неотъемлемой частью производственной системы (например, передача производственных данных, предоставление данных обратной связи), следовательно, производимый продукт участвует в производственном процессе;

6) расширение возможностей аудита и ведения журнала в соответствии с *[6]* (см. 6.8).

7 Угрозы безопасности цифрового производства

7.1 Общие положения

В этом разделе описываются потенциальные угрозы безопасности интеллектуальных производственных систем. При анализе используется подход, основанный на угрозах. Угроза описывает действие, выполняемое злоумышленником, которое приведет к нарушению одной из следующих целей защиты IACS:

- доступность — система автоматизации способна выполнять свои функции по назначению. Производство не нарушается в результате (преднамеренных) атак;
- целостность — система автоматизации работает так, как задумано, и все данные, используемые в производственной системе, не подвергаются вмешательству или модификации неавторизованными лицами;
- конфиденциальность — определенные данные, например интеллектуальная собственность на продукты, средства обработки или машины, личные данные клиентов, ключевые показатели эффективности, не разглашаются посторонним лицам.

Чтобы охватить широкий спектр потенциальных угроз, в настоящем стандарте используются следующие точки зрения:

- обзор вариантов использования — обсуждаются потенциальные угрозы, относящиеся к нескольким вариантам использования, описанным в *[17]*;
- обзор жизненного цикла — рассматриваются потенциальные угрозы, вызванные дополнительными взаимозависимостями в жизненном цикле интеллектуальных производственных систем.

Угрозы, возникающие в разных представлениях, не являются взаимоисключающими, например, угроза, относящаяся к конкретному варианту использования, также возникает для жизненных циклов или функций, связанных с этим вариантом использования.

7.2 Обзор вариантов использования в области кибербезопасности

7.2.1 Общие положения

В разделе 7 анализируется набор выбранных вариантов использования в отношении кибербезопасности. Проанализированы варианты использования согласно *[17]*. Рабочая группа определила дополнительные варианты использования для иллюстрации конкретной проблемы безопасности. Подборка вариантов использования предназначена для того, чтобы дать общее представление об угрозах и вызовах безопасности, характерных для умного производства. Проблемы классифицируются в соответствии с основополагающими требованиями, приведенными в *[6]*, как описано в 6.4.

Там, где это применимо, рисунки по *[17]*, показывающие техническую перспективу варианта использования, были повторно использованы и снабжены комментариями, чтобы проиллюстрировать, к каким взаимодействиям и/или ресурсам применимы выявленные угрозы. Расположение этих ресурсов и взаимодействие внутри системы в значительной степени зависят от реализации и развертывания самой цифровой производственной системы. То же самое относится и к анализу угроз и рисков безопасности. Пункты 7.2.2—7.2.13 не могут заменить анализ угроз и рисков для реальной системы. Цель состоит в том, чтобы дать некоторые рекомендации по обеспечению безопасности при превращении этих абстрактных вариантов использования в реальную систему.

По мере углубления понимания принципов умного производства и безопасности умного производства будут добавляться дополнительные варианты использования. В приложении А представлен обзор проанализированных вариантов использования и основных требований, которые были учтены.

7.2.2 Пример использования «Изготовление индивидуальных изделий»

Производитель хочет предлагать индивидуальные продукты по запросу заказчика на основе адаптируемой производственной системы, чтобы лучше удовлетворять потребности рынка, соответствующие требованиям заказчика.

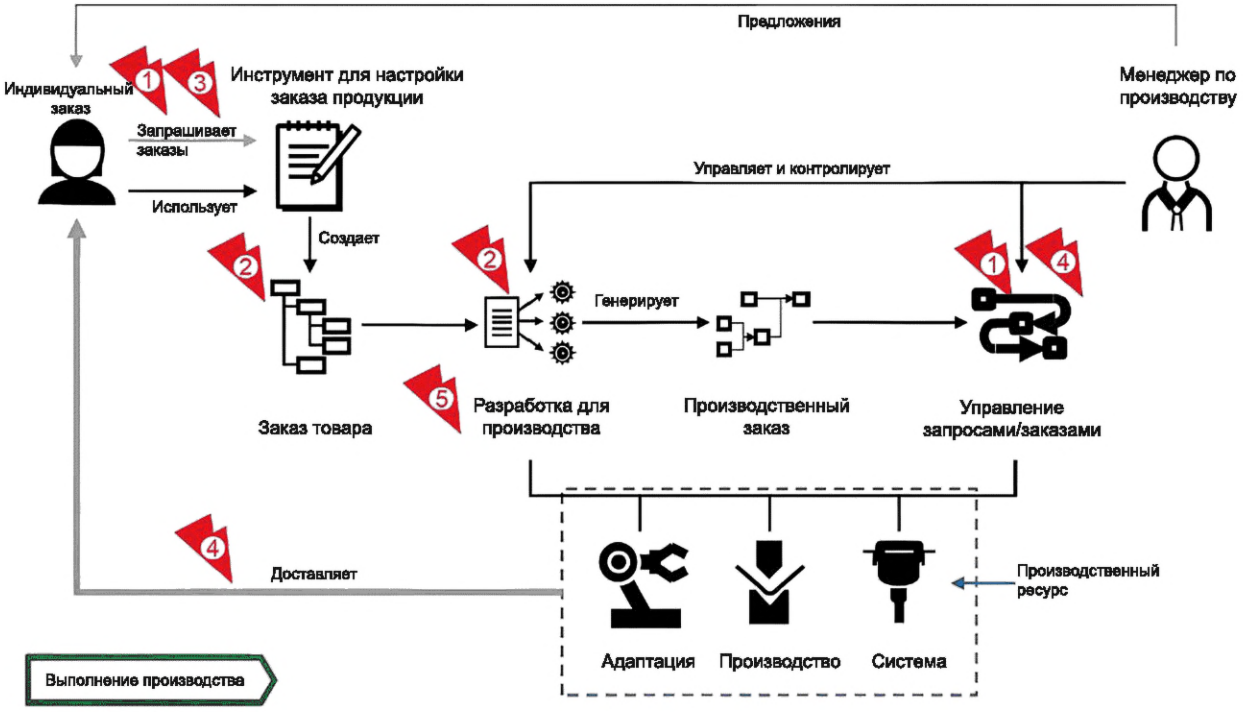

Рисунок 3 — Пример использования «Производство индивидуальных изделий»

На рисунке 3 показаны возможные точки атаки. Потенциальные угрозы и вызовы безопасности подробно описаны в таблице 3.

Таблица 3 — Пример использования «Производство индивидуальных изделий»

Номер п/п	Угроза	Цель защиты	Проблема	Специфика SM
1	Злоумышленник получает доступ к конфиденциальным данным клиента (например, к индивидуальным рецептам, предпочтениям конкретного клиента, адресным данным, ...)	Конфиденциальность	DC01 Конфиденциальность клиентских данных — обеспечение конфиденциальности достоверных клиентских данных. RDF01 Передача клиентских данных, о которых необходимо знать, обеспечивает доступность клиентских данных только в случае необходимости	Индивидуальные данные о продукте клиента
2	Злоумышленник/производитель получает доступ к конфиденциальным данным о продукции (особенно в сценарии «предложение производственных услуг»). Данные могут быть использованы для извлечения интеллектуальной собственности или производства дополнительной продукции	Конфиденциальность	DC05 Конфиденциальность интеллектуальной собственности продукта. DI11 Обеспечить натуральность полуфабрикатов и готовой продукции	Повышенный уровень детализации данных о продукции подвергается воздействию внутри производственной системы

Окончание таблицы 3

Номер п/п	Угроза	Цель защиты	Проблема	Специфика SM
3	Злоумышленник отказывается от индивидуального заказа. Товар должен быть утилизирован/продан по более низкой цене	Честность	AC01 Аутентификация клиента — убедиться в подлинности заказа	Заказы обмениваются между различными доменами безопасности (например, субпоставщиками). Заказы, ориентированные на конкретных клиентов, с меньшей вероятностью найдут альтернативный спрос
4	Злоумышленник манипулирует процессом доставки — например, чтобы получить более ценный продукт вместо того, который был заказан. Кто-то другой получил не тот товар	Честность	AC01 Аутентификация клиента. DI01 Целостность передаваемых данных — обеспечить подлинность и целостность заказа. Соответствующие концепции необходимо найти или разработать в сотрудничестве с логистической отраслью	Заказы обмениваются между различными доменами безопасности (например, субпоставщиками)
5	Злоумышленник разрабатывает заказ на продукцию, используя (известную) ошибку/недостаток в разработке производственного процесса, чтобы нанести ущерб производственной системе (например, превысить фактические ограничения производственной системы)	Доступность	DI12 Целостность данных относительно известных граничных условий — реализовать проверку входных данных, принимать заказы на продукцию только в четко определенном диапазоне изменений. TRE03 Ведение журнала аудита для мониторинга безопасности и криминалистики — вести полный учет заказов на продукцию	Заказ клиента напрямую влияет на производственный процесс (например, передача рецепта, цифровой модели продукта)

7.2.3 Пример использования «Стандартизация производственных технологий»

Производитель запрашивает производственные ресурсы, соответствующие семантически определенным производственным возможностям, с целью повышения эффективности и гибкости производства (например, путем аутсорсинга или инсорсинга производственных заказов).

Поставщик производственных ресурсов хочет предлагать производственные ресурсы, соответствующие семантически определенным производственным возможностям, но также хочет иметь возможность делать уникальные коммерческие предложения.

На рисунке 4 показаны возможные точки атаки. Потенциальные угрозы и вызовы безопасности подробно описаны в таблице 4.



Рисунок 4 — Пример использования «Стандартизация производственных технологий»

Таблица 4 — Пример использования «Стандартизация производственных технологий»

Номер п/п	Угроза	Цель защиты	Проблема	Специфика SM
1	Раскрытие подробных планов строительства (например, 3D-моделей) в рамках производственной сети	Конфиденциальность	DC05 Конфиденциальность интеллектуальной собственности на продукцию — обеспечение конфиденциальности прав интеллектуальной собственности, содержащихся в планах строительства	Оцифрованная информация, которой обмениваются в рамках производственной системы, позволяет легко воспроизводить ее. Задействованы различные заинтересованные стороны в области ИС (план создания продукта, технология производства, оператор)
2	Раскрытие ноу-хау сторонних продуктов, производства или обработки (например, 3D-моделей, технологических данных) во время их использования/обработки производственным устройством	Конфиденциальность	DC07 Доверенное исполнение — сторонние поставщики производственных ноу-хау должны быть уверены, что их IP-адрес не будет скомпрометирован использующими его производственными устройствами	Производственные устройства и технологии производства могут быть разделены (например, модели продуктов, технологические данные, динамически предоставляемые независимыми сторонами)

7.2.4 Пример использования «Гибкое планирование и распределение ресурсов»

Руководитель производства стремится свести к минимуму время простоя (перебои в работе) и оптимизировать использование производственных ресурсов.

На рисунке 5 показаны возможные точки атаки. Потенциальные угрозы и вызовы безопасности подробно описаны в таблице 5.

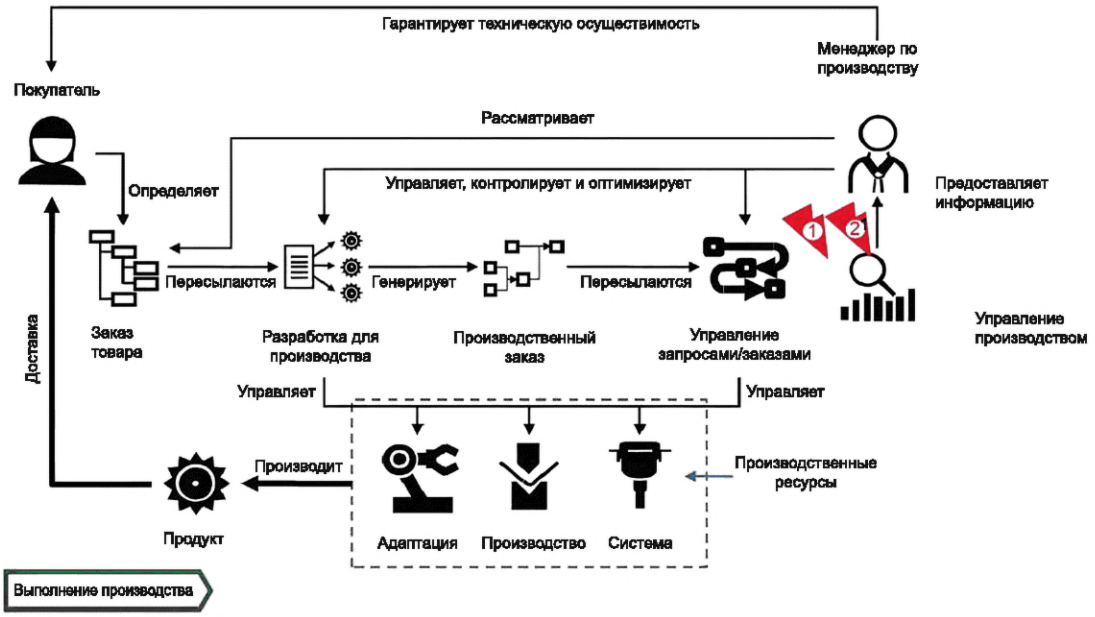

Рисунок 5 — Пример использования «Гибкое планирование и распределение ресурсов»

Таблица 5 — Пример использования «Гибкое планирование и распределение ресурсов»

Номер п/п	Угроза	Цель защиты	Проблема	Специфика SM
1	Злоумышленник имитирует (неожиданное) событие, приводящее к перенастройке системы автоматизации	Целостность	AC06 Проверка подлинности лиц, запрашивающих перепланировку UC01 Использование контроля производственного плана DI04 Целостность данных производственных планов — перепланировка производственного плана должна быть инициирована/подтверждена уполномоченной стороной	Постоянное изменение — это особенность, которая неочевидна для людей-операторов, поскольку вывод из предполагаемого поведения не является очевидным
2	Злоумышленник манипулирует информацией об имеющихся производственных ресурсах, в результате чего производитель не может выполнить свои обязательства	Честность. Доступность	DI04 Целостность данных производственных планов TRE02 Своевременное реагирование, когда система доступна лишь частично	Динамическое внедрение доступных ресурсов вместо фиксированного распределения ресурсов

7.2.5 Пример использования «Модульность производственной системы»

Производитель хочет создать адаптируемую производственную систему, основанную на взаимозаменяемых производственных ресурсах, чтобы лучше реагировать на меняющиеся требования рынка, соответствующие требованиям заказчика.

Новый полевой компонент автоматически добавляется в существующую производственную систему.

Производственная система перенастраивается, например:

- продукт должен быть изготовлен с использованием другого оборудования из-за его доступности (например, непредвиденный простой запланированного станка);
- оборудование перенастраивается для производства другого продукта.

На рисунке 6 показаны возможные точки атаки. Потенциальные угрозы и вызовы безопасности подробно описаны в таблице 6.

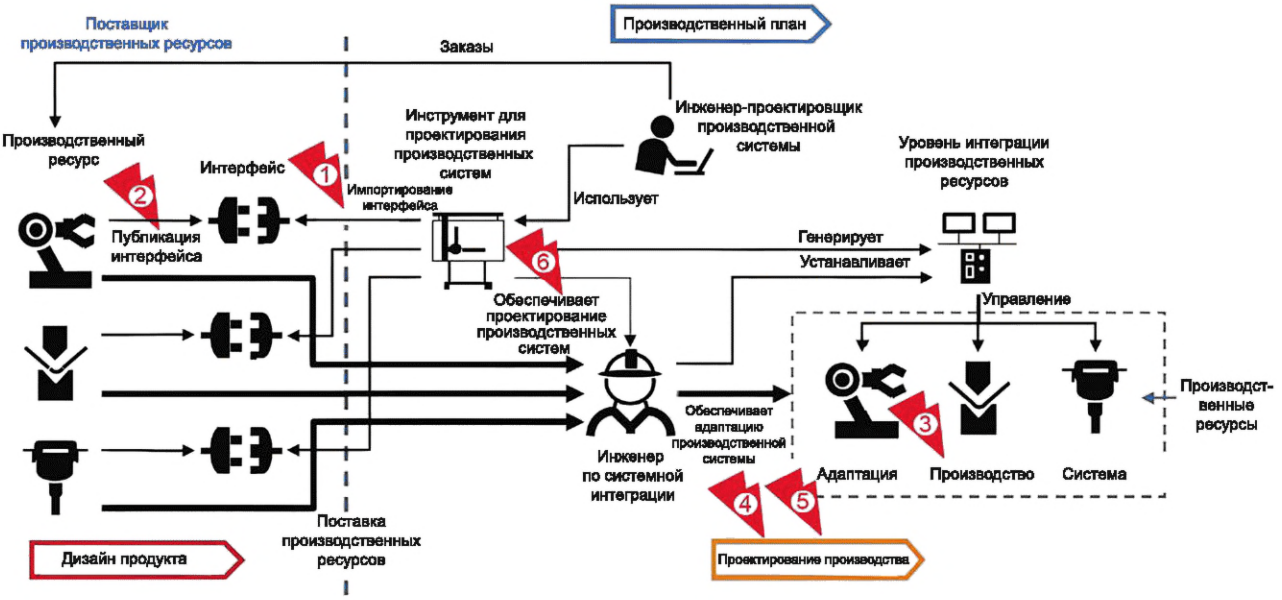

Рисунок 6 — Пример использования «Модульность производственной системы»

Таблица 6 — Пример использования «Модульность производственной системы»

Номер п/п	Угроза	Цель защиты	Проблема	Специфика SM
1	Полевое устройство подключается к производственной системе и получает доступ к конфиденциальной информации, не предназначенной для этого устройства	Целостность	UC05 Использование управления полевыми устройствами — права доступа к новым полевым устройствам должны быть установлены в соответствии с их предполагаемой задачей в производственном процессе	Процесс начальной загрузки системы безопасности. Устройство изначально не известно, но требует достаточных разрешений для интеграции/взаимодействия с существующей системой
2	Новое полевое устройство выдает себя за другое полевое устройство (например, предлагает функции, которые оно на самом деле не может обеспечить) для получения доступа к конфиденциальной информации	Конфиденциальность	AC02 Аутентификация устройств/датчиков — устройство должно предоставить подтвержденную информацию о своей идентификации и свойствах/функциях	Никаких специальных инженерных процессов

Окончание таблицы 6

Номер п/п	Угроза	Цель защиты	Проблема	Специфика SM
3	(Скомпрометированное) новое полевое устройство нарушает производственный процесс	Доступность	UC05 Управление использованием полевых устройств — новые права доступа к полевым устройствам необходимо установить в соответствии с их предполагаемой задачей в производственном процессе. RDF02 Ограничение потока данных, ориентированное на задачи — дальность связи нового устройства должна быть ограничена в соответствии с его предполагаемой задачей в производственном процессе	
4	Злоумышленник использует промежуточные состояния, которые не имеют определенного уровня безопасности	Конфиденциальность, честность	DI06 Целостность системы во время переходов — необходимо, чтобы весь путь перехода был безопасен. Это потенциально исключает несколько (оптимальных) путей перехода	Реконфигурация существующей производственной системы в процессе эксплуатации
5	Злоумышленник пользуется пробелами в защите отдельных устройств во время перехода, например защита зоны может выйти из строя при перемещении устройства	Честность	DI07 Автономная базовая защита конечной точки. Для систем ACS со статическим проектированием часто предполагается, что устройство расположено в выделенной зоне доверия и защищено периметром этой зоны. Это предположение больше не справедливо для всех интеллектуальных производственных систем. Каждое устройство должно обеспечивать некоторую базовую самозащиту на ограниченном функциональном уровне. Некоторые расширенные функции не доступны после того, как устройству удалось проверить соответствие среды определенным условиям (безопасности)	Отдельные устройства/конечные точки больше не могут полагаться на стабильную рабочую среду
6	Злоумышленник определяет новое состояние конфигурации (или переопределяет старое), которое можно легче использовать	Честность	DI03 Целостность данных новых функций/конфигураций — перед внедрением новую конфигурацию необходимо проверить и авторизовать. AC04 Аутентификация поставщиков изменений конфигурации — только авторизованные источники могут инициировать изменения конфигурации	Изменения конфигурации являются нормальными и поэтому не всегда подозрительными

7.2.6 Пример использования «Контуры обратной связи»

Компания-производитель хочет, чтобы клиент (соответствующий рынок) передавал опыт использования (соответствующее восприятие) поставляемого продукта обратно компании-производителю для оптимизации предложения клиенту (соответствующему рынку).

На рисунке 7 показаны возможные точки атаки. Потенциальные угрозы и проблемы безопасности подробно описаны в таблице 7.

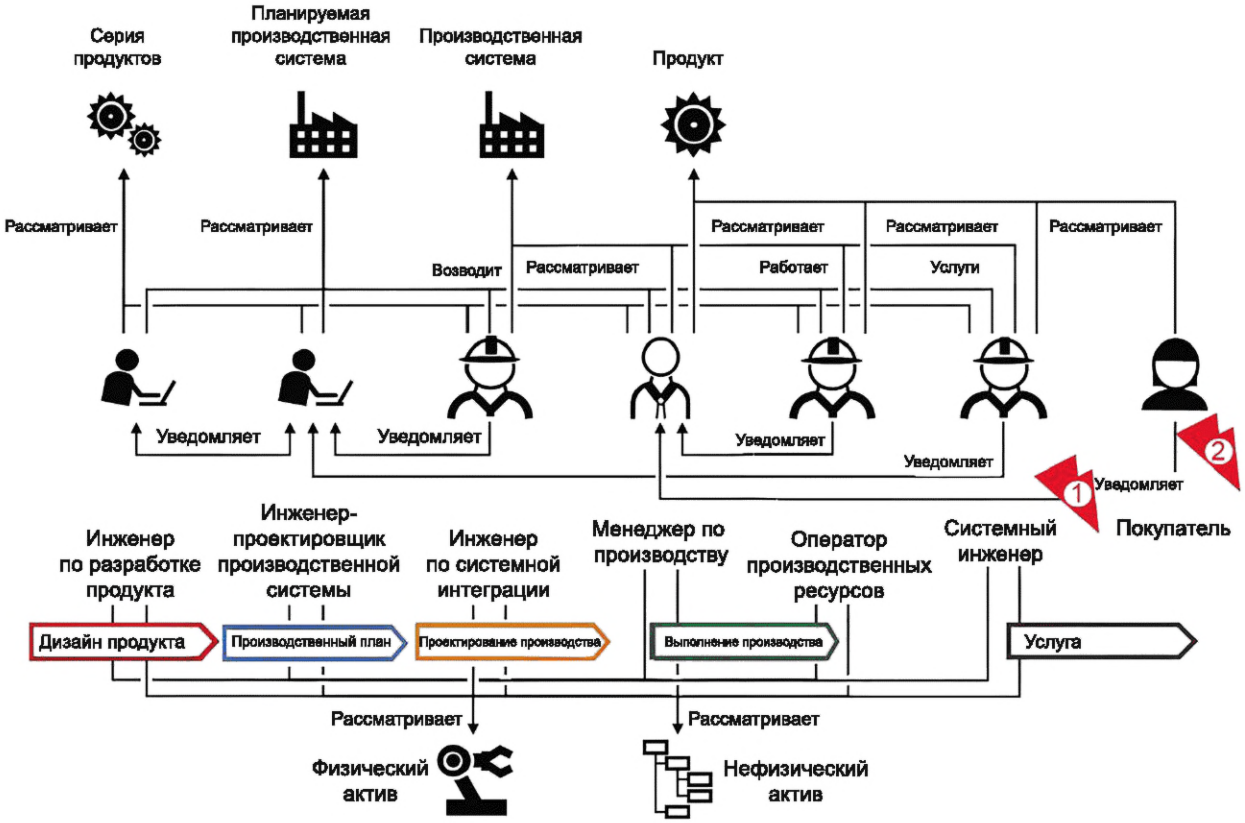

Рисунок 7 — Пример использования «Контуры обратной связи»

Таблица 7 — Пример использования «Контуры обратной связи»

Номер п/п	Угроза	Цель защиты	Проблема	Специфика SM
1	Злоумышленник/потребитель возвращает неверные данные в производственный процесс	Целостность	AC01 Аутентификация клиента — обеспечение подлинности/надежности данных обратной связи между доменом клиента и производственным доменом	Подключенные интеллектуальные продукты являются частью всего жизненного цикла согласно *ГОСТ Р 59799*. Особенно новым является прямое использование данных о клиентах в режиме обратной связи
2	Злоумышленник создает профиль конечного клиента (например, поведение, местоположение) на основе данных обратной связи	Конфиденциальность	DC01 Конфиденциальность данных клиентов — защита конфиденциальности собранных данных конечных пользователей	

7.2.7 Пример использования «Моделирование в действии»

Менеджер по производству хочет смоделировать модель производства, чтобы оптимизировать производство, проверить принципиальную осуществимость, снизить риски безопасности, возникающие в результате реконфигурации производственной системы, и/или ускорить реконфигурацию производственной системы.

В центре внимания анализа безопасности находится использование текущих данных в рамках предопределенных имитационных моделей.

На рисунке 8 показаны возможные точки атаки. Потенциальные угрозы и вызовы безопасности подробно описаны в таблице 8.

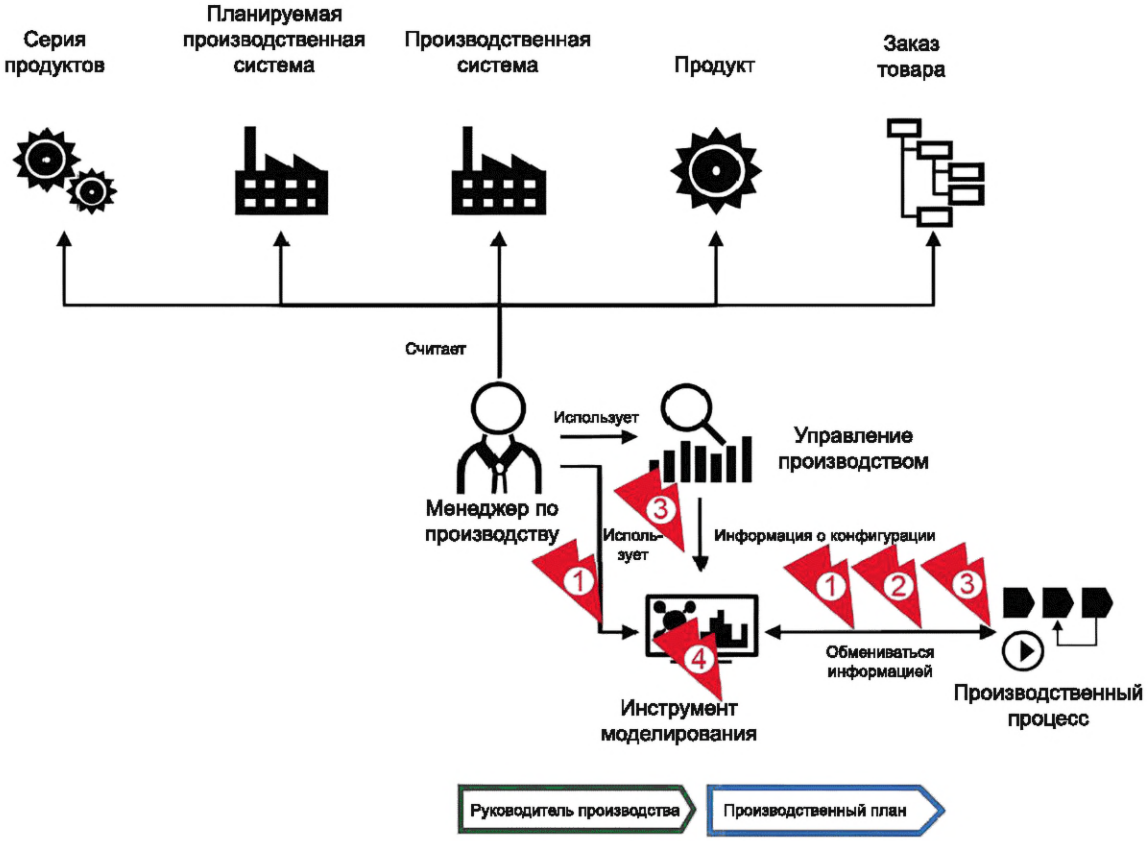

Рисунок 8 — Пример использования «Моделирование в действии»

Таблица 8 — Пример использования «Моделирование в действии»

Номер п/п	Угроза	Цель защиты	Проблема	Специфика SM
1	Данные моделирования используются злоумышленником/конкурентом для анализа производственного процесса с целью получения конкурентного преимущества	Конфиденциальность	DC03 Конфиденциальность имитационной модели данных — сохранность имитационной модели и конфиденциальность	Постоянный обмен данными увеличивает раскрытие критически важных данных
2	Злоумышленник нарушает обмен информацией между имитационной моделью и реальной производственной системой и препятствует принятию своевременных решений	Доступность	RA01 Наличие тока данные моделирования — моделирование необходимо выполнять на текущих данных	Цифровое производство предлагает моделирование для поддержки принятия важных решений

Окончание таблицы 8

Номер п/п	Угроза	Цель защиты	Проблема	Специфика SM
3	Злоумышленник вводит неверные данные в имитационную модель, чтобы инициировать неправильные решения (например, в производстве закончились поставки)	Целостность, доступность	AC03 Аутентификация данных моделирования поставщиков UC03 Использование управления имитационной моделью — только правильно идентифицированные и уполномоченные стороны предоставляют данные для моделирования	Цифровое производство предлагает моделирование для поддержки принятия важных решений
4	Злоумышленник манипулирует симуляционной моделью, чтобы побудить принять неверные решения	Честность	DI02 Целостность данных имитационной модели — целостность имитационной модели (и системы управления моделированием) должна быть обеспечена	

7.2.8 Пример использования «Моделирование в проектировании и инжиниринге»

Инженер-проектировщик завода хочет смоделировать модель проектируемой производственной системы, чтобы снизить риски безопасности, возникающие в результате проектирования производственной системы, и/или ускорить проектирование производственной системы.

В центре внимания анализа безопасности находится создание и распространение имитационных моделей для реальной производственной системы.

На рисунке 9 показаны возможные точки атаки. Потенциальные угрозы и вызовы безопасности подробно описаны в таблице 9.

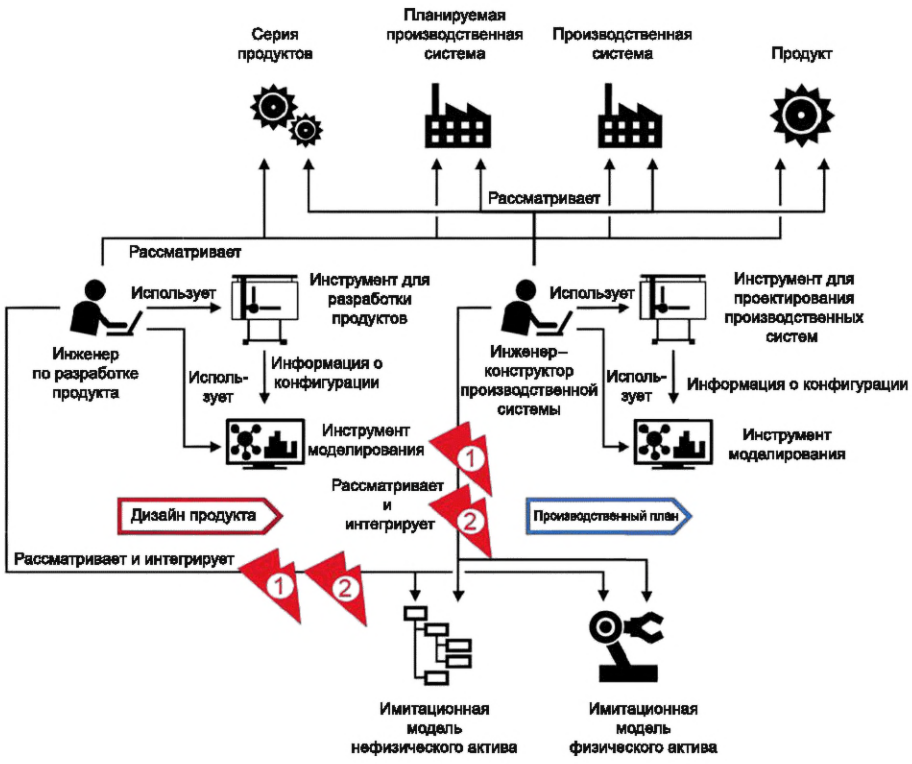

Рисунок 9 — Пример использования «Моделирование в проектировании и инжиниринге»

Таблица 9 — Пример использования «Моделирование в проектировании и инжиниринге»

Номер п/п	Угроза	Цель защиты	Проблема	Специфика SM
1	Моделирование виртуального предприятия используется злоумышленником для оценки потенциальных уязвимостей системы и подготовки атаки на реальную производственную систему	Конфиденциальность	UC03 Использование управления имитационной моделью — ограничить доступ к имитационной модели	Наличие комплексной и актуальной оцифрованной модели завода
2	Имитационная модель используется злоумышленником для анализа производственного процесса с целью получения конкурентного преимущества	Конфиденциальность	DC03 Конфиденциальность данных имитационной модели — сохранять конфиденциальность имитационной модели и данных	Наличие комплексной и актуальной оцифрованной модели завода

7.2.9 Варианты использования «Обновление и функциональная масштабируемость производственных ресурсов» и «Конфигурация устройства»

Цель «Обновления и функциональной масштабируемости производственных ресурсов» заключается в том, что поставщик производственных ресурсов хочет предложить дополнительные функциональные возможности на основе программного обеспечения, которые могут быть разблокированы после того, как производственный ресурс был продан и уже использовался производителем для создания дополнительных источников дохода. Производитель хочет использовать только ту функциональность производственного ресурса, которая необходима для его конкретной цели, но хочет иметь возможность очень гибко реагировать на изменения рынка, обновляя (или даже понижая) производственный ресурс.

Цель раздела «Конфигурация устройства» заключается в том, что поставщик программного обеспечения хочет предложить программные приложения, которые могут быть гибко развернуты на устройствах или в общей вычислительной инфраструктуре.

Потенциальные угрозы и вызовы безопасности подробно описаны в таблице 10.

Таблица 10 — Варианты использования «Обновление и функциональная масштабируемость производственных ресурсов» и «Конфигурация устройства»

Номер п/п	Угроза	Цель защиты	Проблема	Специфика SM
1	Злоумышленник/клиент использует расширенные производственные функции, не заплатив за них	Честность	UC04 Использование контроля производственных возможностей — только авторизованные пользователи получают доступ к определенным производственным возможностям	Функциональность больше не является исключительной и определяется аппаратным обеспечением, но становится «определяемым программным обеспечением»
2	Злоумышленник устанавливает вредоносные дополнительные функции, оказывающие негативное влияние на компьютер или его среду	Целостность, доступность	AC07 Аутентификация поставщиков для функциональных расширений DI03 Целостность данных новых функций/конфигураций — перед установкой новых функций необходимо проверить и авторизовать их	

Окончание таблицы 10

Номер п/п	Угроза	Цель защиты	Проблема	Специфика SM
3	Злоумышленник перепроектирует/извлекает IP-адрес из функционального обновления. Примечание — Функциональное обновление может даже предоставляться заинтересованной стороной, отличной от устройства, например, в виде приложения	Конфиденциальность	Конфиденциальность интеллектуальной собственности продукта — защита ноу-хау, установленных и работающих в потенциально враждебной среде	Функциональные улучшения, добавленные к устройствам независимыми третьими лицами

7.2.10 Вариант использования «Извлечение информации из производственных систем»

Производитель хочет собирать информацию о производственной системе без побочных эффектов и простым способом, чтобы анализировать и обрабатывать эту информацию, используя общую вычислительную инфраструктуру.

На рисунке 10 показаны возможные точки атаки. Потенциальные угрозы и проблемы безопасности подробно описаны в таблице 11.

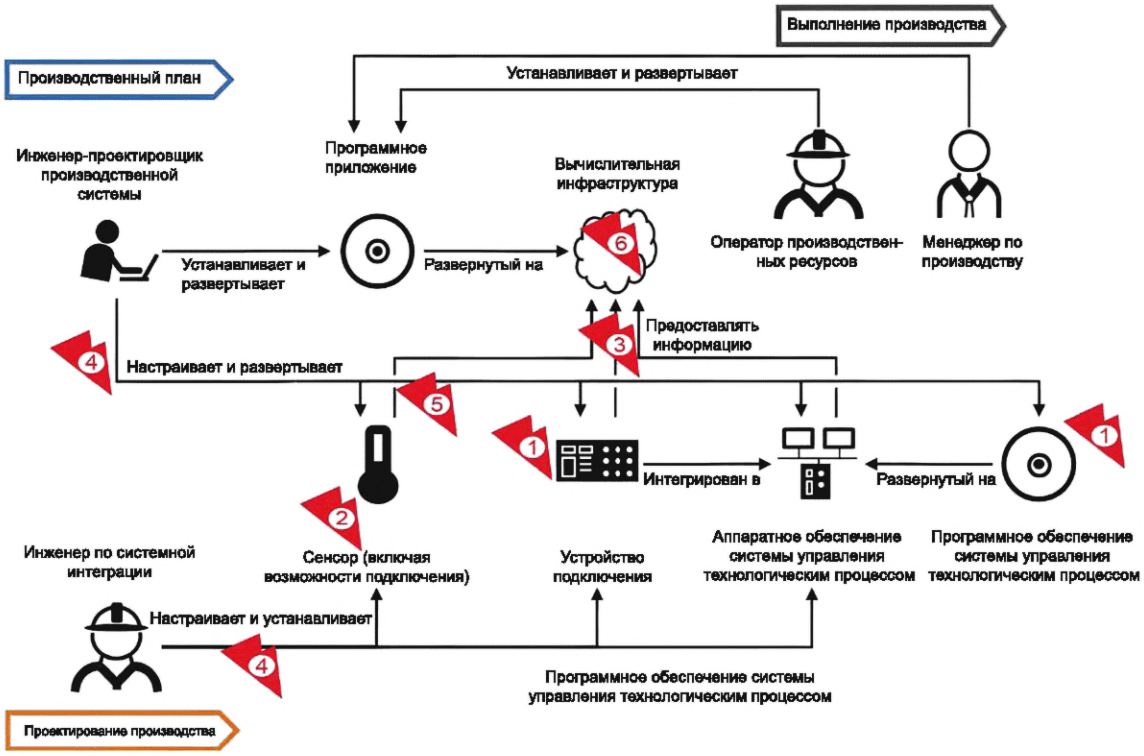

Рисунок 10 — Вариант использования «Извлечение информации из производственных систем»

Таблица 11 — Вариант использования «Извлечение информации из производственных систем»

Номер п/п	Угроза	Цель защиты	Проблема	Специфика SM
1	Злоумышленник подделывает устройство или отправляет собственные или измененные данные во внутреннюю службу и вводит аналитику в заблуждение	Честность	AC02 Аутентификация устройства/датчика AC09 Аутентификация данных датчика DI08 Данные о целостности собранного и агрегированного датчика	
2	Злоумышленник размещает поддельный датчик или интеллектуальное устройство агрегирования датчиков (например, EDGE аналитика) в производственной системе, дающей неверные результаты измерений	Честность	DI09 Обеспечить подлинность установленного устройства/датчика	Прямое подключение от датчика до серверной части (например, облако аналитика)
3	Злоумышленник перехватывает данные датчиков, измененные с помощью внутренней системы	Конфиденциальность	DC02 Конфиденциальность данных в сети	
4	Злоумышленник изменяет конфигурацию датчиков таким образом, что данные непреднамеренно покидают производственную систему	Честность	UC05 Использование управления полевыми устройствами — защита параметров конфигурации устройства/датчика	
5	Управляемый датчик отправляет (необработанные) данные в серверную службу, которая не собиралась покидать производственную систему	Конфиденциальность	RDF03 Ограничение потока/воздействия (необработанных) данных датчиков — клиент/оператор системы имеет возможность решать, какие данные предоставляются внешним поставщикам услуг	
6	Собранные данные датчиков (например, видеопотоки) используются неправомерно для отслеживания персонала, построения профилей (производительности) персонала и т. д.	Конфиденциальность	DC08 Конфиденциальность данных датчиков, относящихся к сотрудникам	

7.2.11 Вариант использования «Самооптимизация производственных ресурсов»

Вариант использования «Оптимизация работы посредством машинного обучения»

Пример использования «Оптимизация проектирования и проектирования посредством машинного обучения»

Аналитика данных применяет технологии машинного обучения (ML) (например, искусственные нейронные сети) к большим объемам данных, собираемых полевыми устройствами и интеллектуальными датчиками (7.2.9).

Потенциальные угрозы и проблемы безопасности подробно описаны в таблице 12.

Таблица 12 — Вариант использования «Машинное обучение»

Номер п/п	Угроза	Цель защиты	Проблема	Специфика SM
1	Злоумышленник предоставляет манипулируемые данные обучения или тестирования, чтобы внести предвзятость в систему	Честность	DI10 Целостность собранных и агрегированных данных датчиков, используемых для обучения и тестирования машинного обучения	Использование машинного обучения
2	Злоумышленник предоставляет системе машинного обучения манипулируемые входные данные, чтобы спровоцировать необученное/неопределенное поведение (входные данные не охватываются обучающими данными)	Честность	DI08 Целостность собранных и агрегированных данных датчиков	Использование машинного обучения
3	Злоумышленник извлекает конфиденциальную информацию, которая изначально содержится в обучающих данных модели ИИ	Конфиденциальность	DC09 Раскрытие конфиденциальных данных, которые содержатся в данных машинного обучения	Использование машинного обучения и данных обучения
4	Злоумышленник пытается извлечь выгоду из неопределенности человека-оператора, возникающей из-за пропажи результатов ИИ	Доступность. Целостность	TRE06 Обеспечить объяснимость предложений/инструкций машинного обучения системы	Принятие решений на основе результатов машинного обучения системы

7.2.12 Пример использования «Проектирование для повышения энергоэффективности» и «Оптимизация энергопотребления»

Менеджер по производству хочет оптимизировать работу производственной системы в соответствии с конкретными ключевыми показателями эффективности использования энергии, например, потреблением энергии и/или затратами на электроэнергию.

Потенциальные угрозы и вызовы безопасности подробно описаны в таблице 13.

Таблица 13 — Пример использования «Проектирование для повышения энергоэффективности» и «Оптимизация энергопотребления»

№ п/п	Угроза	Цель защиты	Проблема	Специфика SM
1	Злоумышленник манипулирует системой, пока она неисправна. Манипуляция не замечена, так как отключение также влияет на системы/решения безопасности или они недоступны во время отключения питания. Это также может произойти непреднамеренно	Целостность. Доступность	RA05 Наличие датчиков и мониторинг — датчики, необходимые для мониторинга безопасности, необходимо подключить к сети и постоянно контролировать. DI05 Целостность технических данных — все, что необходимо для проверки целостности системы во время разработки, теперь должно быть доступно также во время работы	Случайное отключение части системы во время работы

Окончание таблицы 13

№ п/п	Угроза	Цель защиты	Проблема	Специфика SM
2	Злоумышленник использует незащищенную функцию управления энергопотреблением и выключает (частично) производственную систему	Доступность	AC04 Аутентификация конфигурации при смене провайдера — только авторизованные источники могут инициировать изменения. UC05 Использование управления полевыми устройствами — предоставление доступа управления устройством, а также управлением питания или интеллектуальными переключателями	
3	Злоумышленник использует выключение для физического доступа к устройству (например, из-за снижения физической безопасности во время выключения) и получает конфиденциальные данные с устройства	Конфиденциальность	RDF04 Ограничение временной доступности информации, например удаление информации после использования	

7.2.13 Пример использования «бесшовных моделей»

Производитель заинтересован в управлении растущей технической сложностью продуктов и производственных систем для принятия сбалансированных и надежных решений, улучшения рабочих процессов и снижения общих затрат.

Потенциальные угрозы и вызовы безопасности подробно описаны в таблице 14.

Таблица 14 — Пример использования «бесшовных моделей»

Номер п/п	Угроза	Цель защиты	Проблема	Специфика SM
1	Злоумышленник получает доступ к конфиденциальным данным проектирования (например, моделям САПР, планы строительства), обычно не представленным в системе	Конфиденциальность	DC04 Конфиденциальность инженерных данных — используемый формат обмена обеспечивает средства для защиты конфиденциальности данных. UC02 Использование контроля информации — только авторизованные лица имеют доступ к защищенной информации	
2	Злоумышленник манипулирует инженерными и/или проектными данными, чтобы понизить производственный процесс или качество продукции	Честность	DI01 Целостность обмениваемых данных — используемый формат обмена обеспечивает средства защиты целостности	

7.3 Взгляд на кибербезопасность в рамках жизненного цикла цифрового производства

Цифровое производство требует тесного взаимодействия между процессами, относящимися к разным этапам жизненного цикла. Как показано на рисунке 11, различные этапы не только взаимодействуют в процессе производства, но и обмениваются информацией друг с другом на протяжении всего срока службы.

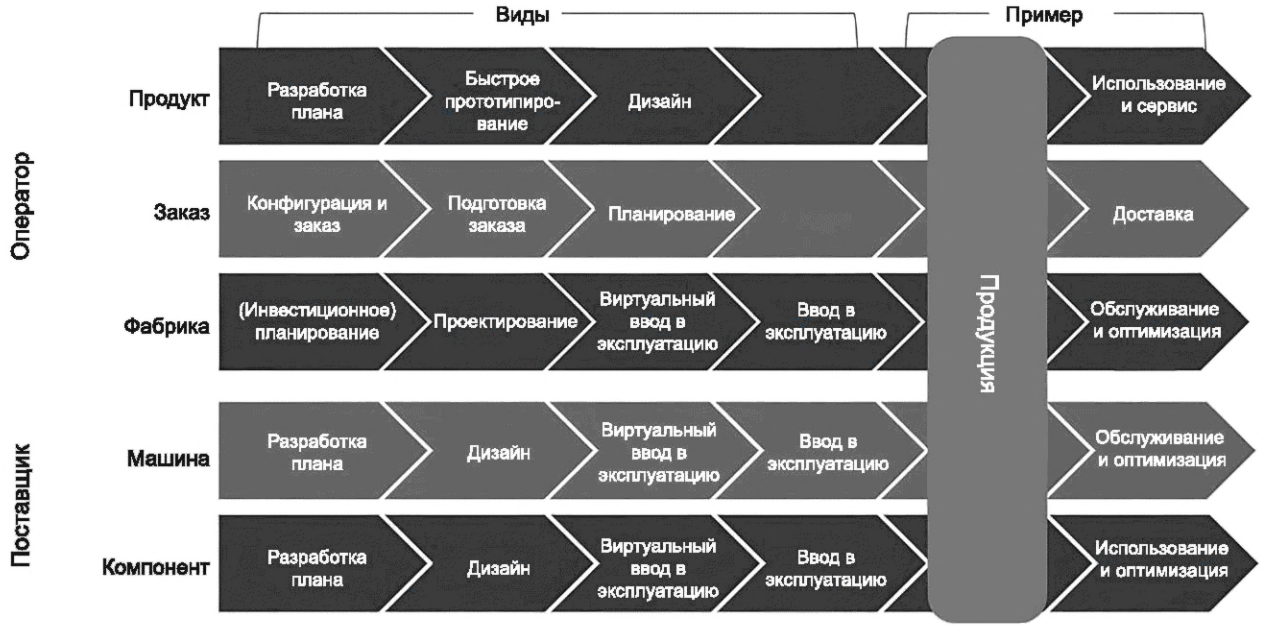

Рисунок 11 — От потоков создания ценности к сетям создания ценности

Представление о кибербезопасности в рамках жизненного цикла цифрового производства представлено в таблице 15.

Таблица 15 — Обзор жизненного цикла умного производства с точки зрения кибербезопасности

Процесс жизненного цикла под атакой	Угроза	Проблема
Конфигурация и заказ	Злоумышленник подслушивает информацию о графике производства, передаваемую на завод через Интернет, например, для получения конкурентных преимуществ	DC02 — например, зашифровать сетевые данные или использовать VPN. DC01 — защита конфиденциальности информации о заказах клиентов, хранящейся на активах SM. DC10 — защита конфигурации графика производства, хранящейся в активах SM
Планирование	Злоумышленник изменяет информацию о графике производства, передаваемую на завод через Интернет, например, чтобы вызвать задержки производства или перепроизводство	DC02 — например, зашифровать сетевые данные или использовать VPN. AC05, UC06 — только аутентифицированным и авторизованным лицам разрешено участвовать в обмене информацией

Окончание таблицы 15

Процесс жизненного цикла под атакой	Угроза	Проблема
Обслуживание и оптимизация	Злоумышленник изменяет информацию о производственных показателях, передаваемую с завода через Интернет, например, чтобы вызвать финансовый ущерб компании (пропущенные заказы или ненужное перепроизводство)	DC02 — например, зашифровать сетевые данные или использовать VPN. AC05, UC06 — только аутентифицированным и авторизованным лицам разрешено участвовать в обмене информацией
Использование и обслуживание	Злоумышленник подслушивает информацию, которая передается в компанию с помощью интеллектуальных продуктов, сообщающих об обслуживании и статусе гарантии через Интернет, например, для идентификации клиентов и выявленных ими проблем	DC02 — например, зашифровать сетевые данные или использовать VPN. AC05, UC06 — только аутентифицированным и авторизованным лицам разрешено участвовать в обмене информацией
Оптимизация	Для повышения производительности уровень защиты снижается. Злоумышленник подслушивает информацию, которая передается с завода поставщикам или от цифрового производственного оборудования, отчетность по техническому обслуживанию и статус гарантии через Интернет, например, для определения оборудования для соревнований и производительности, а также для выявления производственного оборудования	DC02 — например, зашифровать сетевые данные или использовать VPN. AC05, UC06 — только аутентифицированным и авторизованным лицам разрешено участвовать в обмене информацией
Дизайн, планирование	Злоумышленник подслушивает информацию об определении продукции и производственных инструкциях, которая передается на завод через Интернет, например, для кражи интеллектуальной собственности	DC02 — например, зашифровать сетевые данные или использовать VPN. AC05, UC06 — только аутентифицированным и авторизованным лицам разрешено участвовать в обмене информацией
Дизайн, планирование	Злоумышленник изменяет передаваемую на завод информацию об определениях продукции, производственных инструкциях или спецификациях испытаний качества через Интернет, например, чтобы нанести ущерб бренду компании, клиентам или производственному оборудованию	DC02 — например, зашифровать сетевые данные или использовать VPN. AC05, UC06 — только аутентифицированным и авторизованным лицам разрешено участвовать в обмене информацией

8 Краткое изложение проблем

8.1 Общие положения

Еще не проведен исчерпывающий анализ угроз для умного производства, основанный на выборе вариантов использования умного производства, процессов жизненного цикла и функций. В 8.2—8.8 представлен краткий обзор основных задач, которые необходимо решить для создания безопасной цифровой производственной системы.

В каждом подразделе собраны проблемы безопасности, выявленные в представлении вариантов использования и жизненного цикла, связанные с основополагающими требованиями безопасности, определенными в *[6]*, как показано в 6.4.

Поскольку на данный момент был оценен лишь ограниченный набор вариантов использования, обзор еще не считается исчерпывающим. Предлагается продолжить эту работу после того, как будет подготовлен согласованный перечень вариантов использования цифрового производства.

8.2 Контроль идентификации и аутентификации (AC)

Идентификация объектов обеспечивает основу кибербезопасности. При безопасном выполнении многих функций (например, обмен данными, предоставление доступа) в основе надлежащей идентификации участвующих сторон лежит идентификация объектов. Цифровое производство зависит от безопасного обмена информацией по всей сети создания ценности. Безопасный обмен информацией требует однозначной, уникальной идентификации и аутентификации участвующих в нем лиц.

Во многих случаях для умного производства требуются защищенные идентификационные данные (определение защищенных идентификационных данных не входит в рамки настоящего стандарта).

Требования к контролю идентификации и аутентификации (AC) приведены в таблице 16.

Таблица 16 — Проблемы контроля идентификации и аутентификации (AC)

ID	Описание
AC01	Аутентификация клиента
AC02	Аутентификация устройств/датчиков
AC03	Аутентификация поставщиков данных моделирования
AC04	Аутентификация поставщиков изменений конфигурации
AC05	Аутентификация участников сети
AC06	Аутентификация лиц, запрашивающих реструктуризацию
AC07	Аутентификация поставщиков для функциональных улучшений
AC08	Невозможность отказа от аудиторской информации. Повышенная гибкость интеллектуального производства (например, временно развернутые производственные системы сторонних производителей и вход в систему и выход из нее) может потребовать повышенного уровня достоверности отслеживаемой информации. Должна быть обеспечена невозможность отказа от информации об отслеживаемости среди различных заинтересованных сторон
AC09	Аутентификация данных датчиков

Несколько вариантов использования цифрового производства зависят от наличия (само)описательной информации о системе. Например, для реализации сценариев «подключи и производи» недавно добавленное устройство должно иметь возможность рекламировать свои возможности, а также находить и исследовать новые возможности в существующей производственной системе. С одной стороны, необходимая информация должна быть легкодоступной, с другой стороны, несанкционированный доступ и модификация информации приводят к ряду угроз безопасности (см. таблицу 17).

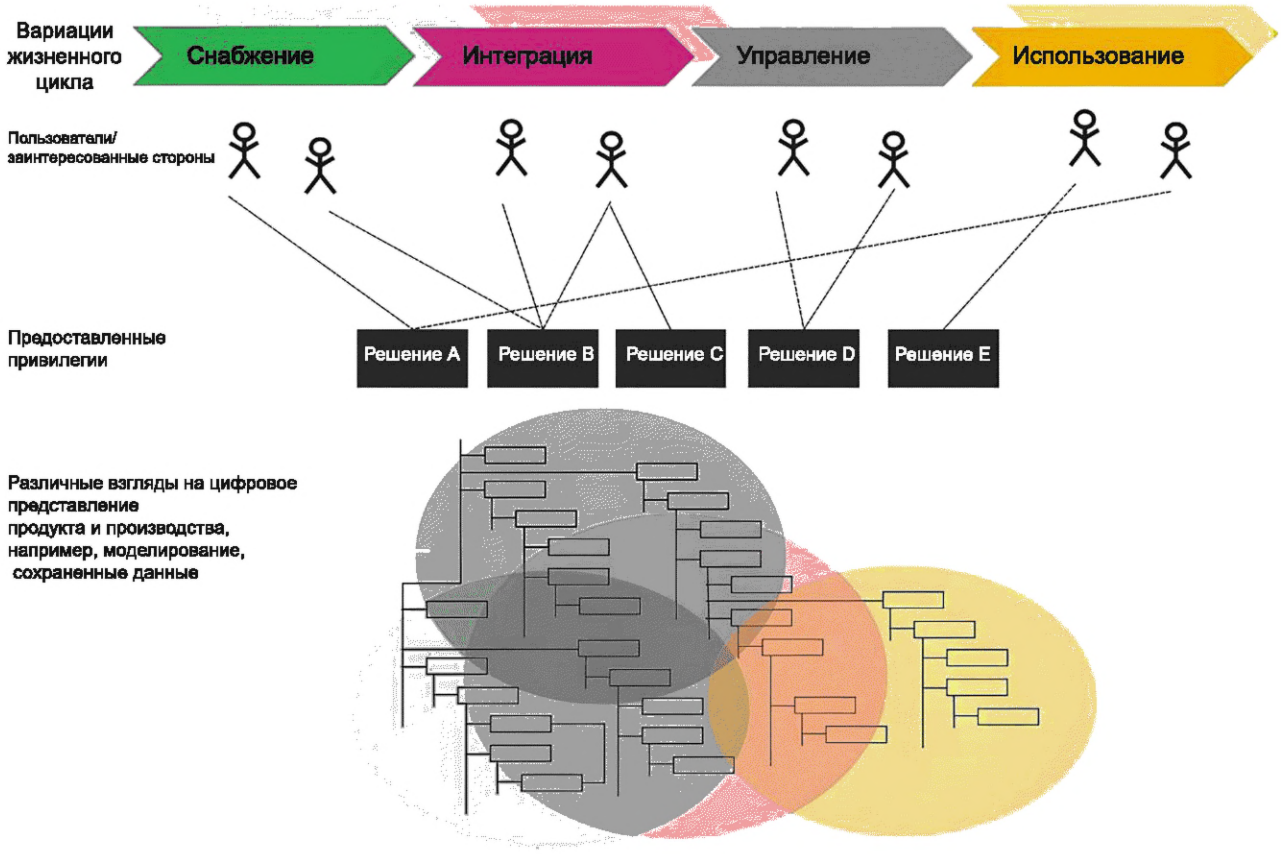

Рисунок 12 — Жизненные циклы, пользователи/заинтересованные стороны, предоставленные привилегии и представления

Как показано на рисунке 12, информация, сопровождающая интеллектуальную производственную систему, обычно сохраняется на нескольких этапах жизненного цикла (например, некоторая информация, первоначально предоставленная поставщиком/производителем устройства, может использоваться интегратором для инженерных задач, во время эксплуатации для задач технического обслуживания и может использоваться для обратной связи с информацией, полученной с помощью конечного продукта). Жизненный цикл существует на разных уровнях абстракции/иерархии (например, устройство автоматизации, продукт для конечного потребителя). Каждый этап жизненного цикла включает в себя взаимодействие различных пользователей/заинтересованных сторон с представлением цифровой производственной системы и артефактами, создаваемыми цифровой производственной системой. Каждому пользователю должны быть предоставлены соответствующие разрешения доступа, необходимые для выполнения текущей задачи. Требования к управлению использованием (UC) приведены в таблице 17.

Таблица 17 — Проблемы с контролем использования (UC)

ID	Описание
UC01	Использование контроля производственного плана
UC02	Использование контроля информации
UC03	Использование контроля имитационной модели
UC04	Использование контроля производственных возможностей
UC05	Использование контроля полевых устройств
UC06	Использование контроля сети
UC07	Использование контроля конфигурации

Дополнительной задачей для умного производства является разработка разумной глобальной политики контроля доступа. Предоставление прав может больше не зависеть только от решения локального администратора, поскольку изменения в локальной системе могут привести к нежелательным побочным эффектам для всей системы в целом благодаря интеллектуальным контурам обратной связи. Это должно быть отражено в процессе управления рисками в соответствии с *[6]*. В качестве первого шага необходимо определить и обеспечить прозрачность в отношении того, какие локальные настройки необходимо перенести в глобальный контекст. Только после того, как это будет обеспечено, можно будет принять решение о локальной политике контроля доступа.

Для организации контроля использования в сложных системах необходим согласованный подход. Существуют различные устоявшиеся парадигмы, такие как управление доступом на основе ролей (RBAC) или атрибутов (ABAC), позволяющие внедрять гибкие и в то же время согласованные политики доступа.

Для определения механизмов контроля доступа в интеллектуальных производственных системах необходимо учитывать следующие моменты:

- необходимость в унифицированном базовом наборе общеизвестных разрешений (например, просмотр, разрешение на чтение ролей, атрибут записи, вызов, ... как указано для OPC UA *[5]*);
- необходимость в унифицированных атрибутах объекта и субъекта, на основе которых строится политика доступа (например, набор хорошо известных ролей);
- начальная настройка управления использованием, например готовое управление доступом для начального уровня доступа с минимальными требованиями к конфигурации самого интеллектуального производственного устройства (например, нецелесообразно настраивать набор пользователей для конкретного завода на устройстве, прежде чем оно сможет подключаться к существующей системе в режиме «подключить-и-производить»). Исходя из этого, конфигурация может быть завершена/расширена;
- универсальный процесс получения разрешений доступа, необходимых для конкретной задачи (например, для начальной загрузки по принципу «Подключи и работай»);
- обеспечение различных уровней контроля доступа (на уровне хоста, на уровне пользователя):
- предоставление базового доступа после аутентификации на уровне хоста;
- предоставление привилегированного доступа после аутентификации на уровне пользователя/приложения;
- разрешение использования и сопоставления между различными удостоверениями (провайдерами удостоверений);
- самоописательное/отражающее представление условий доступа, т. е. ролей, разрешений, ограничений доступа, является неотъемлемой частью информационной модели OPC UA (а также подчиняется механизмам контроля доступа).

8.3 Целостность данных и системы (DI)

Целостность обеих систем и данных, обрабатываемых системами и передаваемых между ними, имеет важное значение. Требования к целостности данных и системы (DI) приведены в таблице 18.

Таблица 18 — Проблемы с целостностью данных и системы (DI)

ID	Описание
DI01	Целостность данных обмена данными
DI02	Целостность данных имитационной модели
DI03	Целостность данных новых функций/конфигураций
DI04	Целостность данных производственных планов
DI05	Целостность данных инженерных данных
DI06	Целостность системы во время переходов
DI07	Автономная базовая защита конечной точки
DI08	Целостность собранных и агрегированных данных датчиков
DI09	Обеспечение подлинности установленных устройств/датчиков

Окончание таблицы 18

ID	Описание
DI10	Целостность (собранных и агрегированных данных датчиков), используемых для обучения и тестирования ML
DI11	Обеспечение подлинности полуфабрикатов и готовых изделий
DI12	Целостность данных относительно известных граничных условий

Примеры использования указывают на следующие проблемы целостности интеллектуальных производственных систем:

- целостность информации, на основе которой изменяется конфигурация или настройка цифровой производственной системы (например, оптимизация) или переносятся производственные планы, очень важна и должна быть подтверждена уполномоченным оператором;
- надежность и целостность данных обратной связи, которыми обмениваются между (неконтролируемой) областью заказчика/потребителя и производственной областью, считается низкой, и данные нуждаются в перепроверке (например, путем сопоставления нескольких наборов данных);
- обеспечение целостности обмениваемых инженерных и проектных данных;
- обеспечение целостности систем моделирования и данных, поступающих в системы моделирования;
- новые функциональные возможности/дополнительные устройства/компоненты проверяются перед установкой, и их ввод в эксплуатацию должен быть подтвержден уполномоченным оператором.

8.4 Конфиденциальность данных (DC)

8.4.1 Общие положения

В умном производстве нужно различать три типа данных/информации.

Данные, которыми необходимо обмениваться между различными заинтересованными сторонами для обеспечения конкретных вариантов использования (например, данные датчиков для интеллектуального анализа данных). Владелец данных намеренно жертвует строгой конфиденциальностью некоторых данных, чтобы получить выгоду от обмена данными с третьей стороной. Однако владелец данных хочет быть уверен, что использование данных ограничено их целевым назначением.

Особый случай касается обработки персональных данных (например, данных конечного клиента, предоставленных посредством обратной связи, и в этом случае применяются правила конфиденциальности).

Как и в случае с классическими производственными системами, существуют также данные, которыми владелец данных не хочет делиться, например, алгоритмический или конструкционный IP-адрес. Особое внимание необходимо уделять тому, чтобы эта информация использовалась в доверительном домене, который не контролируется владельцем информации.

8.4.2 Использование по назначению

Целевое использование относится к надлежащему использованию данных, которые предоставляются с определенной целью для получения всех возможных выгод.

Термин «Конфиденциальность» относится к целевому использованию персональных данных. Граница между фактическими персональными данными и общими данными датчиков различна и может зависеть от контекста. Это проиллюстрировано на рисунке 13.

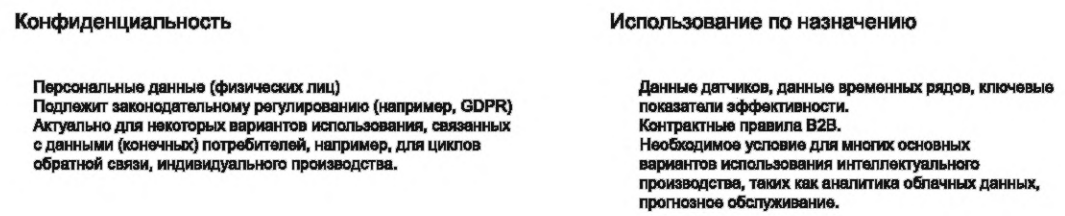

Рисунок 13 — Конфиденциальность и использование по назначению

По возможности следует избегать использования персональных данных в интеллектуальных производственных системах. В случае если речь идет о персональных данных, такие технологии, как псевдонимизация/анонимизация, должны быть максимально закрыты для источника данных, чтобы избежать раскрытия персональных данных. Требования к конфиденциальности данных (DC), касающиеся конфиденциальности, приведены в таблице 19.

Таблица 19 — Проблемы, связанные с конфиденциальностью данных (DC)

ID	Описание
DC01	Конфиденциальность данных клиентов

8.4.3 Конфиденциальность данных

Требования к конфиденциальности данных (DC), отличные от требований к конфиденциальности, приведены в таблице 20.

Таблица 20 — Требования к конфиденциальности данных (DC), отличные от требований к конфиденциальности

ID	Описание
DC02	Конфиденциальность данных в сети
DC03	Конфиденциальность данных имитационной модели
DC04	Конфиденциальность инженерных данных
DC05	Конфиденциальность интеллектуальной собственности продукта
DC06	Конфиденциальность журналов аудита. Информация о трассировке может содержать конфиденциальные данные, которые могут быть использованы злоумышленником для получения информации о слабых сторонах производственной системы. Злоумышленники получают выгоду от извлечения и получения конфиденциальной информации из записей трассировки и узнают о слабых сторонах производственной системы
DC07	Доверенное выполнение
DC08	Конфиденциальность данных датчиков, связанных с сотрудниками/персоналом
DC09	Раскрытие конфиденциальных данных, содержащихся в данных обучения ML
DC10	Конфиденциальность графика производства

8.5 Ограниченный поток данных (RDF)

Требования к ограниченному потоку данных (RDF) приведены в таблице 21.

Таблица 21 — Проблемы с ограниченным потоком данных (RDF)

ID	Описание
RDF01	Необходимый поток данных о клиенте
RDF02	Ограничение потока данных, ориентированного на задачу
RDF03	Ограничение потока/воздействия (сырых) данных датчика
RDF04	Ограничение временной доступности информации, например удаление информации после использования

8.6 Своевременное реагирование на события (TRE)

Отслеживание — это функция, встроенная в производственную систему для отслеживания генеалогии сбоев и атак. В случае инцидента отслеживание позволяет идентифицировать затронутые производственные системы и продукты. Отслеживание является необходимым условием для принятия ответных мер. Это облегчает исправление инцидента и позволяет свести к минимуму последствия отзыва бракованной или пришедшей в негодность продукции.

Что касается безопасности, то отношение к отслеживанию двоякое:

- информация о трассировке предпочтительно предоставляется таким образом, чтобы ее можно было использовать для мониторинга безопасности (например, для получения информации о безопасности и управления событиями) и последующей судебной экспертизы (в случае инцидента);
- информация о безопасности/целостности системы, такая как версия установленных двоичных файлов, исправление для системы безопасности.

Прослеживаемость решает две проблемы:

- какие компоненты/ингредиенты были использованы для создания/производства конкретного продукта (номенклатуры или шихты);
- каковы условия в процессе производства (задействованные системы, данные о качестве, условия хранения, ...).

Отслеживаемость особенно важна в случае, если требуется перезвонить в связи с испорченными/бракованными продуктами. Отслеживаемость позволяет идентифицировать поврежденные продукты и свести к минимуму последствия перезвона. Требования к своевременному реагированию на события (TRE) приведены в таблице 22.

Таблица 22 — Проблемы своевременного реагирования на события (TRE)

ID	Описание
TRE01	Своевременное реагирование на потребление сетевых ресурсов вредоносными объектами
TRE02	Своевременное реагирование, когда система доступна лишь частично
TRE03	Ведение журнала аудита для мониторинга безопасности и криминалистики. Информация о трассировке предпочтительно предоставляется таким образом, чтобы ее можно было использовать для мониторинга безопасности (например, управление информацией о безопасности и событиями) и последующей криминалистики (в случае инцидента)
TRE04	Ведение журнала аудита включает целостность системы и статус исправления. Информация о безопасности/целостности системы, такая как версия установленных двоичных файлов, уровень исправления безопасности, подтверждение целостности системы, собирается и архивируется системой трассировки
TRE05	Защищенная регистрация аудита в случае инцидента. Информация, собранная для отслеживания, может также использоваться для определения воздействия на продукты после инцидента безопасности. Это может потребовать специальных мер защиты для информации отслеживания, чтобы гарантировать ее целостность даже в случае инцидента безопасности (например, удаленное ведение журнала)
TRE06	Обеспечение объяснимости предложений/инструкций системы ML

8.7 Доступность ресурсов (RA)

Требования к доступности ресурсов (RA) приведены в таблице 23.

Таблица 23 — Проблемы с доступностью ресурсов (RA)

ID	Описание
RA01	Доступность текущих данных моделирования
RA02	Доступность сетевых ресурсов
RA03	Восстановление ресурсов после блокировки
RA04	Доступность беспроводного сервиса
RA05	Доступность датчиков и мониторинга
RA06	Доступность журналов аудита. Следует убедиться, что все стороны, затронутые потенциальным спором, могут получить доступ к данным трассировки; в случае использования расширенных механизмов безопасности (например, цифровых подписей) необходимо, чтобы вся информация, требуемая для проверки данных трассировки (например, цифровые удостоверения, сертификаты), была доступна при необходимости

Внедрение безопасности в систему влияет на ее доступность. В частности, наличие необходимых учетных данных безопасности для защиты и доступа к долговечным киберфизическим артефактам (например, цифровым двойникам) на протяжении всего их жизненного цикла требует особого рассмотрения и дальнейшей работы.

Приложение ДА
(информационное)

Сведения о соответствии ссылочных национальных стандартов международным стандартам, использованным в качестве ссылочных в примененном международном документе

Таблица ДА.1

Обозначение ссылочного национального стандарта	Степень соответствия	Обозначение и наименование ссылочного международного стандарта
ГОСТ Р 56205—2014/ IEC/TS 62443-1-1:2009	IDT	IEC/TS 62443-1-1:2009 «Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 1-1. Терминология, концептуальные положения и модели»
ГОСТ Р МЭК 62443-2-1—2015	IDT	IEC 62443-2-1:2010 «Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 2-1. Составление программы обеспечения защищенности (кибербезопасности) системы управления и промышленной автоматики»

Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов:

- IDT — идентичные стандарты.

Приложение ДБ
(справочное)

Сопоставление структуры настоящего стандарта со структурой примененного в нем международного документа

Таблица ДБ.1

Структура настоящего стандарта	Структура международного документа IEC/TR 63283-3:2022
1 Область применения	1 Область применения
2 Нормативные ссылки	2 Нормативные ссылки
3 Термины, определения и сокращения	3 Термины, определения, сокращения и аббревиатуры
4 Задачи кибербезопасности в цифровом производстве	4 Задачи кибербезопасности в цифровом производстве
5 Системная инженерия	5 Системная инженерия
6 Применение серии стандартов МЭК 62443 [6] к цифровому производству	6 Применение IEC 62443 (все части) к цифровому производству
7 Угрозы безопасности цифрового производства	7 Угрозы безопасности в области цифрового производства
8 Краткое изложение проблем	8 Краткое изложение проблем
Приложение ДА Сведения о соответствии ссылочных национальных стандартов международным стандартам, использованным в качестве ссылочных в примененном международном документе	Приложение А Приведение вариантов использования в соответствие с основополагающими требованиями
Приложение ДБ Сопоставление структуры настоящего стандарта со структурой примененного в нем международного документа	Приложение В Защищенные идентификационные данные
Библиография	Библиография

Библиография

[1]	ИСО/МЭК 30141:2024	Интернет вещей. Типовая архитектура (Internet of Things (IoT) Reference architecture)
[2]	ISO/IEC TR 30166:2020	Интернет вещей (IoT). Промышленный IoT (Internet of things (IoT) — Industrial IoT)
[3]	МЭК 62264 (все части)	Интеграция системы управления предприятием (Enterprise-control system integration)
[4]	МЭК 61512 (все части)	Управление периодическими (серийными) технологическими процессами (Batch control)
[5]	ISO/IEC/IEEE 15288:2023	Системная и программная инженерия. Процессы жизненного цикла системы (Systems and software engineering System life cycle processes)
[6]	МЭК 62443 (все части)	Безопасность систем промышленной автоматизации и управления (Security for industrial automation and control systems)
[7]	IEC/TS 62443-1-1:2009	Сети коммуникационные производственные. Безопасность сети и систем. Часть 1-1. Терминология, понятия и модели (Industrial communication networks — Network and system security — Part 1-1: Terminology, concepts and models)
[8]	МЭК 62443-2-1:2024	Безопасность систем промышленной автоматизации и управления (IACS). Часть 2-1. Требования к программе обеспечения безопасности для владельцев активов IACS (Security for industrial automation and control systems — Part 2-1: Security program requirements for IACS asset owners)
[9]	IEC/TR 62443-2-3:2015	Безопасность систем промышленной автоматизации управления. Часть 2-3. Управление внесением исправлений в среде IACS (Security for industrial automation and control systems — Part 2-3: Patch management in the IACS environment)
[10]	МЭК 62443-2-4:2023	Безопасность систем промышленной автоматизации и управления. Часть 2-4. Требования к программе обеспечения безопасности для поставщиков услуг IACS (Security for industrial automation and control systems — Part 2-4: Security program requirements for IACS service providers)
[11]	IEC/TR 62443-3-1:2009	Сети коммуникационные производственные. Безопасность сети и систем. Часть 3-1. Методы обеспечения безопасности для производственных систем автоматизации и управления (Industrial communication networks — Network and system security — Part 3-1: Security technologies for industrial automation and control systems)
[12]	МЭК 62443-3-2:2020	Безопасность промышленных систем автоматизации и управления. Часть 3-2. Оценка рисков, связанных с защитой, при проектировании систем (Security for industrial automation and control systems — Part 3-2: Security risk assessment for system design)
[13]	МЭК 62443-3-3:2013	Сети промышленной коммуникации. Безопасность сетей и систем. Часть 3-3. Требования к системной безопасности и уровни безопасности (Industrial communication networks — Network and system security — Part 3-3: System security requirements and security levels)
[14]	МЭК 62443-4-1:2018	Безопасность систем промышленной автоматизации и управления. Часть 4-1. Требования к жизненному циклу безопасной разработки (SDL) продуктов (Security for industrial automation and control systems — Part 4-1: Secure product development lifecycle requirements)
[15]	МЭК 62443-4-2:2019	Безопасность систем промышленной автоматизации и управления. Часть 4-2. Технические требования к безопасности компонентов IACS (Security for industrial automation and control systems — Part 4-2: Technical security requirements for IACS components)

[16]	IEC/TR 63283-1:2022	Измерение, управление и автоматизация промышленного процесса. Умное производство. Часть 1. Термины и определения (Industrial-process measurement, control and automation — Smart manufacturing — Part 1: Terms and definitions)
[17]	IEC/TR 63283-2:2022	Измерение, управление и автоматизация промышленного процесса. Умное производство. Часть 2. Варианты использования (Industrial-process measurement, control and automation — Smart Manufacturing — Part 2: Use cases)

УДК 004.85:006.354 ОКС 35.240.99

Ключевые слова: цифровая промышленность, цифровое производство, умное производство, кибербезопасность

Редактор *Л.В. Коретникова*
Технический редактор *И.Е. Черепкова*
Корректор *О.В. Лазарева*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 10.01.2025. Подписано в печать 05.02.2025. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 6,05. Уч.-изд. л. 5,02.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении в ФГБУ «Институт стандартизации»
для комплектования Федерального информационного фонда стандартов,
117418 Москва, Нахимовский пр-т, д. 31, к. 2.

gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru