Pilz GmbH & Co. KG
Felix-Wankel-Straße 2
73760, Остфильдерн,
Германия
Германия
www.pilz.com

Защита для компаний, машин и продукции

Функциональная и информационная безопасность — Комплексный подход

Остфильдерн, октябрь 2025 г. — **Происшествия в сфере информационной безопасности уже затрагивают не только ИТ-системы, но и все чаще — производственную среду (ОТ). Инциденты в области информационной безопасности в промышленности включают в себя не только направленные атаки, но и непреднамеренные манипуляции. Миссия информационной безопасности в промышленности — гарантировать эксплуатационную готовность установок и машинного оборудования, а также достоверность и конфиденциальность их данных и процессов. Однако первоочередной целью защиты является функциональная безопасность. Ведь в конечном итоге, если компании не обладают суверенитетом над своими данными, то под угрозой оказываются и сама компания и безопасность ее сотрудников, — без информационной безопасности нет безопасности машин, а без безопасности машин не защищены люди!**

В ЕС признали растущую угрозу и соответствующим образом адаптировали законодательство: на уровне компаний **Директива NIS 2** требует принятия мер для обеспечения высокого общего уровня кибербезопасности в рамках Союза, например, с помощью систем управления информационной безопасностью.

Машинный регламент 2023/1230 теперь предусматривает защиту от манипуляций для установок и машинного оборудования и требует принятия мер информационной

безопасности в промышленности в отношении компонентов машин, влияющих на функциональную безопасность.

Закон о киберустойчивости (CRA) требует принятия мер информационной безопасности в отношении изделий, в состав которых входят цифровые элементы. К ним относятся системы управления, системы ввода-вывода и другие компоненты, используемые в машинном оборудовании.

Компании, машинное оборудование и продукция — на каждом уровне производители машин и операторы сталкиваются с различными проблемами и нормативно-правовыми базами.

Современная система информационной безопасности

Независимо от того, что законодательство делает информационную безопасность в промышленности обязательной, существует ряд веских причин заняться этим вопросом заранее и получить консультацию. Рутинные процессы и условия эксплуатации машинного оборудования могут подвергаться риску несанкционированных манипуляций, если их не проверять регулярно. Например, длительный срок службы машинного оборудования часто приводит к тому, что соответствующие системы устаревают и в какой-то момент перестают соответствовать современным стандартам информационной безопасности. В этих системах имеются бреши в защите данных, которые уже невозможно закрыть, поскольку поставщик прекратил предоставлять обновления в области информационной безопасности. Зачастую защиту от вредоносного ПО невозможно реализовать на конечных устройствах, поскольку некоторые из них слишком устарели, и в результате их производительность снизится, что потенциально может привести к простоям производства.

Повышение уровня информационной безопасности в промышленности, шаг за шагом

В конечном счете, цель состоит в том, чтобы обеспечить защиту хозяйственной деятельности, но для этого компаниям необходимо преодолевать различные трудности: от изучения действующих законодательных требований и обнаружения и устранения уязвимостей в системах до повышения осведомленности и обучения сотрудников, а также последующего обеспечения контроля. Поскольку безопасность — это «движущаяся цель», также необходима регулярная проверка состояния машинного оборудования с точки зрения информационной безопасности. Важно, чтобы в компании были четко определены обязанности, и применялся системный подход, предусматривающий накопление необходимых профессиональных знаний и опыта.

Компания по автоматизации Pilz подготовилась к этим требованиям и разработала индивидуализированный портфель услуг для производителей машин и пользователей по всему миру, который комплексно включает в себя все аспекты защиты человека и машины. Специалисты компании Pilz осведомлены о современных требованиях законодательства и стандартизации и учитывают их в своих рекомендациях. В предложение также входит обучение, позволяющее компаниям расширить или актуализировать свои знания в области информационной безопасности. В практической реализации также используются решения компании Pilz, такие как система идентификации и управления доступом (I.A.M.) для повышения уровня функциональной и информационной безопасности.

Закладка надежного фундамента

Чтобы гарантировать информационную безопасность своего оборудования, специалистам в области машиностроения необходимы глубокие фундаментальные знания, в частности, знание законодательства и применимых стандартов. Эксперты компании Pilz делятся этим опытом в рамках учебного курса «Основы информационной безопасности в промышленности». Слушатели курса изучают угрозы информационной безопасности, надлежащие меры защиты и передовой опыт в контексте информационной безопасности машинного оборудования и сетей. Таким образом, даже новички в области информационной безопасности могут узнать о мерах, которые можно предпринять для эффективной защиты машинного оборудования от кибератак и манипуляций на этапе его производства.

Квалификация «CESA — Сертифицированный эксперт в области информационной безопасности в автоматизации» — компания Pilz предлагает двухдневный экспертный курс, который дает участникам углубленные знания в сфере информационной безопасности в соответствии с актуальными стандартами, в частности, с серией стандартов IEC 62443 (»Промышленные коммуникационные сети. ИТ-безопасность сетей и систем»). Кроме того, обучение охватывает практические меры по снижению рисков, такие как контроль доступа, повышение безопасности сети с использованием технических средств и организационных мер для предотвращения рисков в отношении защиты данных. Участники учатся правильно применять стандарт и демонстрировать соответствие своих систем автоматизации требованиям кибербезопасности. После сдачи экзамена участники получают признанный во всем мире

сертификат TÜV NORD «CESA — Сертифицированный эксперт в области информационной безопасности в автоматизации».

Применение теории на практике

С опорой на теоретические основы и обучение, следующим шагом в укреплении информационной безопасности в промышленности является применение структурированных практических процессов. Консалтинг в области эксплуатационных технологий (OT) позволяет преодолеть разрыв между теоретической базой и стратегиями, подлежащими реализации. Используя пошаговый подход, службы, ответственные за информационную безопасность в промышленности, выявляют уязвимости в сложных системах и разрабатывают меры по минимизации риска. В результате мы получаем всеобъемлющую концепцию безопасности.

Четыре шага к повышению уровня информационной безопасности в промышленности

Процесс обеспечения информационной безопасности в эксплуатационных технологиях состоит из четырех этапов: «Анализ требований к защите», «Оценка рисков информационной безопасности в промышленности», «Концепция информационной безопасности в промышленности» и «Проверка системы информационной безопасности в промышленности».

В ходе анализа требований к защите компания определяет требования к защите отдельных «активов» установки или машины, а также цели их защиты. Второй шаг — это оценка рисков, при которой рассматриваются все риски вместе с вероятностью их возникновения для каждой подсистемы на протяжении всего жизненного цикла оборудования. Следующий

шаг — создание подробной концепции информационной безопасности в промышленности со стратегиями и мерами по предотвращению и снижению рисков, вызванных атаками, манипуляциями и ошибками операторов. Кроме того, создаются политики, правила и инструкции для поддержания безопасной эксплуатации или структуры системы. На последнем этапе — проверка системы информационной безопасности в промышленности — проверяется эффективность реализованных контрмер.

Гарантия эксплуатационной готовности машинного оборудования

Процесс оказания услуг по обеспечению информационной безопасности в промышленности помогает смягчить или предотвратить кибератаки. Количество нарушений информационной безопасности, спровоцированных непреднамеренно, также снижается. Это, в свою очередь, повышает эксплуатационную готовность машинного оборудования и, в конечном счете, обеспечивает экономию средств при сохранении экономической эффективности.

Такой подход в первую очередь защищает людей, работающих с оборудованием, и применяются соответствующие меры информационной безопасности. Ведь следует помнить, что нарушение информационной безопасности может препятствовать мерам функциональной безопасности. Например, световая завеса перед машинным оборудованием гарантирует, что операторы не попадут в опасную зону. Но если злоумышленник сможет повлиять на соответствующий контроллер и механизм, защитная функция световой завесы

больше не может быть гарантирована. Защита данных обеспечивает безопасность машин!

Поэтому в контексте фактического внедрения на машинном оборудовании, функциональную и информационную безопасность имеет смысл рассматривать вместе. Ведь без защиты данных не добиться безопасности машин, а без этого люди не защищены!

Четкое регулирование: кто имеет право эксплуатировать оборудование, и как именно?

Безопасность машины и ее операторов зависит от контроля доступа — будь то люди или сеть. Точки входа должны быть защищены от несанкционированного доступа, чтобы никто не находился в опасной зоне, например, во время работы машины. Даже если эксплуатация или техническое обслуживание установки ведутся с благими намерениями — будь то на площадке или через сеть — это может иметь фатальные последствия.

Идентификация и управление доступом (I.A.M.) является важным элементом, который четко регулирует разрешения и доступ к установкам и оборудованию в компаниях. Сюда относятся организационные меры и технические требования, а также соответствующие функции информационной и функциональной безопасности. Система разрешений доступа, такая как PITreader от Pilz, представляет собой надлежащий продуктовый компонент. Это означает, что пользователи могут удовлетворить требования в отношении защиты сотрудников, защиты ответственности, максимальной производительности и защиты данных.

Только комплексный подход к функциональной и информационной безопасности гарантирует всеобъемлющую защиту человека и машины. Компания больше не вправе решать, хочет ли она обеспечивать информационную безопасность и в какой степени. Это теперь является юридическим требованием. В инжиниринге информационная безопасность в промышленности является не только задачей отдела информационных технологий, но и неотъемлемой частью проектирования и строительства. Ретроспективная реализация защиты данных сложна и обычно означает снижение удобства для пользователя, функциональности и производительности.

((Количество знаков: 9 784))

((Блок:))

Обзор законодательства ЕС в сфере информационной безопасности

В частности, в Европе законодатели отреагировали на уровень угрозы принятием ряда законов. В результате в Европе действуют самые строгие требования в мире. Но уже существуют договоренности с другими странами, и там такие законы тоже будут приняты. Поэтому следует ожидать глобальной гармонизации информационной безопасности.

NIS 2: Больше обязательств для компаний

NIS (сетевая и информационная безопасность) – это директива Европейского союза, направленная на укрепление кибербезопасности. Эта директива существует с 2016 года и до

сих пор применялась к поставщикам критически важной инфраструктуры, включая энергетику, транспорт, банки и финансы, здравоохранение, снабжение и распределение питьевой воды и цифровую инфраструктуру. Поставщики в этих секторах должны были внедрить «соответствующие меры информационной безопасности» и сообщать о любых серьезных инцидентах, связанных с кибербезопасностью. Новая директива NIS 2 ((EU) 2022/2555 ... о мерах по обеспечению высокого общего уровня кибербезопасности на территории Союза) требует от значительно большего количества компаний принятия мер по управлению рисками кибербезопасности в будущем. NIS 2 расширяет секторы, добавляя, например, производство и реализацию промышленных товаров и товаров производственного назначения, включая машиностроение и производителей электрооборудования.

Требования включают анализ рисков и концепции безопасности информационных систем, защиту цепочки поставок и безопасность персонала. Концепции контроля доступа и управления установками являются еще одним требованием, наряду с обязательным обучением руководителей.

Директива была принята в конце 2022 года Европейским парламентом и Советом ЕС. Как и все директивы ЕС, NIS 2 не вступает в силу немедленно и не имеет обязательной силы в отдельных государствах-членах ЕС, но должна быть включена во внутреннее законодательство стран-членов. Компаниям было бы целесообразно заняться NIS 2 как можно скорее и провести комплексную оценку информационной безопасности компании. Например, сюда входит разработка Системы управления информационной безопасностью (ISMS). В этом контексте

полезной является сертификация по стандарту информационной безопасности ISO 27001.

NIS 2 на примере ветряных турбин: С NIS 2 производители оборудования, такие как производители электростанций (например, ветряных турбин), также должны будут соответствовать требованиям в будущем. В свою очередь производителям ветряных турбин нужны решения по автоматизации, контроллеры или датчики. Начиная с определенного размера, производители электрических компонентов также подпадают под NIS 2. А поскольку NIS 2 также предусматривает, что поставщики принимаются во внимание, такая компания, как Pilz, также должна заботиться о безопасности цепочек поставок и предъявлять требования к своим поставщикам. Таким образом, NIS 2 охватывает всю цепочку поставок.

Новый Машинный регламент: нет информационной безопасности — нет маркировки CE

Машинная директива 2006/42/EC имеет особое значение с точки зрения функциональной безопасности машин.

Для ввоза техники в Европу машиностроителям всегда приходилось проходить соответствующую процедуру оценки соответствия, завершающуюся получением маркировки CE.

Технические требования, переизданные в июне 2023 года в виде Машинного регламента, были обновлены в соответствии с уровнем новейших достижений науки и техники. Поскольку это регламент, его не требуется сначала преобразовывать в национальный закон. У производителей машин есть время до 20

января 2027 года, чтобы адаптироваться к новым требованиям и обеспечить соответствие им с ключевой даты.

Машинный регламент заменяет существующую Машинную директиву и, в отличие от нее, делает меры по кибербезопасности обязательными. Если Машинная директива рассматривала исключительно функциональную безопасность, Регламент добавляет целью обеспечение информационной безопасности в рамках «Основных требований по охране труда и технике безопасности (EHSR)», раздел «Защита от злоупотреблений»: функции безопасности машинного оборудования не должны нарушаться в результате непреднамеренного или преднамеренного вмешательства.

Этот новый путь к маркировке CE поднимает ряд новых проблем для производителей и операторов машин, поскольку им придется пересмотреть существующие концепции промышленной и информационной безопасности.

Закон о киберустойчивости — информационная безопасность на протяжении всего жизненного цикла продукта

Помимо проверки компании и оборудования абсолютно необходимо также реализовать меры информационной безопасности непосредственно в устройствах (например, в контроллерах). В сентябре 2022 г. Европейская комиссия представила проект постановления, направленного на повышение кибербезопасности продуктов. Этот Закон об устойчивости к угрозам кибербезопасности (CRA) направлен на производителей изделий с цифровыми элементами (аппаратное

и программное обеспечение), которые способны взаимодействовать с другими изделиями. Это затрагивает продукты из сегмента B2C, такие как смартфоны или роботы-пылесосы, а также продукты из сегмента B2B, такие как контроллеры и датчики, а также чисто программные продукты, такие как операционные системы или сами машины.

Обязанности производителей оборудования по информированию об обнаруженных уязвимостях вступают в силу с 11.09.2026. Изделия, в состав которых входят цифровые элементы, должны соответствовать требованиям CRA с 11.12.2027, чтобы иметь право находиться на рынке ЕС. CRA — это регламент ЕС, и поэтому он незамедлительно вступит в силу в странах-членах ЕС.

Насколько велико будет влияние Закона о киберустойчивости на самом деле, зависит от критериев, которые в конечном итоге будут установлены для классификации продуктов. В соответствии с Законом о киберустойчивости на рынке могут размещаться только продукты, гарантирующие надлежащий уровень кибербезопасности — и это на протяжении всего жизненного цикла продукта. Таким образом, информационная безопасность начинается с разработки продукта. Вот почему в течение нескольких лет компания Pilz также согласовывала свои процессы разработки со стандартом IEC 62443-4-1 «Информационная безопасность систем промышленной автоматизации и управления. Часть 4-1. Требования к защите жизненного цикла разработки изделий», и разработала, например, SecurityBridge, чтобы продемонстрировать свою приверженность информационной безопасности.

((Количество знаков: 6 062))

Pilz — Дух безопасности

Компания Pilz является мировым поставщиком изделий, систем и услуг в области автоматизации. Будучи флагманом в области безопасной автоматизации, компания Pilz обеспечивает безопасность для человека, оборудования и окружающей среды. Основанная в 1948 году, сегодня семейная компания с головным офисом в Остфильдерне — это 2500 сотрудников в 42 дочерних компаниях и филиалах.

Компания-технологический лидер предлагает комплексные решения по автоматизации для обеспечения промышленной и информационной безопасности машинного оборудования. Сюда входят датчики, системы управления и приводная техника, а также устройства для промышленной связи, диагностики и визуализации. В международный спектр услуг также входят консультирование, инжиниринг и обучение. Помимо машиностроения, решения Pilz используются во многих отраслях, например, во внутренней логистике, упаковочной промышленности и на железнодорожном транспорте, или в робототехнике.

www.pilz.com

Компания Pilz в социальных сетях:

На наших каналах в социальных сетях мы предоставляем справочную информацию о компании и людях, которые работают в Pilz, а также информируем о последних новостях из области автоматизации.

www.pilz.com/facebook
www.pilz.com/xing
www.pilz.com/youtube
www.pilz.com/linkedin

Контактные лица для прессы:

Мартин Курт
Корпоративная и техническая пресса
Тел.: +49 711 3409-158
m.kurth@pilz.de

Сабина Каррер
Техническая и корпоративная пресса
Тел.: +49 711 3409-7009
s.skaletz-karrer@pilz.de

Дженни Скарман
Техническая пресса
Телефон: +49 711 3409-1067
j.skarman@pilz.de

Ева Гельнер-Рёссле
Техническая пресса
Тел.: +49 711 3409-7147
e.roessle@pilz.de