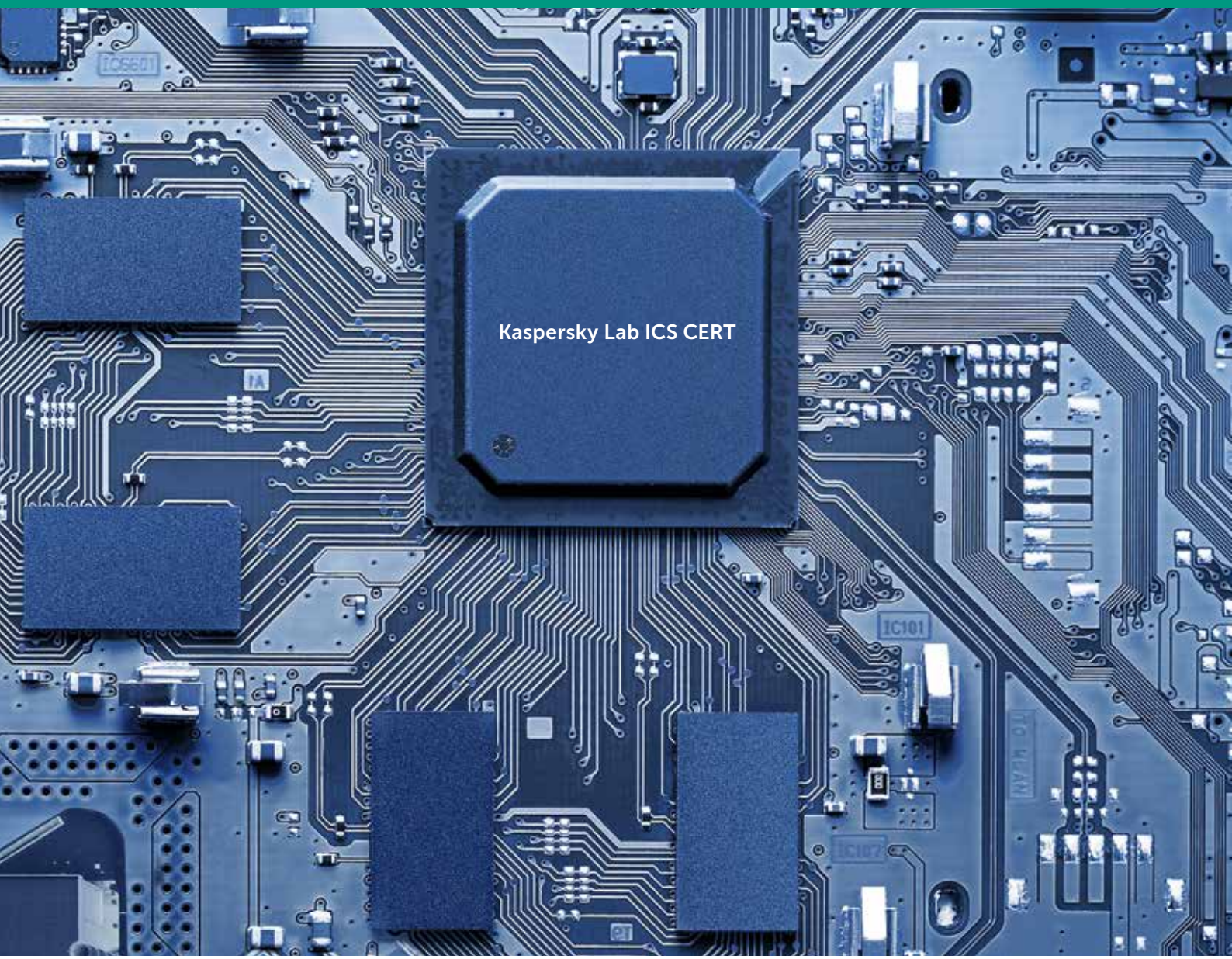


Программа тренингов «Лаборатории Касперского» по промышленной кибербезопасности

Курсы, предлагаемые в 2019 г.

Содержание

Введение

«Лаборатория Касперского» предлагает курсы по повышению осведомленности в области информационной безопасности промышленных предприятий на основе результатов новейших исследований.

Цель нашей программы обучения по кибербезопасности систем промышленной автоматизации – дать возможность специалистам в области информационных технологий (ИТ), автоматизированных систем управления технологическим процессом (АСУ ТП) и информационной безопасности (ИБ), а также руководителям и другим сотрудникам предприятий повысить уровень своих знаний в области промышленной кибербезопасности..

Наши тренеры и партнеры – эксперты в области АСУ ТП

- высоко мотивированы
- дают глубокие знания
- используют гибкий подход
- используют индивидуальный подход

Основные преимущества тренингов

- Изменение поведения – способствует формированию у каждого сотрудника безопасного и ответственного подхода к работе; помогает построить корпоративную среду, основанную на принципе «я, как и все, забочусь о кибербезопасности – это часть моей работы».
- Использование мотивационного подхода, геймификации, различных методов обучения, моделирования атак на основе реальных ситуаций на промышленных предприятиях, интерактивной тренировки навыков кибербезопасности.
- Помощь в повышении экспертного уровня вашей организации. Тренинги позволяют организациям повысить уровень знаний в области кибербезопасности по четырем основным направлениям:
  - Базовые знания в области кибербезопасности систем промышленной автоматизации (АСУ ТП)
  - Тестирование на проникновение АСУ ТП
  - Цифровая криминалистика для АСУ ТП
  - Кибербезопасность интернета вещей
- Возможно регулярное проведение наших тренингов по широкому кругу тем по запросу руководства компании.

Тестирование и сертификация

Каждый тренинг завершается сессиями закрепления полученных знаний и навыков или тестированием. Благодаря этому руководство компании, а также тренеры «Лаборатории Касперского» получают обратную связь по результатам тренинга, которая помогает оценить успешность тренинга и усовершенствовать наши программы.

Для инженеров и других технических специалистов

Однодневный тренинг по повышению осведомленности в области промышленной кибербезопасности

Тренинг предназначен для повышения осведомленности специалистов вашей компании, не связанных с ИТ/АСУ, об актуальных проблемах промышленной кибербезопасности. Обучение построено на анализе сходства и различия корпоративной и технологической сети, ознакомлении с основами кибербезопасности и спецификой промышленной кибербезопасности.

Однодневный тренинг по повышению осведомленности в области промышленной кибербезопасности для сотрудников, не связанных с ИТ/АСУ

Изучаемые темы		Получаемые знания и навыки
• Различия между корпоративными технологическими системами и их конвергенция; ознакомление с архитектурой технологической сети • Основы информационной безопасности: атаки, уязвимости, эксплойты и вредоносное ПО, угрозы, незащищенность, APT-атаки (сценарии атак) • Профили злоумышленников, атакующих корпоративные и технологические сети • Отношения доверия с третьими сторонами • Роли и границы ответственности • Политики безопасности и порядок их применения • Меры противодействия угрозам	1 день	• Основы информационной безопасности: атаки, профили злоумышленников, угрозы, уязвимости и т. д. • Как распознать инциденты кибербезопасности, вредоносное ПО и атаки с применением методов социальной инженерии • Правила кибербезопасности, меры по ее обеспечению и рекомендации для повседневной работы

Для специалистов ИТ/АСУ

Однодневный тренинг по повышению осведомленности в области промышленной кибербезопасности

Тренинг предназначен для повышения осведомленности специалистов вашей компании в области ИТ/АСУ об актуальных тенденциях в области промышленной кибербезопасности и последних инцидентах безопасности. В процессе обучения рассматриваются основные типы уязвимостей систем промышленной автоматизации, разъясняются принципиальные различия между типичными технологическими и корпоративными компьютерными сетями и дается представление о том, как развитие интернета вещей может повлиять на безопасность систем промышленной автоматизации.

Однодневный тренинг по повышению осведомленности в области промышленной кибербезопасности для специалистов ИТ/АСУ

Изучаемые темы		Получаемые знания и навыки
• Ознакомление с архитектурой технологической сети • Основы сетей: архитектура и топология корпоративной и технологической сетей, компоненты и протоколы, используемые в корпоративной и технологической сетях, различия между корпоративной и технологической сетями и их конвергенция • Как развитие промышленного интернета вещей может повлиять на безопасность систем промышленной автоматизации • Профили злоумышленников, атакующих корпоративные и технологические сети • Основы информационной безопасности: атаки, уязвимости, эксплойты и вредоносное ПО, угрозы, незащищенность, APT-атаки (сценарии атак) • Отношения доверия с третьими сторонами • Роли и границы ответственности • Политики безопасности • Меры противодействия угрозам	1 день	• Основы сетей: стандартная топология, компоненты, протоколы, подходы к проектированию • Основы информационной безопасности: атаки, профили злоумышленников, угрозы, уязвимости и т. д. • Вредоносные атаки + APT-атаки + социальная инженерия • Меры противодействия: сегментация, использование сетевого экрана, контроль доступа для устройств, пользователей, сервисов и т. д. • Усиление мер безопасности и рекомендации

Для руководителей и менеджеров среднего звена

Тренинг по повышению осведомленности в области промышленной кибербезопасности

Тренинг предназначен для повышения осведомленности руководителей и менеджеров среднего звена компаний об актуальных тенденциях в области промышленной кибербезопасности и последних инцидентах безопасности. В процессе обучения рассматриваются основные типы уязвимостей систем промышленной автоматизации, разъясняются принципиальные различия между типичными технологическими и корпоративными сетями и дается представление о том, как развитие интернета вещей может повлиять на безопасность систем промышленной автоматизации.

Тренинг по повышению осведомленности в области промышленной кибербезопасности для руководителей и менеджеров среднего звена

Изучаемые темы		Получаемые знания
• Актуальные проблемы кибербезопасности в системах промышленной автоматизации • Принципиальные различия между типичными технологическими и корпоративными сетями • Информация о возможных атаках на системы SCADA • Ознакомление с принципами защиты сетей • Распознавание методов социальной инженерии • Рекомендации по внедрению эшелонированной защиты • Организация эффективно работающего подразделения кибербезопасности • Своевременная и эффективная работа с инцидентами безопасности • Детальное расследование реальных инцидентов кибербезопасности SCADA • Как развитие интернета вещей может повлиять на безопасность систем промышленной автоматизации	2–3 часа	• Основы информационной безопасности: атаки, профили злоумышленников, угрозы, уязвимости и т. д • Меры противодействия угрозам: сегментация, использование сетевого экрана, контроль доступа для устройств, пользователей, сервисов и т. д. • О вредоносных атаках + APT-атаках + социальной инженерии • Меры по укреплению кибербезопасности

Для специалистов в области безопасности ИТ/АСУ

Практика промышленной кибербезопасности – продвинутый курс

Тренинг позволит специалистам в области ИТ/АСУ переосмыслить свое представление о характере угроз, актуальных для вашего предприятия, и векторах атак, направленных на промышленную инфраструктуру, а также вооружит их всеми необходимыми навыками для подготовки базового плана реагирования на инциденты.

Практика промышленной кибербезопасности – продвинутый курс

Изучаемые темы		Получаемые знания и навыки
• Обзор современного ландшафта угроз, проблем безопасности, вопросов, связанных с человеческим фактором, атак на АСУ ТП • Безопасность компьютерных и технологических сетей – особые вопросы • Пример, демонстрирующий методы предотвращения инцидентов, их обнаружения и минимизации их последствий • Выполнение требований промышленных стандартов и законодательства • Виды топологии сети и принципы действия технологий обеспечения кибербезопасности • Роли и структура команд, ответственных за обеспечение кибербезопасности • Распространенные ошибки в области кибербезопасности	1–2 дня	• Понимание современных угроз кибербезопасности и методов борьбы с инцидентами кибербезопасности в вашей отрасли или организации • Распознавание и обнаружение инцидентов кибербезопасности • Проведение простых расследований • Подготовка и реализация эффективного плана реагирования на инциденты • В состав данного курса входят элементы, подбираемые исходя из специфики предприятия. Возможна адаптация курса для проведения в течение 1 или 2 дней, по желанию заказчика • Сертификация по окончании курса

Для специалистов в области безопасности ИТ/АСУ

Тестирование АСУ ТП на проникновение для специалистов по безопасности ИТ/АСУ

Обучение специалистов по безопасности ИТ/АСУ проведению полного и всестороннего тестирования на проникновение в промышленных средах и подготовке экспертных рекомендаций по принятию мер для исправления выявленных недочетов.

Тестирование на проникновение АСУ ТП для профессионалов

Изучаемые темы		Получаемые знания и навыки
• Введение в компоненты, архитектуру и развертывание АСУ ТП на промышленных объектах, включая компании из таких отраслей, как производство и распределение электроэнергии, нефтегазовый сектор и транспорт • Практические приемы тестирования на проникновение и их применение на АСУ ТП в перечисленных выше и других отраслях • Подготовка плана тестирования на проникновение АСУ ТП – факторы и ограничения, которые следует принимать во внимание • Сбор информации • Анализ уязвимостей в системах SCADA и ПЛК • Анализ результатов тестирования на проникновение и подготовка отчетов • Лабораторные работы	5 дней	• Выявление и анализ уязвимостей в автоматизированных системах управления технологическим процессом • Подготовка эффективного плана тестирования на проникновение АСУ ТП • Безопасное и успешное тестирование SCADA, ПЛК и других элементов систем АСУ ТП • Подготовка экспертных рекомендаций по исправлению выявленных недочетов • Лабораторные работы • Сертификация по окончании курса

Цифровая криминалистика в АСУ ТП для специалистов по безопасности ИТ/АСУ

Тренинг позволит специалистам в области безопасности ИТ/АСУ проводить успешные криминалистические расследования в промышленной инфраструктуре с проведением экспертного анализа и предоставлением рекомендаций.

Цифровая криминалистика в АСУ ТП для профессионалов

Изучаемые темы		Получаемые знания и навыки
• Цели, задачи, приемы и методика криминалистического анализа, типы АСУ ТП, базовая модель криминалистического анализа для АСУ ТП, криминалистический анализ ПЛК • Инструментарий цифровой криминалистики, подготовка к сбору улик и их анализ в режиме реального времени, типичные векторы атак на АСУ ТП, анализ вредоносной активности и лечение систем • Практические упражнения: криминалистический анализ АРМ оператора АСУ ТП, ПЛК и сетевого трафика • Лабораторные работы: расследование атаки на электрическую подстанцию и сбор криминалистических данных на ПЛК	4 дня	• Проведение успешных криминалистических расследований в системах АСУ ТП • Создание эффективного плана расследования инцидентов в системах АСУ ТП • Сбор физических и цифровых улик и их анализ • Применение инструментария цифровой криминалистики для систем АСУ ТП и ПЛК • Обнаружение следов вторжения на основе собранных артефактов • Реконструкция временной шкалы инцидентов и использование метки времени • Профессиональные заключения и рекомендации по предотвращению инцидентов в будущем

Для специалистов в области безопасности ИТ/АСУ

Безопасность интернета вещей

Обучение специалистов по безопасности ИТ/АСУ проведению полного и всестороннего исследования устройств интернета вещей (IoT) на уязвимости и подготовке экспертных рекомендаций по принятию мер для исправления выявленных недочетов.

Безопасность интернета вещей (IoT)

Изучаемые темы		Получаемые знания и навыки
• Введение в IoT: определение интернета вещей и общие отличия IoT-устройств от компьютеров; приложения, архитектура, статистика использования, базовые сценарии использования, интеграция корпоративной и частной инфраструктуры • Аппаратные платформы и архитектура IoT, внутренняя память и коммуникационные интерфейсы, получение и анализ прошивки, отладка устройств с использованием различных интерфейсов • Угрозы и уязвимости в интернете вещей. Модели угроз для различных уровней: прошивки, аппаратного обеспечения и каналов связи • Статистика по вредоносному ПО для устройств интернета вещей, ботнеты из устройств интернета вещей, анализ уязвимостей IoT и выбор защитных мер • Лабораторные работы	4 дня	• Анализ устройств интернета вещей на наличие уязвимостей и выбор защитных мер • Выявление и анализ уязвимостей в устройствах интернета вещей (IoT) • Эффективное исследование уязвимостей в устройствах интернета вещей • Подготовка экспертных рекомендаций по исправлению выявленных недочетов

Игровые тренинги Industrial Cyber-Safety Games

Тренировочные интерактивные модули по кибербезопасности для всех уровней технической подготовки. Игры всегда адаптируются к техническому уровню участников, от руководителей и менеджеров до специалистов по ИТ/АСУ и сотрудников, работающих с системами промышленной автоматизации – на производственных линиях, в аппаратных или операционных подразделениях.

Игровые тренинги Industrial Cyber-Safety Games

Цель тренинга		Получаемые знания и навыки
• Игровой тренинг – это программа повышения осведомленности, основанная на принципе обучения на собственном опыте • Интересный, увлекательный и динамичный процесс обучения • Работа в команде помогает формировать отношения сотрудничества • Соревновательный элемент способствует проявлению инициативы и формированию аналитических навыков • Игровой процесс формирует понимание мер кибербезопасности	2 часа	• Сотрудники делают важные практические выводы, связанные с выполнением их рабочих обязанностей • Для обеспечения кибербезопасности необходимо взаимодействие между ИТ и бизнес-подразделениями • Кибератаки приводят к убыткам, и эту проблему необходимо решать на уровне руководства компании • Эффективно составленный бюджет расходов на кибербезопасность гораздо меньше потенциальных убытков и не исчисляется миллионами • Люди приспосабливаются к конкретным требованиям безопасности (аудиты безопасности, использование антивирусов и т. д.) и осознают их важность

Дальнейшее обучение на всех уровнях

Семинары и технические презентации по индустриальной кибербезопасности

Эти мероприятия, организуемые экспертами Kaspersky Lab ICS CERT, предлагаются в виде единого курса или отдельных вебинаров.

Они включают в себя:

- анализ проблем кибербезопасности промышленных предприятий и систем
- промышленного интернета вещей (IIoT) с разбором конкретных ситуаций
- примеры из реальной жизни – уязвимости, обнаруженные экспертами «Лаборатории Касперского»
- введение в проблематику поиска уязвимостей

Список текущих семинаров и технических презентаций по кибербезопасности систем промышленной автоматизации

Подробная информация предоставляется по запросу
(презентации и семинары имеют продолжительность от 20 минут до 2-3 часов)

- IoT на собственном опыте: введение в безопасность интернета вещей и практические упражнения
- Эксплуатация бинарных уязвимостей в реальном мире
- Побег из песочницы: как обойти изоляцию процессов
- Анализ безопасности ядра Linux
- Ландшафт киберугроз: обзор
- Ландшафт киберугроз для систем промышленной автоматизации
- Угрозы класса APT (advanced persistent threats)
- Атрибуция атак: анализ «артефактов»
- Основы реверс-инжиниринга бинарных приложений – Win32, Win64, dotNET, ELF32, ELF64, Android
- Создание правил YARA
- Создание правил SNORT/Suricata
- Криминалистический анализ в Windows
- Продвинутый реверс-инжиниринг: борьба с упаковщиками, обфускацией и защитой от отладчиков
- Моделирование угроз для решений интернета вещей
- Средства и возможности для киберзащиты систем интернета вещей
- Зрелость систем безопасности. Выделение важнейших мер по повышению уровня безопасности
- Архитектура доверия
- Защита критически важной инфраструктуры – принципы управления по всему миру
- Защита критически важной инфраструктуры и стандарты надежности систем электроэнергетики
- Семинар по криминалистической экспертизе в АСУ ТП
- Реагирование на инциденты в АСУ ТП на практических примерах
- Необычное действие обычных вредоносных программ в технологических сетях

Соревнования Capture the Flag с Kaspersky Lab ICS CERT

Что такое Capture the Flag (CTF)

Соревнования CTF – неотъемлемый элемент нашего портфолио тренингов в области кибербезопасности систем промышленной автоматизации. Мы готовы организовать CTF в соответствии с потребностями вашей компании, предоставив необходимые материалы и персонал. Соревнования CTF могут проводиться в формате Jeopardy («Своя игра»), по сценарию нападение/защита или в виде сочетания обоих форматов.

Эксперты Kaspersky Lab ICS CERT прежде всего проводят совещание на месте проведения CTF, чтобы согласовать формат соревнования CTF и другие общие параметры мероприятия. В ходе совещания эксперты «Лаборатории Касперского» дадут краткий обзор возможных сценариев CTF и помогут вашей компании определиться с целями. По результатам этого предварительного обсуждения мы подготовим примерный сценарий и бюджет конкурса. Для успешного проведения мероприятия клиенту необходимо задействовать руководство компании, спонсоров и, по мере необходимости, привлекать специалистов соответствующих подразделений и направлений, таких как ИТ, информационная безопасность, кадры, PR и т. д.

Как проходит CTF

В соревновании Capture the Flag (CTF) для систем промышленной автоматизации принимают участие люди, интересующиеся темой кибербезопасности систем промышленной автоматизации или обладающие навыками в этой области. CTF проходит в форме соревнования, участники которого решают задачи, связанные с проблемами кибербезопасности в целом и безопасности систем промышленной автоматизации в частности, собирая «флаги» и набирая таким образом очки. Они должны захватывать (атаковать/выводить из строя) или защищать компьютерные системы, работающие в среде CTF. Как правило, это командные соревнования, привлекающие самых разных участников, включая студентов, специалистов в области ИТ/АСУ и даже любителей-энтузиастов кибербезопасности. Конкурс CTF может быть рассчитан на участников с разным уровнем квалификации. Продолжительность соревнований – от нескольких часов до нескольких дней.

Как правило, победителем становится участник или команда, набравшая к концу игры наибольшее количество очков. Как во многих спортивных событиях, обычно присуждаются награды за первое, второе и третье места. Чтобы обеспечить честную борьбу и авторитет игровой платформы, правила CTF обычно сообщаются участникам до начала мероприятия. Нарушение этих правил может повлечь за собой ограничения или даже снятие нарушителя с участия в соревновании.

Что дает CTF

Существует множество причин для организации соревнования CTF, в том числе повышение осведомленности и информирование руководства и технических специалистов предприятия о киберугрозах до того, как компания столкнется с ними в реальной жизни.

Сценарий «нападение-защита» может применяться как для обучения персонала, работающего с системами промышленной автоматизации, реагированию на кибератаки, так и для проверки навыков специалистов по безопасности ИТ/АСУ в условиях, максимально приближенных к сценариям реальных атак.

Конкурс CTF дает хорошую возможность познакомить специалистов по безопасности с современными векторами и сценариями атак, а также сложными тактическими схемами и технологиями, применяемыми различными командами экспертов по кибербезопасности из разных стран.

Перед CTF могут также ставиться задачи, связанные с тестированием автоматизированных систем управления и конфигураций, уже применяемых на предприятии или рассматриваемых на предмет их возможной установки/модернизации. Кроме того, это хорошая возможность проверить в действии продукты и решения для защиты АСУТП, уже используемые компанией или рассматриваемые на предмет их возможной установки в корпоративной итехнологической сетях предприятия.

Более подробную информацию можно получить по запросу.

Наши партнеры

Команда ICS CERT «Лаборатории Касперского» проводит тренинги по повышению осведомленности о киберугрозах и углубленному изучению проблем промышленной кибербезопасности в сотрудничестве с исследователями и специалистами в области образования.

Сегодня наблюдается серьезная нехватка квалифицированных специалистов в области безопасности информационных систем и технических средств систем промышленной автоматизации. Поэтому очень важно обеспечить возможности качественного обучения для профессионального развития в данной области.

Мы, команда Kaspersky Lab ICS CERT, совместно с нашими партнерами создаем новые интерактивные обучающие материалы для специалистов ИТ/АСУ и нетехнического персонала на основе знаний и экспертного опыта технических специалистов Kaspersky Lab ICS CERT и наших партнеров.

Об Abiroy

Abiroy – тренинговая компания, специализирующаяся на реализации комплексных проектов в сфере обучения и подготовки персонала с применением лучших мировых практик.

Abiroy является аккредитованным тренинговым центром для проведения программ таких профессиональных организаций, как Международная академия нефти и газа OPITO, Национальный экзаменационный совет Великобритании по охране труда (NEBOSH), Институт по технике безопасности и охране труда на производстве (IOSH).

Abiroy является компанией, сертифицированной по стандартам ISO-9001:2000, Project Management Expert (PME), и предоставляет сертифицированные программы, основанные на таких международно признанных стандартах в области техники безопасности, как ISO 9000, OHSAS 18001, ILO-OSH 2001, а также соответствует стандартам HSG65.

О Fraunhofer IOSB

Основанный 1 января 2010 года Институт оптроники, технологических систем и использования изображений им.Фраунхофера (Fraunhofer IOSB) стал крупнейшим в Европе исследовательским институтом в области проблем захвата, обработки и анализа изображений.

Среди других областей деятельности Fraunhofer IOSB – системы управления и автоматизации технологического процесса и управление информацией и знаниями. Три ключевые компетенции – оптроника, технологические системы и работа с изображениями – определяют уникальный профиль деятельности института.

Лаборатория информационной безопасности систем промышленной автоматизации, действующая в институте Fraunhofer IOSB, обеспечивает идеальную тестовую среду для моделирования реальных сценариев и анализа их последствий. Для этого используется «умная» установка, в которой стандартные системы промышленной автоматизации управляют моделью промышленного предприятия. При этом задействованы все уровни сетевого взаимодействия, применяемые в промышленных средах, со стандартными компонентами, такими как промышленный Ethernet, промышленные сетевые экраны и беспроводные компоненты.

Об Академии Информационных Систем

Академия информационных систем ведет деятельность на рынке услуг дополнительного профессионального образования с 1996 года.

Слушателями АИС являются руководители и специалисты государственных ведомств и органов власти, предприятий с государственным участием, частных коммерческих организаций, индивидуальные предприниматели и физические лица.

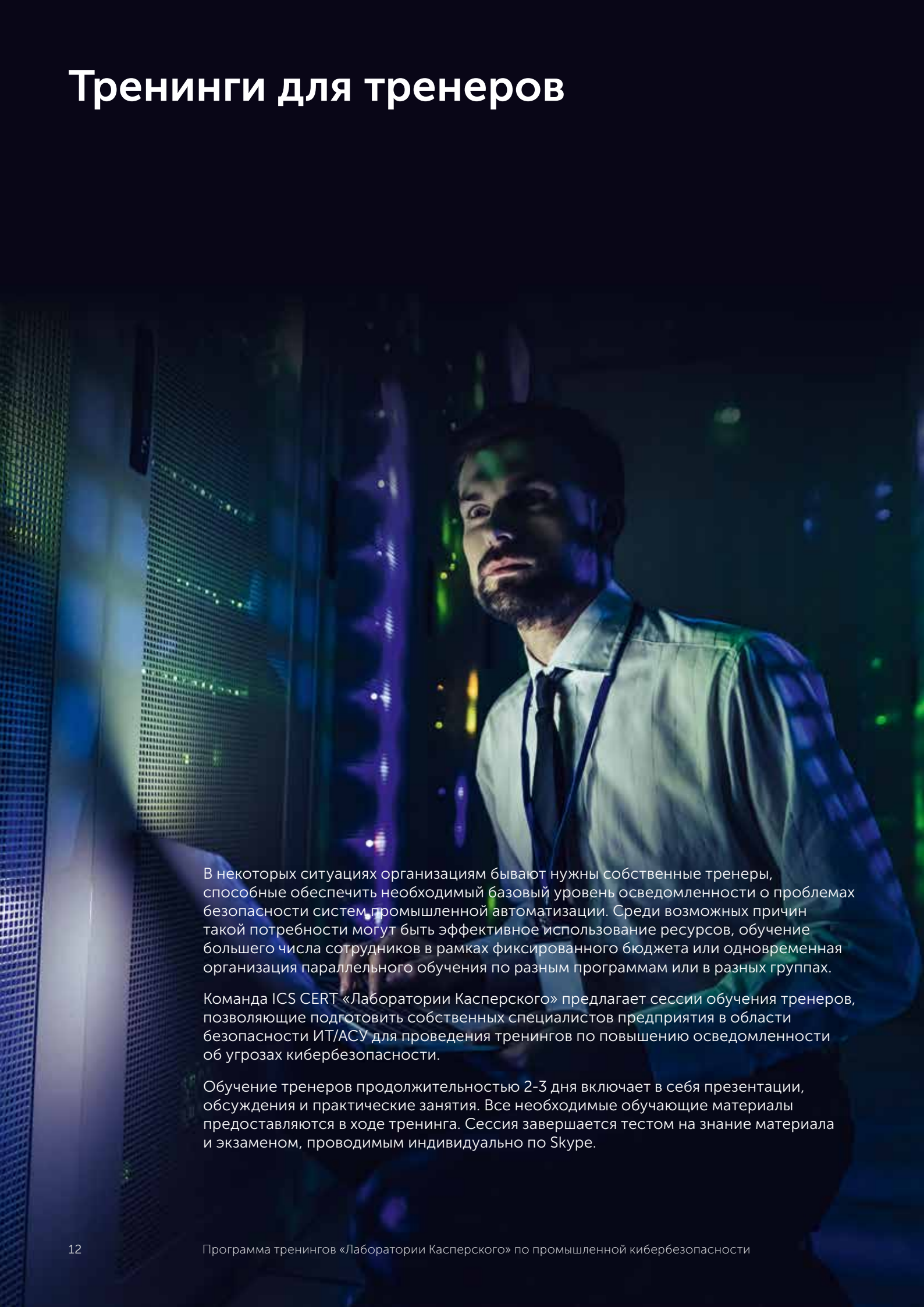
Всего по курсам повышения квалификации и программам профессиональной переподготовки АИС прошли обучение свыше 20 тыс. слушателей.

Курсы АИС читают свыше 50 высококвалифицированных тренеров и преподавателей с большим опытом практической работы, в том числе кандидаты наук, доценты и профессора.

АИС располагает учебными аудиториями и лабораториями для проведения практических занятий по информационным технологиям и средствам защиты информации ведущих российских и зарубежных вендоров (АСКОН, «Лаборатория Касперского», Код Безопасности, ИнфоТекс, КриптоПро, РОСА, Microsoft, StoneSoft, McAfee, ISACA и др.).

Web-sites: www.infosystems.ru, www.vipforum.ru

Тренинги для тренеров



В некоторых ситуациях организациям бывают нужны собственные тренеры, способные обеспечить необходимый базовый уровень осведомленности о проблемах безопасности систем промышленной автоматизации. Среди возможных причин такой потребности могут быть эффективное использование ресурсов, обучение большего числа сотрудников в рамках фиксированного бюджета или одновременная организация параллельного обучения по разным программам или в разных группах.

Команда ICS CERT «Лаборатории Касперского» предлагает сессии обучения тренеров, позволяющие подготовить собственных специалистов предприятия в области безопасности ИТ/АСУ для проведения тренингов по повышению осведомленности об угрозах кибербезопасности.

Обучение тренеров продолжительностью 2-3 дня включает в себя презентации, обсуждения и практические занятия. Все необходимые обучающие материалы предоставляются в ходе тренинга. Сессия завершается тестом на знание материала и экзаменом, проводимым индивидуально по Skype.

Контактная информация

Вам нужна более подробная информация о наших тренингах?

Напишите нам:
Dmitry.Petrovichev@kaspersky.com
Christel.Gampig-Avila@kaspersky.com

О команде Kaspersky Lab ICS CERT

Центр реагирования на инциденты информационной безопасности промышленных инфраструктур «Лаборатории Касперского» (Kaspersky Lab ICS CERT) – глобальный проект «Лаборатории Касперского», нацеленный на координацию действий производителей систем автоматизации, владельцев и операторов промышленных объектов, исследователей информационной безопасности при решении задач защиты промышленных предприятий и объектов критически важных инфраструктур.

Kaspersky Lab ICS CERT ics-cert@kaspersky.com

О Kaspersky Industrial CyberSecurity

Kaspersky® Industrial CyberSecurity

Kaspersky Industrial CyberSecurity — это набор технологий и сервисов, созданных для защиты различных уровней промышленной инфраструктуры и других элементов предприятия, в том числе серверов SCADA, операторских панелей, инженерных рабочих станций, ПЛК, сетевых соединений и даже самих инженеров. При этом решение не влияет на непрерывность технологических процессов.

Узнайте больше на www.kaspersky.com/ics

О «Лаборатории Касперского»

«Лаборатория Касперского» – международная компания, работающая в сфере информационной безопасности с 1997 года. Глубокие экспертные знания и многолетний опыт компании лежат в основе защитных решений и сервисов нового поколения, обеспечивающих безопасность бизнеса, критически важной инфраструктуры, государственных органов и рядовых пользователей. Обширное портфолио «Лаборатории Касперского» включает в себя передовые продукты для защиты конечных устройств, а также ряд специализированных решений и сервисов для борьбы со сложными и постоянно эволюционирующими киберугрозами. Технологии «Лаборатории Касперского» защищают более 400 миллионов пользователей и 270 тысяч корпоративных клиентов во всём мире.
Подробнее на www.kaspersky.ru

www.kaspersky.ru