kaspersky

Основы промышленной кибербезопасности

Тренинги с инструктором

О чем

Очные курсы, предназначенные для слушателей разного уровня подготовки, знакомят с основами кибербезопасности на промышленных предприятиях и дают ориентированные на практику знания по различным аспектам защиты промышленной инфраструктуры.

Зачем

В зависимости от задач слушателя курсы дают общее представление о промышленной кибербезопасности или позволяют приобрести или обогатить знания и навыки для решения конкретных задач по обеспечению кибербезопасности предприятия.

Для кого

Специалисты по ИТ и информационной безопасности, OT-инженеры и операторы, менеджеры среднего звена и руководители.

Проблематика

Промышленная кибербезопасность – это специализированная дисциплина, ориентированная на защиту промышленных систем управления (АСУ ТП), которые управляют критической инфраструктурой и производственными процессами. Ее основное отличие от безопасности информационных систем состоит в обеспечении непрерывности процессов и предотвращении физических последствий кибератак.

Среды АСУ ТП чувствительны к нарушениям доступности и целостности: даже незначительное вмешательство может привести к каскадным физическим сбоям, рискам для безопасности или длительным простоям.

Первостепенной линией защиты является безопасность промышленных сетей. Тренинг охватывает стадии проектирования, модернизации и защиты технологических сетей, а также учитывает специфические аспекты OT, такие как использование специализированных сетевых протоколов. Уделяется внимание задачам поддержания доступности оборудования, предотвращению несанкционированного доступа к оборудованию АСУ ТП и противоаварийной защиты, сохранению целостности программного обеспечения устройств.

В дополнение к техническим мерам необходимы организационные меры. К ним относятся разработка политик безопасности, планов реагирования на инциденты, адаптированных к процессам и технологиям, комплексные программы обучения для формирования культуры осведомленности о

безопасности среди имеющего отношение к ОТ персонала, в частности у инженеров, операторов и менеджеров.

Понимание специфики атак на промышленные системы имеет фундаментальное значение для построения эффективной защиты. Целью кибератаки может быть манипулирование значениями уставок, отключение систем безопасности или подделка сигналов управления, что может привести к повреждению оборудования, остановке процессов или нанесению вреда жизни и здоровью людей. Стратегии защиты разрабатываются таким образом, чтобы обнаруживать и предотвращать соответствующие векторы атак.

В ходе тренинга инструкторы рассказывают, как происходит атака, почему обычные средства противоаварийной защиты могут не помочь противодействовать ей. Также учат понимать, как наиболее эффективно можно противостоять различным атакам, как использовать меры и средства защиты, как выбирать и настраивать решения кибербезопасности и обеспечивать культуру кибербезопасности на предприятии, чтобы добиться наилучших результатов и получить уверенность в должной защите промышленной среды.

Что мы предлагаем

Очные курсы с инструктором – от трехчасового интенсива до углубленной однодневной программы.

Базовый курс «Кибербезопасность современных промышленных систем»

Курс дает основы информационной безопасности на промышленных предприятиях, учит понимать суть инцидентов безопасности и подходов к реагированию, а также правилам безопасного поведения в ежедневной работе.

Программа курса

1. Особенности обеспечения безопасности промышленных систем, архитектура промышленных сетей, классификация основных угроз для АСУ ТП, уязвимости, эксплойты, атаки.
2. Обзор ландшафта угроз для промышленных предприятий, проблемы безопасности, влияние человеческого фактора, атаки на промышленные сети.
3. Типы злоумышленников.
4. Политики и процедуры безопасности.
5. Основы реагирования на инциденты безопасности.
6. Методы социальной инженерии.

Продолжительность: 1 день

Численность группы: 10–25 человек

Основной курс «Промышленная безопасность»

Курс знакомит с основными мерами и рекомендациями по применению механизмов безопасности в промышленных системах, рекомендациями по организации команды кибербезопасности на предприятии, позволяет участникам узнать о различных аспектах кибербезопасности АСУ ТП, таких как выявление инцидентов безопасности, разработка и внедрение эффективного плана реагирования, реализация контрмер (сегментация сети, использование межсетевого экрана, защита изолированной сети) и расследование инцидентов. В процессе обучения проводится разбор реальных примеров расследований инцидентов в АСУ ТП и дается специфика атак на промышленные организации.

Программа курса

1. Обзор ландшафта угроз для промышленных предприятий, проблемы безопасности, влияние человеческого фактора, примеры атак на промышленные сети.
2. Типы злоумышленников.
3. Отличия в защите ИТ- и промышленных сетей.
4. Концепция эшелонированной защиты.
5. Сетевая безопасность в ИТ- и в промышленных сетях.
6. Промышленные сетевые протоколы.
7. Методы предотвращения и детектирования угроз, снижения рисков реализации угроз.
8. Соответствие защищаемых промышленных систем требованиям стандартов и законодательства.
9. Структура команды информационной безопасности, описание ролей.
10. Соображения безопасности при работе с поставщиками.
11. Безопасность изолированных сетей.
12. Подход к реагированию на инциденты кибербезопасности.
13. Влияние развития промышленного интернета вещей на кибербезопасность.

Продолжительность: 1 день

Численность группы: 10–25 человек

Экспресс-курс «Промышленная безопасность»

Курс знакомит с основными понятиями кибербезопасности (атаки, злоумышленники, угрозы, уязвимости и т. д.), понятием ландшафта современных киберугроз и подходами к предотвращению и расследованию инцидентов, учит понимать отличия между безопасностью

в ИТ и АСУ ТП, дает основы правового регулирования в сфере информационной безопасности.

Программа курса

1. Знакомство с основными проблемами кибербезопасности в промышленных средах.
2. Основные отличия между безопасностью в промышленных сетях и информационных сетях.
3. Организация и управление эффективной командой по информационной безопасности на предприятиях.
4. Соответствие защищаемых промышленных систем требованиям стандартов и регулирующих актов в области информационной безопасности.

Продолжительность: 3 часа

Численность группы: 5–10 человек

Требования к слушателям

Курсы адаптируются в соответствии с составом участников каждой группы.

Сертификация

Участникам выдается сертификат о прохождении курса.

Наши инструкторы

Екатерина Рудина, руководитель группы аналитиков по информационной безопасности «Лаборатории Касперского»

Специализируется на исследовании угроз, моделировании и оценке рисков. Имеет 12-летний опыт работы в области промышленной кибербезопасности. Эксперт по нормативной документации (стандарты, законы, руководства, требования и т. д.), связанной с защитой критически важных организаций. Автор документов, разработанных под эгидой Международной организации по стандартизации (ISO), Института инженеров электротехники и электроники (IEEE), Международного союза электросвязи (ITU) и Международного консорциума промышленного интернета (IIC, теперь Digital Twin Consortium), а также национальных стандартов по конструктивной безопасности. Кандидат технических наук.

Семен Корт, ведущий аналитик по информационной безопасности «Лаборатории Касперского»

Специализируется на промышленной кибербезопасности и безопасности интернета вещей. Автор стандартов информационной безопасности и постоянный участник рабочих групп международных организаций по стандартизации, а также Международного консорциума промышленного интернета (IIC, теперь Digital Twin Consortium). Основной автор курса по повышению осведомленности в области промышленной кибербезопасности, преподающий его в компаниях по всему миру. Кандидат технических наук.

Александр Николаев, старший аналитик по информационной безопасности «Лаборатории Касперского»

Специализируется на создании моделей угроз, анализе рисков и разработке архитектур кибербезопасности для промышленных систем управления. Имеет 15-летний опыт работы в области промышленной кибербезопасности (в нефтегазовом, сельскохозяйственном и банковском секторах, а также в судоходстве и авиации). Участник рабочей группы Авиарегистра РФ по разработке документов по кибербезопасности авиационной отрасли на базе Государственного научно-исследовательского института авиационных систем (ГосНИИ АС).

Денис Бабаев, ведущий аналитик по информационной безопасности «Лаборатории Касперского»

Специализируется на моделировании угроз, оценке рисков и проектировании архитектур кибербезопасности для промышленных систем управления преимущественно для атомных и теплоэлектростанций. Имеет более чем 20-летний опыт работы в инжиниринге киберфизических систем, а также в кибербезопасности. Участник технических комитетов Международной электротехнической комиссии (IEC).

Рекомендуем дополнительно

- Цифровая криминалистика и расследование инцидентов в АСУ ТП
- Самостоятельное обучение на онлайн-платформе Kaspersky Automated Security Awareness

Запросить консультацию специалиста

Центр реагирования на инциденты информационной безопасности промышленных инфраструктур «Лаборатории Касперского» (Kaspersky ICS CERT) — глобальный проект «Лаборатории Касперского», направленный на координацию усилий производителей систем автоматизации, владельцев и операторов промышленных объектов, а также исследователей ИТ-безопасности для защиты промышленных предприятий от кибератак. Kaspersky ICS CERT направляет свои усилия в первую очередь на выявление потенциальных и существующих угроз, нацеленных на системы промышленной автоматизации и промышленный интернет вещей.

Kaspersky ICS CERT ics-cert@kaspersky.com